

The Wealth of Networks

How Social Production
Transforms Markets and
Freedom

Yochai Benkler

Yale University Press
New Haven and London

— 1
— 0
— 1

Copyright © 2006 by Yochai Benkler.
All rights reserved.

Subject to the exception immediately following, this book may not be reproduced, in whole or in part, including illustrations, in any form (beyond that copying permitted by Sections 107 and 108 of the U.S. Copyright Law and except by reviewers for the public press), without written permission from the publishers.

The author has made an online version of the book available under a Creative Commons Noncommercial Sharealike license; it can be accessed through the author's website at <http://www.benkler.org>.

Printed in the United States of America.

Library of Congress Cataloging-in-Publication Data

Benkler, Yochai.

The wealth of networks : how social production transforms markets and freedom / Yochai Benkler.

p. cm.

Includes bibliographical references and index.

ISBN-13: 978-0-300-11056-2 (alk. paper)

ISBN-10: 0-300-11056-1 (alk. paper)

1. Information society. 2. Information networks. 3. Computer networks—Social aspects. 4. Computer networks—Economic aspects.

I. Title.

HM851.B457 2006

303.48'33—dc22 2005028316

A catalogue record for this book is available from the British Library.

The paper in this book meets the guidelines for permanence and durability of the Committee on Production Guidelines for Book Longevity of the Council on Library Resources.

10 9 8 7 6 5 4 3 2 1

STRANGE FRUIT

By Lewis Allan

© 1939 (Renewed) by Music Sales Corporation (ASCAP)

International copyright secured. All rights reserved.

All rights outside the United States controlled by Edward B. Marks Music Company.

Reprinted by permission.

— 1
— 0
— 1

Part Three Policies of Freedom at a Moment of Transformation

Part I of this book offers a descriptive, progressive account of emerging patterns of nonmarket individual and cooperative social behavior, and an analysis of why these patterns are internally sustainable and increase information economy productivity. Part II combines descriptive and normative analysis to claim that these emerging practices offer defined improvements in autonomy, democratic discourse, cultural creation, and justice. I have noted periodically, however, that the descriptions of emerging social practices and the analysis of their potential by no means imply that these changes will necessarily become stable or provide the benefits I ascribe them. They are not a deterministic consequence of the adoption of networked computers as core tools of information production and exchange. There is no inevitable historical force that drives the technological-economic moment toward an open, diverse, liberal equilibrium. If the transformation I describe actually generalizes and stabilizes, it could lead to substantial redistribution of power and money. The twentieth-century industrial producers of information, culture, and communications—like Hollywood, the recording in-

— 1
— 0
— 1

dustry, and some of the telecommunications giants—stand to lose much. The winners would be a combination of the widely diffuse population of individuals around the globe and the firms or other toolmakers and platform providers who supply these newly capable individuals with the context for participating in the networked information economy. None of the industrial giants of yore are taking this threat lying down. Technology will not overcome their resistance through an insurmountable progressive impulse of history. The reorganization of production and the advances it can bring in freedom and justice will emerge only as a result of social practices and political actions that successfully resist efforts to regulate the emergence of the networked information economy in order to minimize its impact on the incumbents.

Since the middle of the 1990s, we have seen intensifying battles over the institutional ecology within which the industrial mode of information production and the newly emerging networked modes compete. Partly, this has been a battle over telecommunications infrastructure regulation. Most important, however, this has meant a battle over “intellectual property” protection, very broadly defined. Building upon and extending a twenty-five-year trend of expansion of copyrights, patents, and similar exclusive rights, the last half-decade of the twentieth century saw expansion of institutional mechanisms for exerting exclusive control in multiple dimensions. The term of copyright was lengthened. Patent rights were extended to cover software and business methods. Trademarks were extended by the Antidilution Act of 1995 to cover entirely new values, which became the basis for liability in the early domain-name trademark disputes. Most important, we saw a move to create new legal tools with which information vendors could hermetically seal access to their materials to an extent never before possible. The Digital Millennium Copyright Act (DMCA) prohibited the creation and use of technologies that would allow users to get at materials whose owners control through encryption. It prohibited even technologies that users can employ to use the materials in ways that the owners have no right to prevent. Today we are seeing efforts to further extend similar technological regulations—down to the level of regulating hardware to make sure that it complies with design specifications created by the copyright industries. At other layers of the communications environment, we see efforts to expand software patents, to control the architecture of personal computing devices, and to create ever-stronger property rights in physical infrastructure—be it the telephone lines, cable plant, or wireless frequencies. Together, these legislative and judicial

— 1
 — 0
 — 1

acts have formed what many have been calling a second enclosure movement: A concerted effort to shape the institutional ecology in order to help proprietary models of information production at the expense of burdening nonmarket, nonproprietary production.¹ The new enclosure movement is not driven purely by avarice and rent seeking—though it has much of that too. Some of its components are based in well-meaning judicial and regulatory choices that represent a particular conception of innovation and its relationship to exclusive rights. That conception, focused on mass-media-type content, movies, and music, and on pharmaceutical-style innovation systems, is highly solicitous of the exclusive rights that are the bread and butter of those culturally salient formats. It is also suspicious of, and detrimental to, the forms of nonmarket, commons-based production emerging in the networked information economy.

This new enclosure movement has been the subject of sustained and diverse academic critique since the mid-1980s.² The core of this rich critique has been that the cases and statutes of the past decade or so have upset the traditional balance, in copyrights in particular, between seeking to create incentives through the grant of exclusive rights and assuring access to information through the judicious limitation of these rights and the privileging of various uses. I do not seek to replicate that work here, or to offer a comprehensive listing of all the regulatory moves that have increased the scope of proprietary rights in digital communications networks. Instead, I offer a way of framing these various changes as moves in a large-scale battle over the institutional ecology of the digital environment. By “institutional ecology,” I mean to say that institutions matter to behavior, but in ways that are more complex than usually considered in economic models. They interact with the technological state, the cultural conceptions of behaviors, and with incumbent and emerging social practices that may be motivated not only by self-maximizing behavior, but also by a range of other social and psychological motivations. In this complex ecology, institutions—most prominently, law—affect these other parameters, and are, in turn, affected by them. Institutions coevolve with technology and with social and market behavior. This coevolution leads to periods of relative stability, punctuated by periods of disequilibrium, which may be caused by external shocks or internally generated phase shifts. During these moments, the various parameters will be out of step, and will pull and tug at the pattern of behavior, at the technology, and at the institutional forms of the behavior. After the tugging and pulling has shaped the various parameters in ways that are more con-

— 1
— 0
— 1

sistent with each other, we should expect to see periods of relative stability and coherence.

Chapter 11 is devoted to an overview of the range of discrete policy areas that are shaping the institutional ecology of digital networks, in which proprietary, market-based models of information production compete with those that are individual, social, and peer produced. In almost all contexts, when presented with a policy choice, advanced economies have chosen to regulate information production and exchange in ways that make it easier to pursue a proprietary, exclusion-based model of production of entertainment goods at the expense of commons- and service-based models of information production and exchange. This has been true irrespective of the political party in power in the United States, or the cultural differences in the salience of market orientation between Europe and the United States. However, the technological trajectory, the social practices, and the cultural understanding are often working at cross-purposes with the regulatory impulse. The equilibrium on which these conflicting forces settle will shape, to a large extent, the way in which information, knowledge, and culture are produced and used over the coming few decades. Chapter 12 concludes the book with an overview of what we have seen about the political economy of information and what we might therefore understand to be at stake in the policy choices that liberal democracies and advanced economies will be making in the coming years.

— 1
— 0
— 1

Chapter 11 The Battle Over the Institutional Ecology of the Digital Environment

The decade straddling the turn of the twenty-first century has seen high levels of legislative and policy activity in the domains of information and communications. Between 1995 and 1998, the United States completely overhauled its telecommunications law for the first time in sixty years, departed drastically from decades of practice on wireless regulation, revolutionized the scope and focus of trademark law, lengthened the term of copyright, criminalized individual user infringement, and created new paracopyright powers for rights holders that were so complex that the 1998 Digital Millennium Copyright Act (DMCA) that enacted them was longer than the entire Copyright Act. Europe covered similar ground on telecommunications, and added a new exclusive right in raw facts in databases. Both the United States and the European Union drove for internationalization of the norms they adopted, through the new World Intellectual Property Organization (WIPO) treaties and, more important, through the inclusion of intellectual property concerns in the international trade regime. In the seven years since then, legal battles have raged over the meaning of these changes, as well

— 1
— 0
— 1

as over efforts to extend them in other directions. From telecommunications law to copyrights, from domain name assignment to trespass to server, we have seen a broad range of distinct regulatory moves surrounding the question of control over the basic resources needed to create, encode, transmit, and receive information, knowledge, and culture in the digital environment. As we telescope up from the details of sundry regulatory skirmishes, we begin to see a broad pattern of conflict over the way that access to these core resources will be controlled.

Much of the formal regulatory drive has been to increase the degree to which private, commercial parties can gain and assert exclusivity in core resources necessary for information production and exchange. At the physical layer, the shift to broadband Internet has been accompanied by less competitive pressure and greater legal freedom for providers to exclude competitors from, and shape the use of, their networks. That freedom from both legal and market constraints on exercising control has been complemented by increasing pressures from copyright industries to require that providers exercise greater control over the information flows in their networks in order to enforce copyrights. At the logical layer, anticircumvention provisions and the efforts to squelch peer-to-peer sharing have created institutional pressures on software and protocols to offer a more controlled and controllable environment. At the content layer, we have seen a steady series of institutional changes aimed at tightening exclusivity.

At each of these layers, however, we have also seen countervailing forces. At the physical layer, the Federal Communications Commission's (FCC's) move to permit the development of wireless devices capable of self-configuring as user-owned networks offers an important avenue for a commons-based last mile. The open standards used for personal computer design have provided an open platform. The concerted resistance against efforts to require computers to be designed so they can more reliably enforce copyrights against their users has, to this point, prevented extension of the DMCA approach to hardware design. At the logical layer, the continued centrality of open standard-setting processes and the emergence of free software as a primary modality of producing mission-critical software provide significant resistance to efforts to enclose the logical layer. At the content layer, where law has been perhaps most systematically one-sided in its efforts to enclose, the cultural movements and the technical affordances that form the foundation of the transformation described throughout this book stand as the most significant barrier to enclosure.

— 1
— 0
— 1

It is difficult to tell how much is really at stake, from the long-term perspective, in all these legal battles. From one point of view, law would have to achieve a great deal in order to replicate the twentieth-century model of industrial information economy in the new technical-social context. It would have to curtail some of the most fundamental technical characteristics of computer networks and extinguish some of our most fundamental human motivations and practices of sharing and cooperation. It would have to shift the market away from developing ever-cheaper general-purpose computers whose value to users is precisely their on-the-fly configurability over time, toward more controllable and predictable devices. It would have to squelch the emerging technologies in wireless, storage, and computation that are permitting users to share their excess resources ever more efficiently. It would have to dampen the influence of free software, and prevent people, young and old, from doing the age-old human thing: saying to each other, “here, why don’t you take this, you’ll like it,” with things they can trivially part with and share socially. It is far from obvious that law can, in fact, achieve such basic changes. From another viewpoint, there may be no need to completely squelch all these things. Lessig called this the principle of bovinity: a small number of rules, consistently applied, suffice to control a herd of large animals. There is no need to assure that all people in all contexts continue to behave as couch potatoes for the true scope of the networked information economy to be constrained. It is enough that the core enabling technologies and the core cultural practices are confined to small groups—some teenagers, some countercultural activists. There have been places like the East Village or the Left Bank throughout the period of the industrial information economy. For the gains in autonomy, democracy, justice, and a critical culture that are described in part II to materialize, the practices of nonmarket information production, individually free creation, and cooperative peer production must become more than fringe practices. They must become a part of life for substantial portions of the networked population. The battle over the institutional ecology of the digitally networked environment is waged precisely over how many individual users will continue to participate in making the networked information environment, and how much of the population of consumers will continue to sit on the couch and passively receive the finished goods of industrial information producers.

— 1
— 0
— 1

INSTITUTIONAL ECOLOGY AND PATH DEPENDENCE

The century-old pragmatist turn in American legal thought has led to the development of a large and rich literature about the relationship of law to society and economy. It has both Right and Left versions, and has disciplinary roots in history, economics, sociology, psychology, and critical theory. Explanations are many: some simple, some complex; some analytically tractable, many not. I do not make a substantive contribution to that debate here, but rather build on some of its strains to suggest that the process is complex, and particularly, that the relationship of law to social relations is one of punctuated equilibrium—there are periods of stability followed by periods of upheaval, and then adaptation and stabilization anew, until the next cycle. Hopefully, the preceding ten chapters have provided sufficient reason to think that we are going through a moment of social-economic transformation today, rooted in a technological shock to our basic modes of information, knowledge, and cultural production. Most of this chapter offers a sufficient description of the legislative and judicial battles of the past few years to make the case that we are in the midst of a significant perturbation of some sort. I suggest that the heightened activity is, in fact, a battle, in the domain of law and policy, over the shape of the social settlement that will emerge around the digital computation and communications revolution.

The basic claim is made up of fairly simple components. First, law affects human behavior on a micromotivational level and on a macro-social-organizational level. This is in contradistinction to, on the one hand, the classical Marxist claim that law is epiphenomenal, and, on the other hand, the increasingly rare simple economic models that ignore transaction costs and institutional barriers and simply assume that people will act in order to maximize their welfare, irrespective of institutional arrangements. Second, the causal relationship between law and human behavior is complex. Simple deterministic models of the form “if law X, then behavior Y” have been used as assumptions, but these are widely understood as, and criticized for being, oversimplifications for methodological purposes. Laws do affect human behavior by changing the payoffs to regulated actions directly. However, they also shape social norms with regard to behaviors, psychological attitudes toward various behaviors, the cultural understanding of actions, and the politics of claims about behaviors and practices. These effects are not all linearly additive. Some push back and nullify the law, some amplify its

— 1
— 0
— 1

effects; it is not always predictable which of these any legal change will be. Decreasing the length of a “Walk” signal to assure that pedestrians are not hit by cars may trigger wider adoption of jaywalking as a norm, affecting ultimate behavior in exactly the opposite direction of what was intended. This change may, in turn, affect enforcement regarding jaywalking, or the length of the signals set for cars, because the risks involved in different signal lengths change as actual expected behavior changes, which again may feed back on driving and walking practices. Third, and as part of the complexity of the causal relation, the effects of law differ in different material, social, and cultural contexts. The same law introduced in different societies or at different times will have different effects. It may enable and disable a different set of practices, and trigger a different cascade of feedback and countereffects. This is because human beings are diverse in their motivational structure and their cultural frames of meaning for behavior, for law, or for outcomes. Fourth, the process of lawmaking is not exogenous to the effects of law on social relations and human behavior. One can look at positive political theory or at the history of social movements to see that the shape of law itself is contested in society because it makes (through its complex causal mechanisms) some behaviors less attractive, valuable, or permissible, and others more so. The “winners” and the “losers” battle each other to tweak the institutional playing field to fit their needs. As a consequence of these, there is relatively widespread acceptance that there is path dependence in institutions and social organization. That is, the actual organization of human affairs and legal systems is not converging through a process of either Marxist determinism or its neoclassical economics mirror image, “the most efficient institutions win out in the end.” Different societies will differ in initial conditions and their historically contingent first moves in response to similar perturbations, and variances will emerge in their actual practices and institutional arrangements that persist over time—irrespective of their relative inefficiency or injustice.

The term “institutional ecology” refers to this context-dependent, causally complex, feedback-ridden, path-dependent process. An example of this interaction in the area of communications practices is the description in chapter 6 of how the introduction of radio was received and embedded in different legal and economic systems early in the twentieth century. A series of organizational and institutional choices converged in all nations on a broadcast model, but the American broadcast model, the BBC model, and the state-run monopoly radio models created very different journalistic styles,

— 1
— 0
— 1

consumption expectations and styles, and funding mechanisms in these various systems. These differences, rooted in a series of choices made during a short period in the 1920s, persisted for decades in each of the respective systems. Paul Starr has argued in *The Creation of the Media* that basic institutional choices—from postage pricing to freedom of the press—interacted with cultural practices and political culture to underwrite substantial differences in the print media of the United States, Britain, and much of the European continent in the late eighteenth and throughout much of the nineteenth centuries.¹ Again, the basic institutional and cultural practices were put in place around the time of the American Revolution, and were later overlaid with the introduction of mass-circulation presses and the telegraph in the mid-1800s. Ithiel de Sola Pool's *Technologies of Freedom* describes the battle between newspapers and telegraph operators in the United States and Britain over control of telegraphed news flows. In Britain, this resulted in the nationalization of telegraph and the continued dominance of London and *The Times*. In the United States, it resolved into the pooling model of the Associated Press, based on private lines for news delivery and sharing—the prototype for newspaper chains and later network-television models of mass media.² The possibility of multiple stable equilibria alongside each other evoked by the stories of radio and print media is a common characteristic to both ecological models and analytically tractable models of path dependency. Both methodological approaches depend on feedback effects and therefore suggest that for any given path divergence, there is a point in time where early actions that trigger feedbacks can cause large and sustained differences over time.

Systems that exhibit path dependencies are characterized by periods of relative pliability followed by periods of relative stability. Institutions and social practices coevolve through a series of adaptations—feedback effects from the institutional system to social, cultural, and psychological frameworks; responses into the institutional system; and success and failure of various behavioral patterns and belief systems—until a society reaches a stage of relative stability. It can then be shaken out of that stability by external shocks—like Admiral Perry's arrival in Japan—or internal buildup of pressure to a point of phase transition, as in the case of slavery in the United States. Of course, not all shocks can so neatly be categorized as external or internal—as in the case of the Depression and the New Deal. To say that there are periods of stability is not to say that in such periods, everything is just dandy for everyone. It is only to say that the political, social, economic

— 1
— 0
— 1

settlement is too widely comfortable for, accepted or acquiesced in, by too many agents who in that society have the power to change practices for institutional change to have substantial effects on the range of lived human practices.

The first two parts of this book explained why the introduction of digital computer-communications networks presents a perturbation of transformative potential for the basic model of information production and exchange in modern complex societies. They focused on the technological, economic, and social patterns that are emerging, and how they differ from the industrial information economy that preceded them. This chapter offers a fairly detailed map of how law and policy are being tugged and pulled in response to these changes. Digital computers and networked communications as a broad category will not be rolled back by these laws. Instead, we are seeing a battle—often but not always self-conscious—over the precise shape of these technologies. More important, we are observing a series of efforts to shape the social and economic practices as they develop to take advantage of these new technologies.

A FRAMEWORK FOR MAPPING THE INSTITUTIONAL ECOLOGY

Two specific examples will illustrate the various levels at which law can operate to shape the use of information and its production and exchange. The first example builds on the story from chapter 7 of how embarrassing internal e-mails from Diebold, the electronic voting machine maker, were exposed by investigative journalism conducted on a nonmarket and peer-production model. After students at Swarthmore College posted the files, Diebold made a demand under the DMCA that the college remove the materials or face suit for contributory copyright infringement. The students were therefore forced to remove the materials. However, in order keep the materials available, the students asked students at other institutions to mirror the files, and injected them into the eDonkey, BitTorrent, and FreeNet file-sharing and publication networks. Ultimately, a court held that the unauthorized publication of files that were not intended for sale and carried such high public value was a fair use. This meant that the underlying publication of the files was not itself a violation, and therefore the Internet service provider was not liable for providing a conduit. However, the case was decided on September 30, 2004—long after the information would have been rele-

— 1
— 0
— 1

vant to the voting equipment certification process in California. What kept the information available for public review was not the ultimate vindication of the students' publication. It was the fact that the materials were kept in the public sphere even under threat of litigation. Recall also that at least some of the earlier set of Diebold files that were uncovered by the activist who had started the whole process in early 2003 were zipped, or perhaps encrypted in some form. Scoop, the Web site that published the revelation of the initial files, published—along with its challenge to the Internet community to scour the files and find holes in the system—links to locations in which utilities necessary for reading the files could be found.

There are four primary potential points of failure in this story that could have conspired to prevent the revelation of the Diebold files, or at least to suppress the peer-produced journalistic mode that made them available. First, if the service provider—the college, in this case—had been a sole provider with no alternative physical transmission systems, its decision to block the materials under threat of suit would have prevented publication of the materials throughout the relevant period. Second, the existence of peer-to-peer networks that overlay the physical networks and were used to distribute the materials made expunging them from the Internet practically impossible. There was no single point of storage that could be locked down. This made the prospect of threatening other universities futile. Third, those of the original files that were not in plain text were readable with software utilities that were freely available on the Internet, and to which Scoop pointed its readers. This made the files readable to many more critical eyes than they otherwise would have been. Fourth, and finally, the fact that access to the raw materials—the e-mails—was ultimately found to be privileged under the fair-use doctrine in copyright law allowed all the acts that had been performed in the preceding period under a shadow of legal liability to proceed in the light of legality.

The second example does not involve litigation, but highlights more of the levers open to legal manipulation. In the weeks preceding the American-led invasion of Iraq, a Swedish video artist produced an audio version of Diana Ross and Lionel Richie's love ballad, "Endless Love," lip-synched to news footage of U.S. president George Bush and British prime minister Tony Blair. By carefully synchronizing the lip movements from the various news clips, the video produced the effect of Bush "singing" Richie's part, and Blair "singing" Ross's, serenading each other with an eternal love ballad. No legal action with regard to the release of this short video has been reported. How-

— 1
— 0
— 1

ever, the story adds two components not available in the context of the Diebold files context. First, it highlights that quotation from video and music requires actual copying of the digital file. Unlike text, you cannot simply transcribe the images or the sound. This means that access to the unencrypted bits is more important than in the case of text. Second, it is not at all clear that using the entire song, unmodified, is a “fair use.” While it is true that the Swedish video is unlikely to cut into the market for the original song, there is nothing in the video that is a parody either of the song itself or of the news footage. The video uses “found materials,” that is, materials produced by others, to mix them in a way that is surprising, creative, and creates a genuinely new statement. However, its use of the song is much more complete than the minimalist uses of digital sampling in recorded music, where using a mere two-second, three-note riff from another’s song has been found to be a violation unless done with a negotiated license.³

Combined, the two stories suggest that we can map the resources necessary for a creative communication, whether produced on a market model or a nonmarket model, as including a number of discrete elements. First, there is the universe of “content” itself: existing information, cultural artifacts and communications, and knowledge structures. These include the song and video footage, or the e-mail files, in the two stories. Second, there is the cluster of machinery that goes into capturing, manipulating, fixing and communicating the new cultural utterances or communications made of these inputs, mixed with the creativity, knowledge, information, or communications capacities of the creator of the new statement or communication. These include the physical devices—the computers used by the students and the video artist, as well as by their readers or viewers—and the physical transmission mechanisms used to send the information or communications from one place to another. In the Diebold case, the firm tried to use the Internet service provider liability regime of the DMCA to cut off the machine storage and mechanical communications capacity provided to the students by the university. However, the “machinery” also includes the logical components—the software necessary to capture, read or listen to, cut, paste, and remake the texts or music; the software and protocols necessary to store, retrieve, search, and communicate the information across the Internet.

As these stories suggest, freedom to create and communicate requires use of diverse things and relationships—mechanical devices and protocols, information, cultural materials, and so forth. Because of this diversity of com-

— 1
— 0
— 1

ponents and relationships, the institutional ecology of information production and exchange is a complex one. It includes regulatory and policy elements that affect different industries, draw on various legal doctrines and traditions, and rely on diverse economic and political theories and practices. It includes social norms of sharing and consumption of things conceived of as quite different—bandwidth, computers, and entertainment materials. To make these cohere into a single problem, for several years I have been using a very simple, three-layered representation of the basic functions involved in mediated human communications. These are intended to map how different institutional components interact to affect the answer to the basic questions that define the normative characteristics of a communications system—who gets to say what, to whom, and who decides?⁴

These are the physical, logical, and content layers. The physical layer refers to the material things used to connect human beings to each other. These include the computers, phones, handhelds, wires, wireless links, and the like. The content layer is the set of humanly meaningful statements that human beings utter to and with one another. It includes both the actual utterances and the mechanisms, to the extent that they are based on human communication rather than mechanical processing, for filtering, accreditation, and interpretation. The logical layer represents the algorithms, standards, ways of translating human meaning into something that machines can transmit, store, or compute, and something that machines process into communications meaningful to human beings. These include standards, protocols, and software—both general enabling platforms like operating systems, and more specific applications. A mediated human communication must use all three layers, and each layer therefore represents a resource or a pathway that the communication must use or traverse in order to reach its intended destination. In each and every one of these layers, we have seen the emergence of technical and practical capabilities for using that layer on a nonproprietary model that would make access cheaper, less susceptible to control by any single party or class of parties, or both. In each and every layer, we have seen significant policy battles over whether these nonproprietary or open-platform practices will be facilitated or even permitted. Looking at the aggregate effect, we see that at all these layers, a series of battles is being fought over the degree to which some minimal set of basic resources and capabilities necessary to use and participate in constructing the information environment will be available for use on a nonproprietary, nonmarket basis.

— 1
 — 0
 — 1

In each layer, the policy debate is almost always carried out in local, specific terms. We ask questions like, Will this policy optimize “spectrum management” in these frequencies, or, Will this decrease the number of CDs sold? However, the basic, overarching question that we must learn to ask in all these debates is: Are we leaving enough institutional space for the social-economic practices of networked information production to emerge? The networked information economy requires access to a core set of capabilities—existing information and culture, mechanical means to process, store, and communicate new contributions and mixes, and the logical systems necessary to connect them to each other. What nonmarket forms of production need is a core common infrastructure that anyone can use, irrespective of whether their production model is market-based or not, proprietary or not. In almost all these dimensions, the current trajectory of technological-economic-social trends is indeed leading to the emergence of such a core common infrastructure, and the practices that make up the networked information economy are taking advantage of open resources. Wireless equipment manufacturers are producing devices that let users build their own networks, even if these are now at a primitive stage. The open-innovation ethos of the programmer and Internet engineering community produce both free software and proprietary software that rely on open standards for providing an open logical layer. The emerging practices of free sharing of information, knowledge, and culture that occupy most of the discussion in this book are producing an ever-growing stream of freely and openly accessible content resources. The core common infrastructure appears to be emerging without need for help from a guiding regulatory hand. This may or may not be a stable pattern. It is possible that by some happenstance one or two firms, using one or two critical technologies, will be able to capture and control a bottleneck. At that point, perhaps regulatory intervention will be required. However, from the beginning of legal responses to the Internet and up to this writing in the middle of 2005, the primary role of law has been reactive and reactionary. It has functioned as a point of resistance to the emergence of the networked information economy. It has been used by incumbents from the industrial information economies to contain the risks posed by the emerging capabilities of the networked information environment. What the emerging networked information economy therefore needs, in almost all cases, is not regulatory protection, but regulatory abstinence.

The remainder of this chapter provides a more or less detailed presentation of the decisions being made at each layer, and how they relate to the freedom

— 1
— 0
— 1

to create, individually and with others, without having to go through proprietary, market-based transactional frameworks. Because so many components are involved, and so much has happened since the mid-1990s, the discussion is of necessity both long in the aggregate and truncated in each particular category. To overcome this expositional problem, I have collected the various institutional changes in table 11.1. For readers interested only in the overarching claim of this chapter—that is, that there is, in fact, a battle over the institutional environment, and that many present choices interact to increase or decrease the availability of basic resources for information production and exchange—table 11.1 may provide sufficient detail. For those interested in a case study of the complex relationship between law, technology, social behavior, and market structure, the discussion of peer-to-peer networks may be particularly interesting to pursue.

A quick look at table 11.1 reveals that there is a diverse set of sources of openness. A few of these are legal. Mostly, they are based on technological and social practices, including resistance to legal and regulatory drives toward enclosure. Examples of policy interventions that support an open core common infrastructure are the FCC's increased permission to deploy open wireless networks and the various municipal broadband initiatives. The former is a regulatory intervention, but its form is largely removal of past prohibitions on an entire engineering approach to building wireless systems. Municipal efforts to produce open broadband networks are being resisted at the state legislation level, with statutes that remove the power to provision broadband from the home rule powers of municipalities. For the most part, the drive for openness is based on individual and voluntary cooperative action, not law. The social practices of openness take on a quasi-normative face when practiced in standard-setting bodies like the Internet Engineering Task Force (IETF) or the World Wide Web Consortium (W3C). However, none of these have the force of law. Legal devices also support openness when used in voluntaristic models like free software licensing and Creative Commons-type licensing. However, most often when law has intervened in its regulatory force, as opposed to its contractual-enablement force, it has done so almost entirely on the side of proprietary enclosure.

Another characteristic of the social-economic-institutional struggle is an alliance between a large number of commercial actors and the social sharing culture. We see this in the way that wireless equipment manufacturers are selling into a market of users of WiFi and similar unlicensed wireless devices. We see this in the way that personal computer manufacturers are competing

— 1
— 0
— 1

Table 11.1: Overview of the Institutional Ecology

	Enclosure	Openness
<i>Physical</i> Transport	<ul style="list-style-type: none"> • Broadband treated by FCC as information service • DMCA ISP liability • Municipal broadband barred by states 	<ul style="list-style-type: none"> • Open wireless networks • Municipal broadband initiatives
<i>Physical</i> Devices	<ul style="list-style-type: none"> • CBDPTA: regulatory requirements to implement “trusted systems”; private efforts toward the same goal • Operator-controlled mobile phones 	<ul style="list-style-type: none"> • Standardization • Fiercely competitive market in commodity components
<i>Logical</i> Transmission protocols	Privatized DNS/ICANN	<ul style="list-style-type: none"> • TCP/IP • IETF • p2p networks
<i>Logical</i> Software	DMCA anticircumvention; Proprietary OS; Web browser Software patents	<ul style="list-style-type: none"> • Free software • W3C • P2p software widely used • social acceptability of widespread hacking of copy protection
<i>Content</i>	<ul style="list-style-type: none"> • Copyright expansion • “Right to read” • No de minimis digital sampling • “Fair use” narrowed: effect on potential market “commercial” defined broadly • Criminalization • Term extension • Contractual enclosure: UCITA • Trademark dilution • Database protection • Linking and trespass to chattels • International “harmonization” and trade enforcement of maximal exclusive rights regimes 	<ul style="list-style-type: none"> • Increasing sharing practices and adoption of sharing licensing practices • Musicians distribute music freely • Creative Commons; other open publication models • Widespread social disdain for copyright • International jurisdictional arbitrage • Early signs of a global access to knowledge movement combining developing nations with free information ecology advocates, both market and non-market, raising a challenge to the enclosure movement

— 1
— 0
— 1

over decreasing margins by producing the most general-purpose machines that would be most flexible for their users, rather than machines that would most effectively implement the interests of Hollywood and the recording industry. We see this in the way that service and equipment-based firms, like IBM and Hewlett-Packard (HP), support open-source and free software. The alliance between the diffuse users and the companies that are adapting their business models to serve them as users, instead of as passive consumers, affects the political economy of this institutional battle in favor of openness. On the other hand, security consciousness in the United States has led to some efforts to tip the balance in favor of closed proprietary systems, apparently because these are currently perceived as more secure, or at least more amenable to government control. While orthogonal in its political origins to the battle between proprietary and commons-based strategies for information production, this drive does tilt the field in favor of enclosure, at least at the time of this writing in 2005.

Over the past few years, we have also seen that the global character of the Internet is a major limit on effective enclosure, when openness is a function of technical and social practices, and enclosure is a function of law.⁵ When Napster was shut down in the United States, for example, KaZaa emerged in the Netherlands, from where it later moved to Australia. This force is meeting the countervailing force of international harmonization—a series of bilateral and multilateral efforts to “harmonize” exclusive rights regimes internationally and efforts to coordinate international enforcement. It is difficult at this stage to predict which of these forces will ultimately have the upper hand. It is not too early to map in which direction each is pushing. And it is therefore not too early to characterize the normative implications of the success or failure of these institutional efforts.

THE PHYSICAL LAYER

The physical layer encompasses both transmission channels and devices for producing and communicating information. In the broadcast and telephone era, devices were starkly differentiated. Consumers owned dumb terminals. Providers owned sophisticated networks and equipment: transmitters and switches. Consumers could therefore consume whatever providers could produce most efficiently that the providers believed consumers would pay for. Central to the emergence of the freedom of users in the networked environment is an erosion of the differentiation between consumer and provider

— 1
— 0
— 1

equipment. Consumers came to use general-purpose computers that could do whatever their owners wanted, instead of special-purpose terminals that could only do what their vendors designed them to do. These devices were initially connected over a transmission network—the public phone system—that was regulated as a common carrier. Common carriage required the network owners to carry all communications without differentiating by type or content. The network was neutral as among communications. The transition to broadband networks, and to a lesser extent the emergence of Internet services on mobile phones, are threatening to undermine that neutrality and nudge the network away from its end-to-end, user-centric model to one designed more like a five-thousand-channel broadcast model. At the same time, Hollywood and the recording industry are pressuring the U.S. Congress to impose regulatory requirements on the design of personal computers so that they can be relied on not to copy music and movies without permission. In the process, the law seeks to nudge personal computers away from being purely general-purpose computation devices toward being devices with factory-defined behaviors vis-à-vis predicted-use patterns, like glorified televisions and CD players. The emergence of the networked information economy as described in this book depends on the continued existence of an open transport network connecting general-purpose computers. It therefore also depends on the failure of the efforts to restructure the network on the model of proprietary networks connecting terminals with sufficiently controlled capabilities to be predictable and well behaved from the perspective of incumbent production models.

Transport: Wires and Wireless

Recall the Cisco white paper quoted in chapter 5. In it, Cisco touted the value of its then new router, which would allow a broadband provider to differentiate streams of information going to and from the home at the packet level. If the packet came from a competitor, or someone the user wanted to see or hear but the owner preferred that the user did not, the packet could be slowed down or dropped. If it came from the owner or an affiliate, it could be speeded up. The purpose of the router was not to enable evil control over users. It was to provide better-functioning networks. America Online (AOL), for example, has been reported as blocking its users from reaching Web sites that have been advertised in spam e-mails. The theory is that if spammers know their Web site will be inaccessible to AOL customers, they will stop.⁶ The ability of service providers to block sites or packets from

— 1
— 0
— 1

certain senders and promote packets from others may indeed be used to improve the network. However, whether this ability will in fact be used to improve service depends on the extent to which the interests of all users, and particularly those concerned with productive uses of the network, are aligned with the interests of the service providers. Clearly, when in 2005 Telus, Canada's second largest telecommunications company, blocked access to the Web site of the Telecommunications Workers Union for all of its own clients and those of internet service providers that relied on its backbone network, it was not seeking to improve service for those customers' benefit, but to control a conversation in which it had an intense interest. When there is a misalignment, the question is what, if anything, disciplines the service providers' use of the technological capabilities they possess? One source of discipline would be a genuinely competitive market. The transition to broadband has, however, severely constrained the degree of competition in Internet access services. Another would be regulation: requiring owners to treat all packets equally. This solution, while simple to describe, remains highly controversial in the policy world. It has strong supporters and strong opposition from the incumbent broadband providers, and has, as a practical matter, been rejected for the time being by the FCC. The third type of solution would be both more radical and less "interventionist" from the perspective of regulation. It would involve eliminating contemporary regulatory barriers to the emergence of a user-owned wireless infrastructure. It would allow users to deploy their own equipment, share their wireless capacity, and create a "last mile" owned by all users in common, and controlled by none. This would, in effect, put equipment manufacturers in competition to construct the "last mile" of broadband networks, and thereby open up the market in "middle-mile" Internet connection services.

Since the early 1990s, when the Clinton administration announced its "Agenda for Action" for what was then called "the information superhighway," it was the policy of the United States to "let the private sector lead" in deployment of the Internet. To a greater or lesser degree, this commitment to private provisioning was adopted in most other advanced economies in the world. In the first few years, this meant that investment in the backbone of the Internet was private, and heavily funded by the stock bubble of the late 1990s. It also meant that the last distribution bottleneck—the "last mile"—was privately owned. Until the end of the 1990s, the last mile was made mostly of dial-up connections over the copper wires of the incumbent local exchange carriers. This meant that the physical layer was not only

— 1
— 0
— 1

proprietary, but that it was, for all practical purposes, monopolistically owned. Why, then, did the early Internet nonetheless develop into a robust, end-to-end neutral network? As Lessig showed, this was because the telephone carriers were regulated as common carriers. They were required to carry all traffic without discrimination. Whether a bit stream came from Cable News Network (CNN) or from an individual blog, all streams—upstream from the user and downstream to the user—were treated neutrally.

BROADBAND REGULATION

The end of the 1990s saw the emergence of broadband networks. In the United States, cable systems, using hybrid fiber-coaxial systems, moved first, and became the primary providers. The incumbent local telephone carriers have been playing catch-up ever since, using digital subscriber line (DSL) techniques to squeeze sufficient speed out of their copper infrastructure to remain competitive, while slowly rolling out fiber infrastructure closer to the home. As of 2003, the incumbent cable carriers and the incumbent local telephone companies accounted for roughly 96 percent of all broadband access to homes and small offices.⁷ In 1999–2000, as cable was beginning to move into a more prominent position, academic critique began to emerge, stating that the cable broadband architecture could be manipulated to deviate from the neutral, end-to-end architecture of the Internet. One such paper was written by Jerome Saltzer, one of the authors of the paper that originally defined the “end-to-end” design principle of the Internet in 1980, and Lessig and Mark Lemley wrote another. These papers began to emphasize that cable broadband providers technically could, and had commercial incentive to, stop treating all communications neutrally. They could begin to move from a network where almost all functions are performed by user-owned computers at the ends of the network to one where more is done by provider equipment at the core. The introduction of the Cisco policy router was seen as a stark marker of how things could change.

The following two years saw significant regulatory battles over whether the cable providers would be required to behave as commons carriers. In particular, the question was whether they would be required to offer competitors nondiscriminatory access to their networks, so that these competitors could compete in Internet services. The theory was that competition would discipline the incumbents from skewing their networks too far away from what users valued as an open Internet. The first round of battles occurred at the municipal level. Local franchising authorities tried to use their power

— 1
— 0
— 1

over cable licenses to require cable operators to offer open access to their competitors if they chose to offer cable broadband. The cable providers challenged these regulations in courts. The most prominent decision came out of Portland, Oregon, where the Federal Court of Appeals for the Ninth Circuit held that broadband was part information service and part telecommunications service, but not a cable service. The FCC, not the cable franchising authority, had power to regulate it.⁸ At the same time, as part of the approval of the AOL–Time Warner merger, the Federal Trade Commission (FTC) required the new company to give at least three competitors open access to its broadband facilities, should AOL be offered cable broadband facilities over Time Warner.

The AOL–Time Warner merger requirements, along with the Ninth Circuit’s finding that cable broadband included a telecommunications component, seemed to indicate that cable broadband transport would come to be treated as a common carrier. This was not to be. In late 2001 and the middle of 2002, the FCC issued a series of reports that would reach the exact opposite result. Cable broadband, the commission held, was an information service, not a telecommunications service. This created an imbalance with the telecommunications status of broadband over telephone infrastructure, which at the time was treated as a telecommunications service. The commission dealt with this imbalance by holding that broadband over telephone infrastructure, like broadband over cable, was now to be treated as an information service. Adopting this definition was perhaps admissible as a matter of legal reasoning, but it certainly was not required by either sound legal reasoning or policy. The FCC’s reasoning effectively took the business model that cable operators had successfully used to capture two-thirds of the market in broadband—bundling two discrete functionalities, transport (carrying bits) and higher-level services (like e-mail and Web hosting)—and treated it as though it described the intrinsic nature of “broadband cable” as a service. Because that service included more than just carriage of bits, it could be called an information service. Of course, it would have been as legally admissible, and more technically accurate, to do as the Ninth Circuit had done. That is, to say that cable broadband bundles two distinct services: carriage and information-use tools. The former is a telecommunications service. In June of 2005, the Supreme Court in the *Brand X* case upheld the FCC’s authority to make this legally admissible policy error, upholding as a matter of deference to the expert agency the Commission’s position that cable broadband services should be treated as information services.⁹ As a matter

— 1
 — 0
 — 1

of policy, the designation of broadband services as “information services” more or less locked the FCC into a “no regulation” approach. As information services, broadband providers obtained the legal power to “edit” their programming, just like any operator of an information service, like a Web site. Indeed, this new designation has placed a serious question mark over whether future efforts to regulate carriage decisions would be considered constitutional, or would instead be treated as violations of the carriers’ “free speech” rights as a provider of information. Over the course of the 1990s, there were a number of instances where carriers—particularly cable, but also telephone companies—were required by law to carry some signals from competitors. In particular, cable providers were required to carry over-the-air broadcast television, telephone carriers, in FCC rules called “video dialtone,” were required to offer video on a common carriage basis, and cable providers that chose to offer broadband were required to make their infrastructure available to competitors on a common carrier model. In each of these cases, the carriage requirements were subjected to First Amendment scrutiny by courts. In the case of cable carriage of broadcast television, the carriage requirements were only upheld after six years of litigation.¹⁰ In cases involving video common carriage requirements applied to telephone companies and cable broadband, lower courts struck down the carriage requirements as violating the telephone and cable companies’ free-speech rights.¹¹ To a large extent, then, the FCC’s regulatory definition left the incumbent cable and telephone providers—who control 96 percent of broadband connections to home and small offices—unregulated, and potentially constitutionally immune to access regulation and carriage requirements.

Since 2003 the cable access debate—over whether competitors should get access to the transport networks of incumbent broadband carriers—has been replaced with an effort to seek behavioral regulation in the form of “network neutrality.” This regulatory concept would require broadband providers to treat all packets equally, without forcing them to open their network up to competitors or impose any other of the commitments associated with common carriage. The concept has the backing of some very powerful actors, including Microsoft, and more recently MCI, which still owns much of the Internet backbone, though not the last mile. For this reason, if for no other, it remains as of this writing a viable path for institutional reform that would balance the basic structural shift of Internet infrastructure from a common-carriage to a privately controlled model. Even if successful, the drive to network neutrality would keep the physical infrastructure a technical bottle-

— 1
 — 0
 — 1

neck, owned by a small number of firms facing very limited competition, with wide legal latitude for using that control to affect the flow of information over their networks.

OPEN WIRELESS NETWORKS

A more basic and structural opportunity to create an open broadband infrastructure is, however, emerging in the wireless domain. To see how, we must first recognize that opportunities to control the broadband infrastructure in general are not evenly distributed throughout the networked infrastructure. The long-haul portions of the network have multiple redundant paths with no clear choke points. The primary choke point over the physical transport of bits across the Internet is in the last mile of all but the most highly connected districts. That is, the primary bottleneck is the wire or cable connecting the home and small office to the network. It is here that cable and local telephone incumbents control the market. It is here that the high costs of digging trenches, pulling fiber, and getting wires through and into walls pose a prohibitive barrier to competition. And it is here, in the last mile, that unlicensed wireless approaches now offer the greatest promise to deliver a common physical infrastructure of first and last resort, owned by its users, shared as a commons, and offering no entity a bottleneck from which to control who gets to say what to whom.

As discussed in chapter 6, from the end of World War I and through the mid-twenties, improvements in the capacity of expensive transmitters and a series of strategic moves by the owners of the core patents in radio transmission led to the emergence of the industrial model of radio communications that typified the twentieth century. Radio came to be dominated by a small number of professional, commercial networks, based on high-capital-cost transmitters. These were supported by a regulatory framework tailored to making the primary model of radio utilization for most Americans passive reception, with simple receivers, of commercial programming delivered with high-powered transmitters. This industrial model, which assumed large-scale capital investment in the core of the network and small-scale investments at the edges, optimized for receiving what is generated at the core, imprinted on wireless communications systems both at the level of design and at the level of regulation. When mobile telephony came along, it replicated the same model, using relatively cheap handsets oriented toward an infrastructure-centric deployment of towers. The regulatory model followed Hoover's initial pattern and perfected it. A government agency strictly controlled who may

— 1
— 0
— 1

place a transmitter, where, with what antenna height, and using what power. The justification was avoidance of interference. The presence of strict licensing was used as the basic assumption in the engineering of wireless systems throughout this period. Since 1959, economic analysis of wireless regulation has criticized this approach, but only on the basis that it inefficiently regulated the legal right to construct a wireless system by using strictly regulated spectrum licenses, instead of creating a market in “spectrum use” rights.¹² This critique kept the basic engineering assumptions stable—for radio to be useful, a high-powered transmitter must be received by simple receivers. Given this engineering assumption, someone had to control the right to emit energy in any range of radio frequencies. The economists wanted the controller to be a property owner with a flexible, transferable right. The regulators wanted it to be a licensee subject to regulatory oversight and approval by the FCC.

As chapter 3 explained, by the time that legislatures in the United States and around the world had begun to accede to the wisdom of the economists’ critique, it had been rendered obsolete by technology. In particular, it had been rendered obsolete by the fact that the declining cost of computation and the increasing sophistication of communications protocols among end-user devices in a network made possible new, sharing-based solutions to the problem of how to allow users to communicate without wires. Instead of having a regulation-determined exclusive right to transmit, which may or may not be subject to market reallocation, it is possible to have a market in smart radio equipment owned by individuals. These devices have the technical ability to share capacity and cooperate in the creation of wireless carriage capacity. These radios can, for example, cooperate by relaying each other’s messages or temporarily “lending” their antennae to neighbors to help them decipher messages of senders, without anyone having exclusive use of the spectrum. Just as PCs can cooperate to create a supercomputer in SETI@Home by sharing their computation, and a global-scale, peer-to-peer data-storage and retrieval system by sharing their hard drives, computationally intensive radios can share their capacity to produce a local wireless broadband infrastructure. Open wireless networks allow users to install their own wireless device—much like the WiFi devices that have become popular. These devices then search automatically for neighbors with similar capabilities, and self-configure into a high-speed wireless data network. Reaching this goal does not, at this point, require significant technological innovation. The technology is there, though it does require substantial en-

___ 1
___ 0
___ 1

gineering effort to implement. The economic incentives to develop such devices are fairly straightforward. Users already require wireless local networks. They will gain added utility from extending their range for themselves, which would be coupled with the possibility of sharing with others to provide significant wide-area network capacity for whose availability they need not rely on any particular provider. Ultimately, it would be a way for users to circumvent the monopoly last mile and recapture some of the rents they currently pay. Equipment manufacturers obviously have an incentive to try to cut into the rents captured by the broadband monopoly/oligopoly by offering an equipment-embedded alternative.

My point here is not to consider the comparative efficiency of a market in wireless licenses and a market in end-user equipment designed for sharing channels that no one owns. It is to highlight the implications of the emergence of a last mile that is owned by no one in particular, and is the product of cooperation among neighbors in the form of, “I’ll carry your bits if you carry mine.” At the simplest level, neighbors could access locally relevant information directly, over a wide-area network. More significant, the fact that users in a locality coproduced their own last-mile infrastructure would allow commercial Internet providers to set up Internet points of presence anywhere within the “cloud” of the locale. The last mile would be provided not by these competing Internet service providers, but by the cooperative efforts of the residents of local neighborhoods. Competitors in providing the “middle mile”—the connection from the last mile to the Internet cloud—could emerge, in a way that they cannot if they must first lay their own last mile all the way to each home. The users, rather than the middle-mile providers, shall have paid the capital cost of producing the local transmission system—their own cooperative radios. The presence of a commons-based, coproduced last mile alongside the proprietary broadband network eliminates the last mile as a bottleneck for control over who speaks, with what degree of ease, and with what types of production values and interactivity.

The development of open wireless networks, owned by their users and focused on sophisticated general-purpose devices at their edges also offers a counterpoint to the emerging trend among mobile telephony providers to offer a relatively limited and controlled version of the Internet over the phones they sell. Some wireless providers are simply offering mobile Internet connections throughout their networks, for laptops. Others, however, are using their networks to allow customers to use their ever-more-sophisticated phones to surf portions of the Web. These latter services diverge in their

— 1
— 0
— 1

styles. Some tend to be limited, offering only a set of affiliated Web sites rather than genuine connectivity to the Internet itself with a general-purpose device. Sprint's "News" offerings, for example, connects users to CNNtoGo, ABCNews.com, and the like, but will not enable a user to reach the blogosphere to upload a photo of protesters being manhandled, for example. So while mobility in principle increases the power of the Web, and text messaging puts e-mail-like capabilities everywhere, the effect of the implementations of the Web on phones is more ambiguous. It could be more like a Web-enabled reception device than a genuinely active node in a multidirectional network. Widespread adoption of open wireless networks would give mobile phone manufacturers a new option. They could build into the mobile telephones the ability to tap into open wireless networks, and use them as general-purpose access points to the Internet. The extent to which this will be a viable option for the mobile telephone manufacturers depends on how much the incumbent mobile telephone service providers, those who purchased their licenses at high-priced auctions, will resist this move. Most users buy their phones from their providers, not from general electronic equipment stores. Phones are often tied to specific providers in ways that users are not able to change for themselves. In these conditions, it is likely that mobile providers will resist the competition from free open wireless systems for "data minutes" by refusing to sell dual-purpose equipment. Worse, they may boycott manufacturers who make mobile phones that are also general-purpose Web-surfing devices over open wireless networks. How that conflict will go, and whether users would be willing to carry a separate small device to enable them to have open Internet access alongside their mobile phone, will determine the extent to which the benefits of open wireless networks will be transposed into the mobile domain. Normatively, that outcome has significant implications. From the perspective of the citizen watchdog function, ubiquitous availability of capture, rendering, and communication capabilities are important. From the perspective of personal autonomy as informed action in context, extending openness to mobile units would provide significant advantages to allow individuals to construct their own information environment on the go, as they are confronting decisions and points of action in their daily lives.

MUNICIPAL BROADBAND INITIATIVES

One alternative path for the emergence of basic physical information transport infrastructure on a nonmarket model is the drive to establish municipal

___ 1
 ___ 0
 ___ 1

systems. These proposed systems would not be commons-based in the sense that they would not be created by the cooperative actions of individuals without formal structure. They would be public, like highways, sidewalks, parks, and sewage systems. Whether they are, or are not, ultimately to perform as commons would depend on how they would be regulated. In the United States, given the First Amendment constraints on government preferring some speech to other speech in public fora, it is likely that municipal systems would be managed as commons. In this regard, they would have parallel beneficial characteristics to those of open wireless systems. The basic thesis underlying municipal broadband initiatives is similar to that which has led some municipalities to create municipal utilities or transportation hubs. Connectivity has strong positive externalities. It makes a city's residents more available for the information economy and the city itself a more attractive locale for businesses. Most of the efforts have indeed been phrased in these instrumental terms. The initial drive has been the creation of municipal fiber-to-the-home networks. The town of Bristol, Virginia, is an example. It has a population of slightly more than seventeen thousand. Median household income is 68 percent of the national median. These statistics made it an unattractive locus for early broadband rollout by incumbent providers. However, in 2003, Bristol residents had one of the most advanced residential fiber-to-the-home networks in the country, available for less than forty dollars a month. Unsurprisingly, therefore, the city had broadband penetration rivaling many of the top U.S. markets with denser and wealthier populations. The "miracle" of Bristol is that the residents of the town, fed up with waiting for the local telephone and cable companies, built their own, municipally owned network. Theirs has become among the most ambitious and successful of more than five hundred publicly owned utilities in the United States that offer high-speed Internet, cable, and telephone services to their residents. Some of the larger cities—Chicago and Philadelphia, most prominently—are moving as of this writing in a similar direction. The idea in Chicago is that basic "dark fiber"—that is, the physical fiber going to the home, but without the electronics that would determine what kinds of uses the connectivity could be put to—would be built by the city. Access to use this entirely neutral, high-capacity platform would then be open to anyone—commercial and noncommercial alike. The drive in Philadelphia emphasizes the other, more recently available avenue—wireless. The quality of WiFi and the widespread adoption of wireless techniques have moved other municipalities to adopt wireless or mixed-fiber wireless strategies. Municipalities are

— 1
— 0
— 1

proposing to use publicly owned facilities to place wireless points of access around the town, covering the area in a cloud of connectivity and providing open Internet access from anywhere in the city. Philadelphia's initiative has received the widest public attention, although other, smaller cities are closer to having a wireless cloud over the city already.

The incumbent broadband providers have not taken kindly to the municipal assault on their monopoly (or oligopoly) profits. When the city of Abilene, Texas, tried to offer municipal broadband service in the late-1990s, Southwestern Bell (SBC) persuaded the Texas legislature to pass a law that prohibited local governments from providing high-speed Internet access. The town appealed to the FCC and the Federal Court of Appeals in Washington, D.C. Both bodies held that when Congress passed the 1996 Telecommunications Act, and said that, "no state . . . regulation . . . may prohibit . . . the ability of any entity to provide . . . telecommunications service," municipalities were not included in the term "any entity." As the D.C. Circuit put it, "any" might have some significance "depending on the speaker's tone of voice," but here it did not really mean "*any* entity," only some. And states could certainly regulate the actions of municipalities, which are treated in U.S. law as merely their subdivisions or organs.¹³ Bristol, Virginia, had to fight off similar efforts to prohibit its plans through state law before it was able to roll out its network. In early 2004, the U.S. Supreme Court was presented with the practice of state preemption of municipal broadband efforts and chose to leave the municipalities to fend for themselves. A coalition of Missouri municipalities challenged a Missouri law that, like the Texas law, prohibited them from stepping in to offer their citizens broadband service. The Court of the Appeals for the Eighth Circuit agreed with the municipalities. The 1996 Act, after all, was intended precisely to allow anyone to compete with the incumbents. The section that prohibited states from regulating the ability of "any entity" to enter the telecommunications service market precisely anticipated that the local incumbents would use their clout in state legislatures to thwart the federal policy of introducing competition into the local loop. Here, the incumbents were doing just that, but the Supreme Court reversed the Eighth Circuit decision. Without dwelling too much on the wisdom of allowing citizens of municipalities to decide for themselves whether they want a municipal system, the court issued an opinion that was technically defensible in terms of statutory interpretation, but effectively invited the incumbent broadband providers to put their lobbying efforts into persuading state legislators to prohibit municipal efforts.¹⁴ After

— 1
— 0
— 1

Philadelphia rolled out its wireless plan, it was not long before the Pennsylvania legislature passed a similar law prohibiting municipalities from offering broadband. While Philadelphia's plan itself was grandfathered, future expansion from a series of wireless "hot spots" in open area to a genuine municipal network will likely be challenged under the new state law. Other municipalities in Pennsylvania are entirely foreclosed from pursuing this option. In this domain, at least as of 2005, the incumbents seem to have had some substantial success in containing the emergence of municipal broadband networks as a significant approach to eliminating the bottleneck in local network infrastructure.

Devices

The second major component of the physical layer of the networked environment is comprised of the devices people use to compute and communicate. Personal computers, handhelds, game consoles, and to a lesser extent, but lurking in the background, televisions, are the primary relevant devices. In the United States, personal computers are the overwhelmingly dominant mode of connectivity. In Europe and Japan, mobile handheld devices occupy a much larger space. Game consoles are beginning to provide an alternative computationally intensive device, and Web-TV has been a background idea for a while. The increasing digitization of both over-the-air and cable broadcast makes digital TV a background presence, if not an immediate alternative avenue, to Internet communications. None of these devices are constructed by a commons—in the way that open wireless networks, free software, or peer-produced content can be. Personal computers, however, are built on open architecture, using highly standardized commodity components and open interfaces in an enormously competitive market. As a practical matter, therefore, PCs provide an open-platform device. Handhelds, game consoles, and digital televisions, on the other hand, use more or less proprietary architectures and interfaces and are produced in a less-competitive market—not because there is no competition among the manufacturers, but because the distribution chain, through the service providers, is relatively controlled. The result is that configurations and features can more readily be customized for personal computers. New uses can be developed and implemented in the hardware without permission from any owner of a manufacturing or distribution outlet. As handhelds grow in their capabilities, and personal computers collapse in size, the two modes of communicating are bumping into each other's turf. At the moment, there is no obvious regulatory push to

___ 1
 ___ 0
 ___ 1

nudge one or the other out. Observing the evolution of these markets therefore has less to do with policy. As we look at these markets, however, it is important to recognize that the outcome of this competition is not normatively neutral. The capabilities made possible by personal computers underlie much of the social and economic activity described throughout this book. Proprietary handhelds, and even more so, game consoles and televisions, are, presently at least, platforms that choreograph their use. They structure their users' capabilities according to design requirements set by their producers and distributors. A physical layer usable with general-purpose computers is one that is pliable and open for any number of uses by individuals, in a way that a physical layer used through more narrowly scripted devices is not.

The major regulatory threat to the openness of personal computers comes from efforts to regulate the use of copyrighted materials. This question is explored in greater depth in the context of discussing the logical layer. Here, I only note that peer-to-peer networks, and what Fisher has called "promiscuous copying" on the Internet, have created a perceived threat to the very existence of the major players in the industrial cultural production system—Hollywood and the recording industry. These industries are enormously adept at driving the regulation of their business environment—the laws of copyright, in particular. As the threat of copying and sharing of their content by users increased, these industries have maintained a steady pressure on Congress, the courts, and the executive to ratchet up the degree to which their rights are enforced. As we will see in looking at the logical and content layers, these efforts have been successful in changing the law and pushing for more aggressive enforcement. They have not, however, succeeded in suppressing widespread copying. Copying continues, if not entirely unabated, certainly at a rate that was impossible a mere six years ago.

One major dimension of the effort to stop copying has been a drive to regulate the design of personal computers. Pioneered by Senator Fritz Hollings in mid-2001, a number of bills were drafted and lobbied for: the first was the Security Systems Standards and Certification Act; the second, Consumer Broadband and Digital Television Promotion Act (CBDTPA), was actually introduced in the Senate in 2002.¹⁵ The basic structure of these proposed statutes was that they required manufacturers to design their computers to be "trusted systems." The term "trusted," however, had a very odd meaning. The point is that the system, or computer, can be trusted to perform in certain predictable ways, irrespective of what its owner wishes.

— 1
— 0
— 1

The impulse is trivial to explain. If you believe that most users are using their personal computers to copy films and music illegally, then you can think of these users as untrustworthy. In order to be able to distribute films and music in the digital environment that is trustworthy, one must disable the users from behaving as they would choose to. The result is a range of efforts at producing what has derisively been called “the Fritz chip”: legal mandates that systems be designed so that personal computers cannot run programs that are not certified properly to the chip. The most successful of these campaigns was Hollywood’s achievement in persuading the FCC to require manufacturers of all devices capable of receiving digital television signals from the television set to comply with a particular “trusted system” standard. This “broadcast flag” regulation was odd in two distinct ways. First, the rule-making documents show quite clearly that this was a rule driven by Hollywood, not by the broadcasters. This is unusual because the industries that usually play a central role in these rule makings are those regulated by the FCC, such as broadcasters and cable systems. Second, the FCC was not, in fact, regulating the industries that it normally has jurisdiction to regulate. Instead, the rule applied to any device that could use digital television signals *after* they had already been received in the home. In other words, they were regulating practically every computer and digital-video-capable consumer electronics device imaginable. The Court of Appeals ultimately indeed struck down the regulation as wildly beyond the agency’s jurisdiction, but the broadcast flag nonetheless is the closest that the industrial information economy incumbents have come to achieving regulatory control over the design of computers.

The efforts to regulate hardware to fit the distribution model of Hollywood and the recording industry pose a significant danger to the networked information environment. The core design principle of general-purpose computers is that they are open for varied uses over time, as their owners change their priorities and preferences. It is this general-purpose character that has allowed personal computers to take on such varied roles since their adoption in the 1980s. The purpose of the Fritz chip-style laws is to make computing devices less flexible. It is to define a range of socially, culturally, and economically acceptable uses of the machines that are predicted by the legislature and the industry actors, and to implement factory-defined capabilities that are not flexible, and do not give end users the freedom to change the intended use over time and to adapt to changing social and economic conditions and opportunities.

___ 1
___ 0
___ 1

The political economy of this regulatory effort, and similar drives that have been more successful in the logical and content layers, is uncharacteristic of American politics. Personal computers, software, and telecommunications services are significantly larger industries than Hollywood and the recording industry. Verizon alone has roughly similar annual revenues to the entire U.S. movie industry. Each one of the industries that the content industries have tried to regulate has revenues several times greater than do the movie and music industries combined. The relative successes of Hollywood and the recording industry in regulating the logical and content layers, and the viability of their efforts to pass a Fritz chip law, attest to the remarkable cultural power of these industries and to their lobbying prowess. The reason is likely historical. The software and hardware industries in particular have developed mostly outside of the regulatory arena; only around 2002 did they begin to understand that what goes on in Washington could really hurt them. The telecommunications carriers, which are some of the oldest hands at the regulatory game, have had some success in preventing regulations that would force them to police their users and limit Internet use. However, the bulk of their lobbying efforts have been aimed elsewhere. The institutions of higher education, which have found themselves under attack for not policing their students' use of peer-to-peer networks, have been entirely ineffective at presenting their cultural and economic value and the importance of open Internet access to higher education, as compared to the hypothetical losses of Hollywood and the recording industry. Despite the past successes of these entertainment-industry incumbents, two elements suggest that physical device regulation of the CBDPTA form will not follow the same successful path of similar legislation at the logical layer, the DMCA of 1998. The first element is the fact that, unlike in 1998, the technology industries have now realized that Hollywood is seeking to severely constrain their design space. Industries with half a trillion dollars a year in revenues tend to have significant pull in American and international lawmaking bodies, even against industries, like movies and sound recording, that have high cultural visibility but no more than seventy-five billion dollars a year in revenues. The second is that in 1998, there were very few public advocacy organizations operating in the space of intellectual property and trying to play watchdog and to speak for the interests of users. By 2004, a number of organizations dedicated to users' rights in the digital environment emerged to make that conflict clear. The combination of well-defined business interests with increasing representation of user interests creates a political land-

— 1
— 0
— 1

scape in which it will be difficult to pass sweeping laws to limit the flexibility of personal computers. The most recent iteration of the Fritz chip agenda, the Inducing Infringement of Copyrights Act of 2004 was indeed defeated, for the time being, by a coalition of high-technology firms and people who would have formerly been seen as left-of-center media activists.

Regulation of device design remains at the frontier of the battles over the institutional ecology of the digital environment. It is precisely ubiquitous access to basic, general-purpose computers, as opposed to glorified televisions or telephone handsets, that lies at the very heart of the networked information economy. And it is therefore precisely ubiquitous access to such basic machines that is a precondition to the improvements in freedom and justice that we can see emerging in the digital environment.

THE LOGICAL LAYER

At the logical layer, most of the efforts aimed to secure a proprietary model and a more tightly controlled institutional ecology follow a similar pattern to the efforts to regulate device design. They come from the needs of the content-layer businesses—Hollywood and the recording industry, in particular. Unlike the physical transmission layer, which is historically rooted in a proprietary but regulated organizational form, most of the logical layer of the Internet has its roots in open, nonproprietary protocols and standards. The broad term “logical layer” combines a wide range of quite different functionalities. The most basic logical components—the basic protocols and standards for Internet connectivity—have from the beginning of the Internet been open, unowned, and used in common by all Internet users and applications. They were developed by computer scientists funded primarily with public money. The basic Internet Protocol (IP) and Transmission Control Protocol (TCP) are open for all to use. Most of the basic standards for communicating were developed in the IETF, a loosely defined standards-setting body that works almost entirely on a meritocratic basis—a body that Michael Froomkin once suggested is the closest earthly approximation of Habermas’s ideal speech situation. Individual computer engineers contributed irrespective of formal status or organizational affiliation, and the organization ran on the principle that Dave Clark termed “rough consensus and running code.” The World Wide Web protocols and authoring conventions HTTP and HTML were created, and over the course of their lives, shepherded by Tim Berners Lee, who has chosen to dedicate his efforts to making

— 1
— 0
— 1

the Web a public good rather than cashing in on his innovation. The sheer technical necessity of these basic protocols and the cultural stature of their achievement within the engineering community have given these open processes and their commonslike institutional structure a strong gravitational pull on the design of other components of the logical layer, at least insofar as it relates to the communication side of the Internet.

This basic open model has been in constant tension with the proprietary models that have come to use and focus on the Internet in the past decade. By the mid-1990s, the development of graphical-user interfaces to the Web drove Internet use out of universities and into homes. Commercial actors began to look for ways to capture the commercial value of the human potential of the World Wide Web and the Internet, while Hollywood and the recording industry saw the threat of one giant worldwide copying machine looming large. At the same time, the Clinton administration's search of "third-way" liberal agenda manifested in these areas as a commitment to "let the private sector lead" in deployment of the Internet, and an "intellectual property" policy based on extreme protectionism for the exclusive-rights-dependent industries aimed, in the metaphors of that time, to get cars on the information superhighway or help the Internet become a celestial jukebox. The result was a series of moves designed to make the institutional ecology of the Internet more conducive to the proprietary model.

The Digital Millennium Copyright Act of 1998

No piece of legislation more clearly represents the battle over the institutional ecology of the digital environment than the pompously named Digital Millennium Copyright Act of 1998 (DMCA). The DMCA was the culmination of more than three years of lobbying and varied efforts, both domestically in the United States and internationally, over the passage of two WIPO treaties in 1996. The basic worldview behind it, expressed in a 1995 white paper issued by the Clinton administration, was that in order for the National Information Infrastructure (NII) to take off, it had to have "content," and that its great promise was that it could deliver the equivalent of thousands of channels of entertainment. This would only happen, however, if the NII was made safe for delivery of digital content without making it easily copied and distributed without authorization and without payment. The two core recommendations of that early road map were focused on regulating technology and organizational responsibility. First, law was to reg-

___ 1
___ 0
___ 1

ulate the development of technologies that might defeat any encryption or other mechanisms that the owners of copyrighted materials would use to prevent use of their works. Second, Internet service providers were to be held accountable for infringements made by their users, so that they would have an incentive to police their systems. Early efforts to pass this agenda in legislation were resisted, primarily by the large telecommunications service providers. The Baby Bells—U.S. regional telephone companies that were created from the breakup of AT&T (Ma Bell) in 1984, when the telecommunications company was split up in order to introduce a more competitive structure to the telecom industry—also played a role in partly defeating implementation of this agenda in the negotiations toward new WIPO treaties in 1996, treaties that ultimately included a much-muted version of the white paper agenda. Nonetheless, the following year saw significant lobbying for “implementing legislation” to bring U.S. law in line with the requirements of the new WIPO treaties. This new posture placed the emphasis of congressional debates on national industrial policy and the importance of strong protection to the export activities of the U.S. content industries. It was enough to tip the balance in favor of passage of the DMCA. The Internet service provider liability portions bore the marks of a hard-fought battle. The core concerns of the telecommunications companies were addressed by creating an explicit exemption for pure carriage of traffic. Furthermore, providers of more sophisticated services, like Web hosting, were provided immunity from liability for simple failure to police their system actively. In exchange, however, service providers were required to respond to requests by copyright owners by immediately removing materials that the copyright owners deemed infringing. This was the provision under which Diebold forced Swarthmore to remove the embarrassing e-mail records from the students’ Web sites. The other, more basic, element of the DMCA was the anticircumvention regime it put in place. Pamela Samuelson has described the anticircumvention provisions of the DMCA as the result of a battle between Hollywood and Silicon Valley. At the time, unlike the telecommunications giants who were born of and made within the regulatory environment, Silicon Valley did not quite understand that what happened in Washington, D.C., could affect its business. The Act was therefore an almost unqualified victory for Hollywood, moderated only by a long list of weak exemptions for various parties that bothered to show up and lobby against it.

The central feature of the DMCA, a long and convoluted piece of legis-

— 1
— 0
— 1

lation, is its anticircumvention and antidevice provisions. These provisions made it illegal to use, develop, or sell technologies that had certain properties. Copyright owners believed that it would be possible to build strong encryption into media products distributed on the Internet. If they did so successfully, the copyright owners could charge for digital distribution and users would not be able to make unauthorized copies of the works. If this outcome was achieved, the content industries could simply keep their traditional business model—selling movies or music as discrete packages—at lower cost, and with a more refined ability to extract the value users got from using their materials. The DMCA was intended to make this possible by outlawing technologies that would allow users to get around, or circumvent, the protection measures that the owners of copyrighted materials put in place. At first blush, this proposition sounds entirely reasonable. If you think of the content of a music file as a home, and of the copy protection mechanism as its lock, then all the DMCA does is prohibit the making and distributing of burglary tools. This is indeed how the legislation was presented by its supporters. From this perspective, even the relatively draconian consequences spelled out in the DMCA's criminal penalties seem defensible.

There are two distinct problems with this way of presenting what the DMCA does. First, copyrights are far from coextensive with real property. There are many uses of existing works that are permissible to all. They are treated in copyright law like walking on the sidewalk or in a public park is treated in property law, not like walking across the land of a neighbor. This is true, most obviously, for older works whose copyright has expired. This is true for certain kinds of uses of a work, like quoting it for purposes of criticism or parody. Encryption and other copy-protection techniques are not limited by the definition of legal rights. They can be used to protect all kinds of digital files—whether their contents are still covered by copyright or not, and whether the uses that users wish to make of them are privileged or not. Circumvention techniques, similarly, can be used to circumvent copy-protection mechanisms for purposes both legitimate and illegitimate. A barbed wire cutter, to borrow Boyle's metaphor, could be a burglary tool if the barbed wire is placed at the property line. However, it could equally be a tool for exercising your privilege if the private barbed wire has been drawn around public lands or across a sidewalk or highway. The DMCA prohibited all wire cutters, even though there were many uses of these technologies that could be used for legal purposes. Imagine a ten-year-old girl doing her homework on the history of the Holocaust. She includes in her multimedia paper

___ 1
 ___ 0
 ___ 1

a clip from Steven Spielberg's film, *Schindler's List*, in which a little girl in red, the only color image on an otherwise black-and-white screen, walks through the pandemonium of a deportation. In her project, the child painstakingly superimposes her own face over that of the girl in the film for the entire sequence, frame by frame. She calls the paper, "My Grandmother." There is little question that most copyright lawyers (not retained by the owner of the movie) would say that this use would count as a "fair use," and would be privileged under the Copyright Act. There is also little question that if *Schindler's List* was only available in encrypted digital form, a company would have violated the DMCA if it distributed a product that enabled the girl to get around the encryption in order to use the snippet she needed, and which by traditional copyright law she was permitted to use. It is in the face of this concern about overreaching by those who employ technological protection measures that Julie Cohen argued for the "right to hack"—to circumvent code that impedes one's exercise of one's privileged uses.

The second problem with the DMCA is that its definitions are broad and malleable. Simple acts like writing an academic paper on how the encryption works, or publishing a report on the Web that tells users where they can find information about how to circumvent a copy-protection mechanism could be included in the definition of providing a circumvention device. Edward Felten is a computer scientist at Princeton. As he was preparing to publish an academic paper on encryption, he received a threatening letter from the Recording Industry Association of America (RIAA), telling him that publication of the paper constituted a violation of the DMCA. The music industry had spent substantial sums on developing encryption for digital music distribution. In order to test the system before it actually entrusted music with this wrapper, the industry issued a public challenge, inviting cryptographers to try to break the code. Felten succeeded in doing so, but did not continue to test his solutions because the industry required that, in order to continue testing, he sign a nondisclosure agreement. Felten is an academic, not a businessperson. He works to make knowledge public, not to keep it secret. He refused to sign the nondisclosure agreement, and prepared to publish his initial findings, which he had made without entering any nondisclosure agreement. As he did so, he received the RIAA's threatening letter. In response, he asked a federal district court to declare that publication of his findings was not a violation of the DMCA. The RIAA, realizing that trying to silence academic publication of a criticism of the

___ 1
___ 0
___ 1

weakness of its approach to encryption was not the best litigation stance, moved to dismiss the case by promising it would never bring suit.¹⁶

Another case did not end so well for the defendant. It involved a suit by the eight Hollywood studios against a hacker magazine, *2600*. The studios sought an injunction prohibiting *2600* from making available a program called DeCSS, which circumvents the copy-protection scheme used to control access to DVDs, named CSS. CSS prevents copying or any use of DVDs unauthorized by the vendor. DeCSS was written by a fifteen-year-old Norwegian named Jon Johanson, who claimed (though the district court discounted his claim) to have written it as part of an effort to create a DVD player for GNU/Linux-based machines. A copy of DeCSS, together with a story about it was posted on the *2600* site. The industry obtained an injunction against *2600*, prohibiting not only the posting of DeCSS, but also its linking to other sites that post the program—that is, telling users where they can get the program, rather than actually distributing a circumvention program. That decision may or may not have been correct on the merits. There are strong arguments in favor of the proposition that making DVDs compatible with GNU/Linux systems is a fair use. There are strong arguments that the DMCA goes much farther than it needs to in restricting speech of software programmers and Web authors, and so is invalid under the First Amendment. The court rejected these arguments.

The point here is not, however, to revisit the legal correctness of that decision, but to illustrate the effects of the DMCA as an element in the institutional ecology of the logical layer. The DMCA is intended as a strong legal barrier to certain technological paths of innovation at the logical layer of the digital environment. It is intended specifically to preserve the “thing-” or “goods”-like nature of entertainment products—music and movies, in particular. As such, it is intended to, and does to some extent, shape the technological development toward treating information and culture as finished goods, rather than as the outputs of social and communications processes that blur the production-consumption distinction. It makes it more difficult for individuals and nonmarket actors to gain access to digital materials that the technology, the market, and the social practices, left unregulated, would have made readily available. It makes practices of cutting and pasting, changing and annotating existing cultural materials harder to do than the technology would have made possible. I have argued elsewhere that when Congress self-consciously makes it harder for individuals to use what-

— 1
— 0
— 1

they please, in the interest of some public goal (in this case, preservation of Hollywood and the recording industry for the public good), it must justify its acts under the First Amendment. However, the important question is not one of U.S. constitutional law.

The more general claim, true for any country that decides to enforce a DMCA-like law, is that prohibiting technologies that allow individuals to make flexible and creative uses of digital cultural materials burdens the development of the networked information economy and society. It burdens individual autonomy, the emergence of the networked public sphere and critical culture, and some of the paths available for global human development that the networked information economy makes possible. All these losses will be incurred in expectation of improvements in creativity, even though it is not at all clear that doing so would actually improve, even on a simple utilitarian calculus, the creative production of any given country or region. Passing a DMCA-type law will not by itself squelch the development of nonmarket and peer production. Indeed, many of these technological and social-economic developments emerged and have flourished after the DMCA was already in place. It does, however, represent a choice to tilt the institutional ecology in favor of industrial production and distribution of cultural packaged goods, at the expense of commons-based relations of sharing information, knowledge, and culture. Twentieth-century cultural materials provide the most immediate and important source of references and images for contemporary cultural creation. Given the relatively recent provenance of movies, recorded music, and photography, much of contemporary culture was created in these media. These basic materials for the creation of contemporary multimedia culture are, in turn, encoded in formats that cannot simply be copied by hand, as texts might be even in the teeth of technical protection measures. The capacity to copy mechanically is a necessary precondition for the capacity to quote and combine existing materials of these kinds into new cultural statements and conversational moves. Preserving the capacity of industrial cultural producers to maintain a hermetic seal on the use of materials to which they own copyright can be bought only at the cost of disabling the newly emerging modes of cultural production from quoting and directly building upon much of the culture of the last century.

The Battle over Peer-to-Peer Networks

The second major institutional battle over the technical and social trajectory of Internet development has revolved around peer-to-peer (p2p) networks. I

___ 1
___ 0
___ 1

offer a detailed description of it here, but not because I think it will be the make-it-or-break-it of the networked information economy. If any laws have that determinative a power, they are the Fritz chip and DMCA. However, the peer-to-peer legal battle offers an excellent case study of just how difficult it is to evaluate the effects of institutional ecology on technology, economic organization, and social practice.

Peer-to-peer technologies as a global phenomenon emerged from Napster and its use by tens of millions of users around the globe for unauthorized sharing of music files. In the six years since their introduction, p2p networks have developed robust and impressive technical capabilities. They have been adopted by more than one hundred million users, and are increasingly applied to uses well beyond music sharing. These developments have occurred despite a systematic and aggressive campaign of litigation and criminal enforcement in a number of national systems against both developers and users. Technically, p2p networks are algorithms that run on top of the Internet and allow users to connect directly from one end user's machine to another. In theory, that is how the whole Internet works—or at least how it worked when there were a small number of computers attached to it. In practice, most users connect through an Internet service provider, and most content available for access on the Internet was available on a server owned and operated by someone distinct from its users. In the late 1990s, there were rudimentary utilities that allowed one user to access information stored on the computer of another, but no widely used utility allowed large numbers of individuals to search each other's hard drives and share data directly from one user to another. Around 1998–1999, early Internet music distribution models, like MP3.com, therefore provided a centralized distribution point for music. This made them highly vulnerable to legal attack. Shawn Fanning, then eighteen years old, was apparently looking for ways to do what teenagers always do—share their music with friends—in a way that would not involve a central point of storing and copying. He developed Napster—the first major, widely adopted p2p technology. Unlike MP3.com, users of Napster could connect their computers directly—one person could download a song stored on the computer of another without mediation. All that the Napster site itself did, in addition to providing the end-user software, was to provide a centralized directory of which songs resided on which machine. There is little disagreement in the literature that it is an infringement under U.S. copyright law for any given user to allow others to duplicate copyrighted music from his or her computer to theirs. The centralizing role of Napster

— 1
— 0
— 1

in facilitating these exchanges, alongside a number of ill-considered statements by some of its principals, were enough to render the company liable for contributory copyright infringement.

The genie of p2p technology and the social practice of sharing music, however, were already out of the bottle. The story of the following few years, to the extent that one can tell a history of the present and the recent past, offers two core insights. First, it shows how institutional design can be a battleground over the conditions of cultural production in the digital environment. Second, it exposes the limits of the extent to which the institutional ecology can determine the ultimate structure of behavior at a moment of significant and rapid technological and social perturbation. Napster's judicial closure provided no real respite for the recording industry. As Napster was winding down, Gnutella, a free software alternative, had already begun to replace it. Gnutella did not depend on any centralized component, not even to facilitate search. This meant that there was no central provider. There was no firm against which to bring action. Even if there were, it would be impossible to "shut down" use of the program. Gnutella was a freestanding program that individual users could install. Once installed, its users could connect to anyone else who had installed the program, without passing through any choke point. There was no central server to shut down. Gnutella had some technical imperfections, but these were soon overcome by other implementations of p2p. The most successful improvement over Gnutella was the FastTrack architecture, now used by Kazaa, Grokster, and other applications, including some free software applications. It improves on the search capabilities of Gnutella by designating some users as "supernodes," which store information about what songs are available in their "neighborhood." This avoids Gnutella's primary weakness, the relatively high degree of network overhead traffic. The supernodes operate on an ad hoc basis. They change based on whose computer is available with enough storage and bandwidth. They too, therefore, provide no litigation target. Other technologies have developed to speed up or make more robust the distribution of files, including BitTorrent, eDonkey and its free-software relative eMule, and many others. Within less than two years of Napster's closure, more people were using these various platforms to share files than Napster had users at its height. Some of these new firms found themselves again under legal assault—both in the United States and abroad.

As the technologies grew and developed, and as the legal attacks increased, the basic problem presented by the litigation against technology manufac-

— 1
— 0
— 1

turers became evident. Peer-to-peer techniques can be used for a wide range of uses, only some of which are illegal. At the simplest level, they can be used to distribute music that is released by an increasing number of bands freely. These bands hope to get exposure that they can parley into concert performances. As recorded music from the 1950s begins to fall into the public domain in Europe and Australia, golden oldies become another legitimate reason to use p2p technologies. More important, p2p systems are being adapted to different kinds of uses. Chapter 7 discusses how FreeNet is being used to disseminate subversive documents, using the persistence and robustness of p2p networks to evade detection and suppression by authoritarian regimes. BitTorrent was initially developed to deal with the large file transfers required for free software distributions. BitTorrent and eDonkey were both used by the Swarthmore students when their college shut down their Internet connection in response to Diebold's letter threatening action under the service provider liability provisions of the DMCA. The founders of KaZaa have begun to offer an Internet telephony utility, Skype, which allows users to make phone calls from one computer to another for free, and from their computer to the telephone network for a small fee. Skype is a p2p technology.

In other words, p2p is developing as a general approach toward producing distributed data storage and retrieval systems, just as open wireless networks and distributed computing are emerging to take advantage of personal devices to produce distributed communications and computation systems, respectively. As the social and technological uses of p2p technologies grow and diversify, the legal assault on all p2p developers becomes less sustainable—both as a legal matter and as a social-technical matter. KaZaa was sued in the Netherlands, and moved to Australia. It was later subject to actions in Australia, but by that time, the Dutch courts found the company not to be liable to the music labels. Grokster, a firm based in the United States, was initially found to have offered a sufficiently diverse set of capabilities, beyond merely facilitating copyright infringements, that the Court of Appeals for the Ninth Circuit refused to find it liable simply for making and distributing its software. The Supreme Court reversed that holding, however, returning the case to the lower courts to find, factually, whether Grokster had actual intent to facilitate illegal copying.¹⁷ Even if Grokster ultimately loses, the FastTrack network architecture will not disappear; clients (that is, end user software) will continue to exist, including free software clients. Perhaps it will be harder to raise money for businesses located within the United States

— 1
— 0
— 1

to operate in this technological space, because the new rule announced by the Supreme Court in *Grokster* raises the risk of litigation for innovators in the p2p space. However, as with encryption regulation in the mid-1990s, it is not clear that the United States can unilaterally prevent the development of technology for which there is worldwide demand and with regard to whose development there is globally accessible talent.

How important more generally are these legal battles to the organization of cultural production in the networked environment? There are two components to the answer: The first component considers the likely effect of the legal battles on the development and adoption of the technology and the social practice of promiscuous copying. In this domain, law seems unlikely to prevent the continued development of p2p technologies. It has, however, had two opposite results. First, it has affected the path of the technological evolution in a way that is contrary to the industry interests but consistent with increasing distribution of the core functions of the logical layer. Second, it seems to have dampened somewhat the social practice of file sharing. The second component assumes that a range of p2p technologies will continue to be widely adopted, and that some significant amount of sharing will continue to be practiced. The question then becomes what effect this will have on the primary cultural industries that have fought this technology—movies and recorded music. Within this new context, music will likely change more radically than movies, and the primary effect will be on the accreditation function—how music is recognized and adopted by fans. Film, if it is substantially affected, will likely be affected largely by a shift in tastes.

MP3.com was the first major music distribution site shut down by litigation. From the industry's perspective, it should have represented an entirely unthreatening business model. Users paid a subscription fee, in exchange for which they were allowed to download music. There were various quirks and kinks in this model that made it unattractive to the music industry at the time: the industry did not control this major site, and therefore had to share the rents from the music, and more important, there was no effective control over the music files once downloaded. However, from the perspective of 2005, MP3.com was a vastly more manageable technology for the sound recording business model than a free software file-sharing client. MP3.com was a single site, with a corporate owner that could be (and was) held responsible. It controlled which user had access to what files—by requiring each user to insert a CD into the computer to prove that he or she had bought the CD—so that usage could in principle be monitored and, if

___ 1
___ 0
___ 1

desired, compensation could be tied to usage. It did not fundamentally change the social practice of choosing music. It provided something that was more like a music-on-demand jukebox than a point of music sharing. As a legal matter, MP3.com's infringement was centered on the fact that it stored and delivered the music from this central server instead of from the licensed individual copies. In response to the shutdown of MP3.com, Napster redesigned the role of the centralized mode, and left storage in the hands of users, keeping only the directory and search functions centralized. When Napster was shut down, Gnutella and later FastTrack further decentralized the system, offering a fully decentralized, ad hoc reconfigurable cataloging and search function. Because these algorithms represent architecture and a protocol-based network, not a particular program, they are usable in many different implementations. This includes free software programs like MLDonkey—which is a nascent file-sharing system that is aimed to run simultaneously across most of the popular file-sharing networks, including FastTrack, BitTorrent, and Overnet, the eDonkey network. These programs are now written by, and available from, many different jurisdictions. There is no central point of control over their distribution. There is no central point through which to measure and charge for their use. They are, from a technical perspective, much more resilient to litigation attack, and much less friendly to various possible models of charging for downloads or usage. From a technological perspective, then, the litigation backfired. It created a network that is less susceptible to integration into an industrial model of music distribution based on royalty payments per user or use.

It is harder to gauge, however, whether the litigation was a success or a failure from a social-practice point of view. There have been conflicting reports on the effects of file sharing and the litigation on CD sales. The recording industry claimed that CD sales were down because of file sharing, but more independent academic studies suggested that CD sales were not independently affected by file sharing, as opposed to the general economic downturn.¹⁸ The Pew project on Internet and American Life user survey data suggests that the litigation strategy against individual users has dampened the use of file sharing, though file sharing is still substantially more common among users than paying for files from the newly emerging pay-per-download authorized services. In mid-2003, the Pew study found that 29 percent of Internet users surveyed said they had downloaded music files, identical to the percentage of users who had downloaded music in the first quarter of 2001, the heyday of Napster. Twenty-one percent responded that

— 1
— 0
— 1

they allow others to download from their computer.¹⁹ This meant that somewhere between twenty-six and thirty-five million adults in the United States alone were sharing music files in mid-2003, when the recording industry began to sue individual users. Of these, fully two-thirds expressly stated that they did not care whether the files they downloaded were or were not copyrighted. By the end of 2003, five months after the industry began to sue individuals, the number of respondents who admitted to downloading music dropped by half. During the next few months, these numbers increased slightly to twenty-three million adults, remaining below the mid-2003 numbers in absolute terms and more so in terms of percentage of Internet users. Of those who had at one point downloaded, but had stopped, roughly a third said that the threat of suit was the reason they had stopped file sharing.²⁰ During this same period, use of pay online music download services, like iTunes, rose to about 7 percent of Internet users. Sharing of all kinds of media files—music, movies, and games—was at 23 percent of adult Internet users. These numbers do indeed suggest that, in the aggregate, music downloading is reported somewhat less often than it was in the past. It is hard to tell how much of this reduction is due to actual behavioral change as compared to an unwillingness to self-report on behavior that could subject one to litigation. It is impossible to tell how much of an effect the litigation has had specifically on sharing by younger people—teenagers and college students—who make up a large portion of both CD buyers and file sharers. Nonetheless, the reduction in the total number of self-reported users and the relatively steady percentage of total Internet users who share files of various kinds suggest that the litigation does seem to have had a moderating effect on file sharing as a social practice. It has not, however, prevented file sharing from continuing to be a major behavioral pattern among one-fifth to one-quarter of Internet users, and likely a much higher proportion in the most relevant populations from the perspective of the music and movie industries—teenagers and young adults.

From the perspective of understanding the effects of institutional ecology, then, the still-raging battle over peer-to-peer networks presents an ambiguous picture. One can speculate with some degree of confidence that, had Napster not been stopped by litigation, file sharing would have been a much wider social practice than it is today. The application was extremely easy to use; it offered a single network for all file-sharing users, thereby offering an extremely diverse and universal content distribution network; and for a brief period, it was a cultural icon and a seemingly acceptable social practice. The

— 1
— 0
— 1

period of regrouping that followed its closure; the imperfect interfaces of early Gnutella clients; the relative fragmentation of file sharing into a number of networks, each with a smaller coverage of content than was present; and the fear of personal litigation risk are likely to have limited adoption. On the other hand, in the longer run, the technological developments have created platforms that are less compatible with the industrial model, and which would be harder to integrate into a stable settlement for music distribution in the digital environment.

Prediction aside, it is not immediately obvious why peer-to-peer networks contribute to the kinds of nonmarket production and creativity that I have focused on as the core of the networked information economy. At first blush, they seem simply to be mechanisms for fans to get industrially produced recorded music without paying musicians. This has little to do with democratization of creativity. To see why p2p networks nonetheless are a part of the development of a more attractive cultural production system, and how they can therefore affect the industrial organization of cultural production, we can look first at music, and then, independently, at movies. The industrial structure of each is different, and the likely effects of p2p networks are different in each case.

Recorded music began with the phonograph—a packaged good intended primarily for home consumption. The industry that grew around the ability to stamp and distribute records divided the revenue structure such that artists have been paid primarily from live public performances and merchandizing. Very few musicians, including successful recording artists, make money from recording royalties. The recording industry takes almost all of the revenues from record and CD sales, and provides primarily promotion and distribution. It does not bear the capital cost of the initial musical creation; artists do. With the declining cost of computation, that cost has become relatively low, often simply a computer owned by artists themselves, much as they own their instruments. Because of this industrial structure, peer-to-peer networks are a genuine threat to displacing the entire recording industry, while leaving musicians, if not entirely unaffected, relatively insulated from the change and perhaps mildly better off. Just as the recording industry stamps CDs, promotes them on radio stations, and places them on distribution chain shelves, p2p networks produce the physical and informational aspects of a music distribution system. However, p2p networks do so collaboratively, by sharing the capacity of their computers, hard drives, and network connections. Filtering and accreditation, or “promotion,” are produced on the

— 1
— 0
— 1

model that Eben Moglen called “anarchist distribution.” Jane’s friends and friends of her friends are more likely to know exactly what music would make her happy than are recording executives trying to predict which song to place, on which station and which shelf, to expose her to exactly the music she is most likely to buy in a context where she would buy it. File-sharing systems produce distribution and “promotion” of music in a social-sharing modality. Alongside peer-produced music reviews, they could entirely supplant the role of the recording industry.

Musicians and songwriters seem to be relatively insulated from the effects of p2p networks, and on balance, are probably affected positively. The most comprehensive survey data available, from mid-2004, shows that 35 percent of musicians and songwriters said that free downloads have helped their careers. Only 5 percent said it has hurt them. Thirty percent said it increased attendance at concerts, 21 percent that it helped them sell CDs and other merchandise, and 19 percent that it helped them gain radio playing time. These results are consistent with what one would expect given the revenue structure of the industry, although the study did not separate answers out based on whether the respondent was able to live entirely or primarily on their music, which represented only 16 percent of the respondents to the survey. In all, it appears that much of the actual flow of revenue to artists—from performances and other sources—is stable. This is likely to remain true even if the CD market were entirely displaced by peer-to-peer distribution. Musicians will still be able to play for their dinner, at least not significantly less so than they can today. Perhaps there will be fewer millionaires. Perhaps fewer mediocre musicians with attractive physiques will be sold as “geniuses,” and more talented musicians will be heard than otherwise would have, and will as a result be able to get paying gigs instead of waiting tables or “getting a job.” But it would be silly to think that music, a cultural form without which no human society has existed, will cease to be in our world if we abandon the industrial form it took for the blink of a historical eye that was the twentieth century. Music was not born with the phonograph, nor will it die with the peer-to-peer network. The terms of the debate, then, are about cultural policy; perhaps about industrial policy. Will we get the kind of music we want in this system, whoever “we” are? Will American recording companies continue to get the export revenue streams they do? Will artists be able to live from making music? Some of these arguments are serious. Some are but a tempest in a monopoly-rent teapot. It is clear that a technological change has rendered obsolete a particular mode of distributing

— 1
— 0
— 1

information and culture. Distribution, once the sole domain of market-based firms, now can be produced by decentralized networks of users, sharing instantiations of music they deem attractive with others, using equipment they own and generic network connections. This distribution network, in turn, allows a much more diverse range of musicians to reach much more finely grained audiences than were optimal for industrial production and distribution of mechanical instantiations of music in vinyl or CD formats. The legal battles reflect an effort by an incumbent industry to preserve its very lucrative business model. The industry has, to this point, delayed the transition to peer-based distribution, but it is unclear for how long or to what extent it will be successful in preventing the gradual transition to user-based distribution.

The movie industry has a different industrial structure and likely a different trajectory in its relations to p2p networks. First and foremost, movies began as a relatively high capital cost experience good. Making a movie, as opposed to writing a song, was something that required a studio and a large workforce. It could not be done by a musician with a guitar or a piano. Furthermore, movies were, throughout most of their history, collective experience goods. They were a medium for public performance experienced outside of the home, in a social context. With the introduction of television, it was easy to adapt movie revenue structure by delaying release of films to television viewing until after demand for the movie at the theater declined, as well as to develop their capabilities into a new line of business—television production. However, theatrical release continued to be the major source of revenue. When video came along, the movie industry cried murder in the Sony Betamax case, but actually found it quite easy to work videocassettes into yet another release window, like television, and another medium, the made-for-video movie. Digital distribution affects the distribution of cultural artifacts as packaged goods for home consumption. It does not affect the social experience of going out to the movies. At most, it could affect the consumption of the twenty-year-old mode of movie distribution: videos and DVDs. As recently as the year 2000, when the Hollywood studios were litigating the DeCSS case, they represented to the court that home video sales were roughly 40 percent of revenue, a number consistent with other reports.²¹ The remainder, composed of theatrical release revenues and various television releases, remains reasonably unthreatened as a set of modes of revenue capture to sustain the high-production value, high-cost movies that typify Hollywood. Forty percent is undoubtedly a large chunk, but unlike

___ 1
 ___ 0
 ___ 1

the recording industry, which began with individually owned recordings, the movie industry preexisted videocassettes and DVDs, and is likely to outlive them even if p2p networks were to eliminate that market entirely, which is doubtful.

The harder and more interesting question is whether cheap high-quality digital video-capture and editing technologies combined with p2p networks for efficient distribution could make film a more diverse medium than it is now. The potential hypothetical promise of p2p networks like BitTorrent is that they could offer very robust and efficient distribution networks for films outside the mainstream industry. Unlike garage bands and small-scale music productions, however, this promise is as yet speculative. We do not invest in public education for film creation, as we do in the teaching of writing. Most of the raw materials out of which a culture of digital capture and amateur editing could develop are themselves under copyright, a subject we return to when considering the content layer. There are some early efforts, like atomfilms.com, at short movie distribution. The technological capabilities are there. It is possible that if films older than thirty or even fifty years were released into the public domain, they would form the raw material out of which a new cultural production practice would form. If it did, p2p networks would likely play an important role in their distribution. However, for now, although the sound recording and movie industries stand shoulder to shoulder in the lobbying efforts, their circumstances and likely trajectory in relation to file sharing are likely quite different.

The battles over p2p and the DMCA offer some insight into the potential, but also the limits, of tweaking the institutional ecology. The ambition of the industrial cultural producers in both cases was significant. They sought to deploy law to shape emerging technologies and social practices to make sure that the business model they had adopted for the technologies of film and sound recording continued to work in the digital environment. Doing so effectively would require substantial elimination of certain lines of innovation, like certain kinds of decryption and p2p networks. It would require outlawing behavior widely adopted by people around the world—social sharing of most things that they can easily share—which, in the case of music, has been adopted by tens of millions of people around the world. The belief that all this could be changed in a globally interconnected network through the use of law was perhaps naïve. Nonetheless, the legal efforts have had some impact on social practices and on the ready availability of materials

— 1
— 0
— 1

for free use. The DMCA may not have made any single copyright protection mechanism hold up to the scrutiny of hackers and crackers around the Internet. However, it has prevented circumvention devices from being integrated into mainstream platforms, like the Windows operating system or some of the main antivirus programs, which would have been “natural” places for them to appear in consumer markets. The p2p litigation did not eliminate the p2p networks, but it does seem to have successfully dampened the social practice of file sharing. One can take quite different views of these effects from a policy perspective. However, it is clear that they are self-conscious efforts to tweak the institutional ecology of the digital environment in order to dampen the most direct threats it poses for the twentieth-century industrial model of cultural production. In the case of the DMCA, this is done at the direct cost of making it substantially harder for users to make creative use of the existing stock of audiovisual materials from the twentieth century—materials that are absolutely central to our cultural self-understanding at the beginning of the twenty-first century. In the case of p2p networks, the cost to nonmarket production is more indirect, and may vary across different cultural forms. The most important long-term effect of the pressure that this litigation has put on technology to develop decentralized search and retrieval systems may, ultimately and ironically, be to improve the efficiency of radically decentralized cultural production and distribution, and make decentralized production more, rather than less, robust to the vicissitudes of institutional ecology.

The Domain Name System: From Public Trust to the Fetishism of Mnemonics

Not all battles over the role of property-like arrangements at the logical layer originate from Hollywood and the recording industry. One of the major battles outside of the ambit of the copyright industries concerned the allocation and ownership of domain names. At stake was the degree to which brand name ownership in the material world could be leveraged into attention on the Internet. Domain names are alphanumeric mnemonics used to represent actual Internet addresses of computers connected to the network. While 130.132.51.8 is hard for human beings to remember, www.yale.edu is easier. The two strings have identical meaning to any computer connected to the Internet—they refer to a server that responds to World Wide Web queries for Yale University’s main site. Every computer connected to the Internet has a unique address, either permanent or assigned by a provider

— 1
— 0
— 1

for the session. That requires that someone distribute addresses—both numeric and mnemonic. Until 1992, names and numbers were assigned on a purely first-come, first-served basis by Jon Postel, one of the very first developers of the Internet, under U.S. government contract. Postel also ran a computer, called the root server, to which all computers would turn to ask the numeric address of letters.mnemonic.edu, so they could translate what the human operator remembered as the address into one their machine could use. Postel called this system “the Internet Assigned Numbers Authority, IANA,” whose motto he set as, “Dedicated to preserving the central coordinating functions of the global Internet for the public good.” In 1992, Postel got tired of this coordinating job, and the government contracted it to a private firm called Network Solutions, Inc., or NSI. As the number of applications grew, and as the administration sought to make this system pay for itself, NSI was allowed in 1995 to begin to charge fees for assigning names and numbers. At about the same time, widespread adoption of a graphical browser made using the World Wide Web radically simpler and more intuitive to the uninitiated. These two developments brought together two forces to bear on the domain name issue—each with a very different origin and intent. The first force consisted of the engineers who had created and developed the Internet, led by Postel, who saw the domain name space to be a public trust and resisted its commercialization by NSI. The second force consisted of trademark owners and their lawyers, who suddenly realized the potential for using control over domain names to extend the value of their brand names to a new domain of trade—e-commerce. These two forces placed the U.S. government under pressure to do two things: (1) release the monopoly that NSI—a for-profit corporation—had on the domain name space, and (2) find an efficient means of allowing trademark owners to control the use of alphanumeric strings used in their trademarks as domain names. Postel initially tried to “take back the root” by asking various regional domain name servers to point to his computer, instead of to the one maintained by NSI in Virginia. This caused uproar in the government, and Postel was accused of attacking and hijacking the Internet! His stature and passion, however, placed significant weight on the side of keeping the naming system as an open public trust. That position came to an abrupt end with his death in 1996. By late 1996, a self-appointed International Ad Hoc Committee (IAHC) was formed, with the blessing of the Internet Society (ISOC), a professional membership society for individuals and organizations involved in Internet planning. IAHC’s membership was about half intellectual prop-

— 1
— 0
— 1

erty lawyers and half engineers. In February 1997, IAHC came out with a document called the gTLD-MoU (generic top-level domain name memorandum of understanding). Although the product of a small group, the gTLD-MoU claimed to speak for “The Internet Community.” Although it involved no governments, it was deposited “for signature” with the International Telecommunications Union (ITU). Dutifully, some 226 organizations—Internet services companies, telecommunications providers, consulting firms, and a few chapters of the ISOC signed on. Section 2 of the gTLD-MoU, announcing its principles, reveals the driving forces of the project. While it begins with the announcement that the top-level domain space “is a public resource and is subject to the public trust,” it quickly commits to the principle that “the current and future Internet name space stakeholders can benefit most from a self-regulatory and market-oriented approach to Internet domain name registration services.” This results in two policy principles: (1) commercial competition in domain name registration by releasing the monopoly NSI had, and (2) protecting trademarks in the alphanumeric strings that make up the second-level domain names. The final, internationalizing component of the effort—represented by the interests of the WIPO and ITU bureaucracies—was attained by creating a Council of Registrars as a Swiss corporation, and creating special relationships with the ITU and the WIPO.

None of this institutional edifice could be built without the U.S. government. In early 1998, the administration responded to this ferment with a green paper, seeking the creation of a private, nonprofit corporation registered in the United States to take on management of the domain name issue. By its own terms, the green paper responded to concerns of the domain name registration monopoly and of trademark issues in domain names, first and foremost, and to some extent to increasing clamor from abroad for a voice in Internet governance. Despite a cool response from the European Union, the U.S. government proceeded to finalize a white paper and authorize the creation of its preferred model—the private, nonprofit corporation. Thus was born the Internet Corporation for Assigned Names and Numbers (ICANN) as a private, nonprofit California corporation. Over time, it succeeded in large measure in loosening NSI’s monopoly on domain name registration. Its efforts on the trademark side effectively created a global preemptive property right. Following an invitation in the U.S. government’s white paper for ICANN to study the proper approach to trademark enforcement in the domain name space, ICANN and WIPO initiated a process

— 1
— 0
— 1

that began in July 1998 and ended in April 1999. As Froomkin describes his experience as a public-interest expert in this process, the process feigned transparency and open discourse, but was in actuality an opaque staff-driven drafting effort.²² The result was a very strong global property right available to trademark owners in the alphanumeric strings that make up domain names. This was supported by binding arbitration. Because it controlled the root server, ICANN could enforce its arbitration decisions worldwide. If ICANN decides that, say, the McDonald's fast-food corporation and not a hypothetical farmer named Old McDonald owned www.mcdonalds.com, all computers in the world would be referred to the corporate site, not the personal one. Not entirely satisfied with the degree to which the ICANN-WIPO process protected their trademarks, some of the major trademark owners lobbied the U.S. Congress to pass an even stricter law. This law would make it easier for the owners of commercial brand names to obtain domain names that include their brand, whether or not there was any probability that users would actually confuse sites like the hypothetical Old McDonald's with that of the fast-food chain.

The degree to which the increased appropriation of the domain name space is important is a function of the extent to which the cultural practice of using human memory to find information will continue to be widespread. The underlying assumption of the value of trademarked alphanumeric strings as second-level domain names is that users will approach electronic commerce by typing in "www.brandname.com" as their standard way of relating to information on the Net. This is far from obviously the most efficient solution. In physical space, where collecting comparative information on price, quality, and so on is very costly, brand names serve an important informational role. In cyberspace, where software can compare prices, and product-review services that link to vendors are easy to set up and cheap to implement, the brand name becomes an encumbrance on good information, not its facilitator. If users are limited, for instance, to hunting around as to whether information they seek is on www.brandname.com, www.brand_name.com, or www.brand.net, name recognition from the real world becomes a bottleneck to e-commerce. And this is precisely the reason why owners of established marks sought to assure early adoption of trademarks in domain names—it assures users that they can, in fact, find their accustomed products on the Web without having to go through search algorithms that might expose them to comparison with pesky start-up competitors. As search engines become better and more tightly integrated into the basic

— 1
— 0
— 1

browser functionality, the idea that a user who wants to buy from Delta Airlines would simply type “www.delta.com,” as opposed to plugging “delta airlines” into an integrated search toolbar and getting the airline as a first hit becomes quaint. However, quaint inefficient cultural practices can persist. And if this indeed is one that will persist, then the contours of the property right matter. As the law has developed over the past few years, ownership of a trademark that includes a certain alphanumeric string almost always gives the owner of the trademark a preemptive right in using the letters and numbers incorporated in that mark as a domain name.

Domain name disputes have fallen into three main categories. There are cases of simple arbitrage. Individuals who predicted that having a domain name with the brand name in it would be valuable, registered such domain names aplenty, and waited for the flat-footed brand name owners to pay them to hand over the domain. There is nothing more inefficient about this form of arbitrage than any other. The arbitrageurs “reserved” commercially valuable names so they could be auctioned, rather than taken up by someone who might have a non-negotiable interest in the name—for example, someone whose personal name it was. These arbitrageurs were nonetheless branded pirates and hijackers, and the consistent result of all the cases on domain names has been that the corporate owners of brand names receive the domain names associated with their brands without having to pay the arbitrageurs. Indeed, the arbitrageurs were subject to damage judgments. A second kind of case involved bona fide holders of domain names that made sense for them, but were nonetheless shared with a famous brand name. One child nicknamed “Pokey” registered “pokey.org,” and his battle to keep that name against a toy manufacturer that sold a toy called “pokey” became a poster child for this type of case. Results have been more mixed in this case, depending on how sympathetic the early registrant was. The third type of case—and in many senses, most important from the perspective of freedom to participate not merely as a consumer in the networked environment, but as a producer—involves those who use brand names to draw attention to the fact that they are attacking the owner of the brand. One well-known example occurred when Verizon Wireless was launched. The same hacker magazine involved in the DeCSS case, *2600*, purchased the domain name “verizonreallysucks.com” to poke fun at Verizon. In response to a letter requiring that they give up the domain name, the magazine purchased the domain name “VerizonShouldSpendMoreTimeFixingItsNetworkAndLessMoneyOnLawyers.com.” These types of cases have again met with varying

— 1
 — 0
 — 1

degrees of sympathy from courts and arbitrators under the ICANN process, although it is fairly obvious that using a brand name in order to mock and criticize its owner and the cultural meaning it tries to attach to its mark is at the very core of fair use, cultural criticism, and free expression.

The point here is not to argue for one type of answer or another in terms of trademark law, constitutional law, or the logic of ICANN. It is to identify points of pressure where the drive to create proprietary rights is creating points of control over the flow of information and the freedom to make meaning in the networked environment. The domain name issue was seen by many as momentous when it was new. ICANN has drawn a variety of both yearnings and fears as a potential source of democratic governance for the Internet or a platform for U.S. hegemony. I suspect that neither of these will turn out to be true. The importance of property rights in domain names is directly based on the search practices of users. Search engines, directories, review sites, and referrals through links play a large role in enabling users to find information they are interested in. Control over the domain name space is unlikely to provide a real bottleneck that will prevent both commercial competitors and individual speakers from drawing attention to their competition or criticism. However, the battle is indicative of the efforts to use proprietary rights in a particular element of the institutional ecology of the logical layer—trademarks in domain names—to tilt the environment in favor of the owners of famous brand names, and against individuals, noncommercial actors, and smaller, less-known competitors.

The Browser Wars

A much more fundamental battle over the logical layer has occurred in the browser wars. Here, the “institutional” component is not formal institutions, like laws or regulations, but technical practice institutions—the standards for Web site design. Unlike on the network protocol side, the device side of the logical layer—the software running personal computers—was thoroughly property-based by the mid-1990s. Microsoft’s dominance in desktop operating systems was well established, and there was strong presence of other software publishers in consumer applications, pulling the logical layer toward a proprietary model. In 1995, Microsoft came to perceive the Internet and particularly the World Wide Web as a threat to its control over the desktop. The user-side Web browser threatened to make the desktop a more open environment that would undermine its monopoly. Since that time, the two pulls—the openness of the nonproprietary network and the closed nature

— 1
— 0
— 1

of the desktop—have engaged in a fairly energetic tug-of-war over the digital environment. This push-me-pull-you game is played out both in the domain of market share, where Microsoft has been immensely successful, and in the domain of standard setting, where it has been only moderately successful. In market share, the story is well known and has been well documented in the Microsoft antitrust litigation. Part of the reason that it is so hard for a new operating system to compete with Microsoft's is that application developers write first, and sometimes only, for the already-dominant operating system. A firm investing millions of dollars in developing a new piece of photo-editing software will usually choose to write it so that it works with the operating system that has two hundred million users, not the one that has only fifteen million users. Microsoft feared that Netscape's browser, dominant in the mid-1990s, would come to be a universal translator among applications—that developers could write their applications to run on the browser, and the browser would handle translation across different operating systems. If that were to happen, Microsoft's operating system would have to compete on intrinsic quality. Windows would lose the boost of the felicitous feedback effect, where more users mean more applications, and this greater number of applications in turn draws more new users, and so forth. To prevent this eventuality, Microsoft engaged in a series of practices, ultimately found to have violated the antitrust laws, aimed at getting a dominant majority of Internet users to adopt Microsoft's Internet Explorer (IE). Illegal or not, these practices succeeded in making IE the dominant browser, overtaking the original market leader, Netscape, within a short number of years. By the time the antitrust case was completed, Netscape had turned browser development over to the open-source development community, but under licensing conditions sufficiently vague so that the project generated little early engagement. Only around 2001–2002, did the Mozilla browser development project get sufficient independence and security for developers to begin to contribute energetically. It was only in late 2004, early 2005, that Mozilla Firefox became the first major release of a free software browser that showed promise of capturing some user-share back from IE.

Microsoft's dominance over the operating system and browser has not, as a practical matter, resulted in tight control over the information flow and use on the Internet. This is so for three reasons. First, the TCP/IP protocol is more fundamental to Internet communications. It allows any application or content to run across the network, as long as it knows how to translate itself into very simple packets with standard addressing information. To pre-

— 1
— 0
— 1

vent applications from doing this over basic TCP/IP would make the Microsoft operating system substantially crippling to many applications developers, which brings us to the second reason. Microsoft's dominance depends to a great extent on the vastly greater library of applications available to run on Windows. To make this library possible, Microsoft makes available a wide range of application program interfaces that developers can use without seeking Microsoft's permission. As a strategic decision about what enhances its core dominance, Microsoft may tilt the application development arena in its favor, but not enough to make it too hard for most applications to be implemented on a Windows platform. While not nearly as open as a genuinely open-source platform, Windows is also a far cry from a completely controlled platform, whose owner seeks to control all applications that are permitted to be developed for, and all uses that can be made of, its platform. Third, while IE controls much of the browser market share, Microsoft has not succeeded in dominating the standards for Web authoring. Web browser standard setting happens on the turf of the mythic creator of the Web—Tim Berners Lee. Lee chairs the W3C, a nonprofit organization that sets the standard ways in which Web pages are authored so that they have a predictable appearance on the browser's screen. Microsoft has, over the years, introduced various proprietary extensions that are not part of the Web standard, and has persuaded many Web authors to optimize their Web sites to IE. If it succeeds, it will have wrested practical control over standard setting from the W3C. However, as of this writing, Web pages generally continue to be authored using mostly standard, open extensions, and anyone browsing the Internet with a free software browser, like any of the Mozilla family, will be able to read and interact with most Web sites, including the major e-commerce sites, without encountering nonstandard interfaces optimized for IE. At a minimum, these sites are able to query the browser as to whether or not it is IE, and serve it with either the open standard or the proprietary standard version accordingly.

Free Software

The role of Mozilla in the browser wars points to the much more substantial and general role of the free software movement and the open-source development community as major sources of openness, and as a backstop against appropriation of the logical layer. In some of the most fundamental uses of the Internet—Web-server software, Web-scripting software, and e-mail servers—free or open-source software has a dominant user share. In others, like

___ 1
 ___ 0
 ___ 1

the operating system, it offers a robust alternative sufficiently significant to prevent enclosure of an entire component of the logical layer. Because of its licensing structure and the fact that the technical specifications are open for inspection and use by anyone, free software offers the most completely open, commons-based institutional and organizational arrangement for any resource or capability in the digital environment. Any resource in the logical layer that is the product of a free software development project is institutionally designed to be available for nonmarket, nonproprietary strategies of use. The same openness, however, makes free software resistant to control. If one tries to implement a constraining implementation of a certain function—for example, an audio driver that will not allow music to be played without proper authorization from a copyright holder—the openness of the code for inspection will allow users to identify what, and how, the software is constraining. The same institutional framework will allow any developer to “fix” the problem and change the way the software behaves. This is how free and open-source software is developed to begin with. One cannot limit access to the software—for purposes of inspection and modification—to developers whose behavior can be controlled by contract or property and still have the software be “open source” or free. As long as free software can provide a fully implemented alternative to the computing functionalities users want, perfect enclosure of the logical layer is impossible. This openness is a boon for those who wish the network to develop in response to a wide range of motivations and practices. However, it presents a serious problem for anyone who seeks to constrain the range of uses made of the Internet. And, just as they did in the context of trusted systems, the incumbent industrial culture producers—Hollywood and the recording industry—would, in fact, like to control how the Internet is used and how software behaves.

Software Patents

Throughout most of its history, software has been protected primarily by copyright, if at all. Beginning in the early 1980s, and culminating formally in the late 1990s, the Federal Circuit, the appellate court that oversees the U.S. patent law, made clear that software was patentable. The result has been that software has increasingly become the subject of patent rights. There is now pressure for the European Union to pass a similar reform, and to internationalize the patentability of software more generally. There are a variety of policy questions surrounding the advisability of software patents. Software

___ 1
 ___ 0
 ___ 1

development is a highly incremental process. This means that patents tend to impose a burden on a substantial amount of future innovation, and to reward innovation steps whose qualitative improvement over past contributions may be too small to justify the discontinuity represented by a patent grant. Moreover, innovation in the software business has flourished without patents, and there is no obvious reason to implement a new exclusive right in a market that seems to have been enormously innovative without it. Most important, software components interact with each other constantly. Sometimes interoperating with a certain program may be absolutely necessary to perform a function, not because the software is so good, but because it has become the standard. The patent then may extend to the very functionality, whereas a copyright would have extended only to the particular code by which it was achieved. The primary fear is that patents over standards could become major bottlenecks.

From the perspective of the battle over the institutional ecology, free software and open-source development stand to lose the most from software patents. A patent holder may charge a firm that develops dependent software in order to capture rents. However, there is no obvious party to charge for free software development. Even if the patent owner has a very open licensing policy—say, licensing the patent nonexclusively to anyone without discrimination for \$10,000—most free software developers will not be able to play. IBM and Red Hat may pay for licenses, but the individual contributor hacking away at his or her computer, will not be able to. The basic driver of free software innovation is easy ubiquitous access to the state of the art, coupled with diverse motivations and talents brought to bear on a particular design problem. If working on a problem requires a patent license, and if any new development must not only write new source code, but also avoid replicating a broad scope patent or else pay a large fee, then the conditions for free software development are thoroughly undermined. Free software is responsible for some of the most basic and widely used innovations and utilities on the Internet today. Software more generally is heavily populated by service firms that do not functionally rely on exclusive rights, copyrights, or patents. Neither free software nor service-based software development need patents, and both, particularly free and open-source software, stand to be stifled significantly by widespread software patenting. As seen in the case of the browser war, in the case of Gnutella, and the much more widely used basic utilities of the Web—Apache server software, a number of free e-mail servers, and the Perl scripting language—free and open-

— 1
— 0
— 1

source software developers provide central chunks of the logical layer. They do so in a way that leaves that layer open for anyone to use and build upon. The drive to increase the degree of exclusivity available for software by adopting patents over and above copyright threatens the continued vitality of this development methodology. In particular, it threatens to take certain discrete application areas that may require access to patented standard elements or protocols out of the domain of what can be done by free software. As such, it poses a significant threat to the availability of an open logical layer for at least some forms of network use.

THE CONTENT LAYER

The last set of resources necessary for information production and exchange is the universe of existing information, knowledge, and culture. The battle over the scope, breadth, extent, and enforcement of copyright, patent, trademarks, and a variety of exotic rights like trespass to chattels or the right to link has been the subject of a large legal literature. Instead of covering the entire range of enclosure efforts of the past decade or more, I offer a set of brief descriptions of the choices being made in this domain. The intention is not to criticize or judge the intrinsic logic of any of these legal changes, but merely to illustrate how all these toggles of institutional ecology are being set in favor of proprietary strategies, at the expense of nonproprietary producers.

Copyright

The first domain in which we have seen a systematic preference for commercial producers that rely on property over commons-based producers is in copyright. This preference arises from a combination of expansive interpretations of what rights include, a niggardly interpretive attitude toward users' privileges, especially fair use, and increased criminalization. These have made copyright law significantly more industrial-production friendly than it was in the past or than it need be from the perspective of optimizing creativity or welfare in the networked information economy, rather than rent-extraction by incumbents.

Right to Read. Jessica Litman early diagnosed an emerging new "right to read."²³ The basic right of copyright, to control copying, was never seen to include the right to control who reads an existing copy, when, and how

— 1
— 0
— 1

many times. Once a user bought a copy, he or she could read it many times, lend it to a friend, or leave it on the park bench or in the library for anyone else to read. This provided a coarse valve to limit the deadweight loss associated with appropriating a public good like information. As a happenstance of computer technology, reading on a screen involves making a temporary copy of a file onto the temporary memory of the computer. An early decision of the Ninth Circuit Court of Appeals, *MAI Systems*, treated RAM (random-access memory) copies of this sort as “copies” for purposes of copyright.²⁴ This position, while weakly defended, was not later challenged or rejected by other courts. Its result is that every act of reading on a screen involves “making a copy” within the meaning of the Copyright Act. As a practical matter, this interpretation expands the formal rights of copyright holders to cover any and all computer-mediated uses of their works, because no use can be made with a computer without at least formally implicating the right to copy. More important than the formal legal right, however, this universal baseline claim to a right to control even simple reading of one’s copyrighted work marked a change in attitude. Justified later through various claims—such as the efficiency of private ordering or of price discrimination—it came to stand for a fairly broad proposition: Owners should have the right to control all valuable uses of their works. Combined with the possibility and existence of technical controls on actual use and the DMCA’s prohibition on circumventing those controls, this means that copyright law has shifted. It existed throughout most of its history as a regulatory provision that reserved certain uses of works for exclusive control by authors, but left other, not explicitly constrained uses free. It has now become a law that gives rights holders the exclusive right to control any computer-mediated use of their works, and captures in its regulatory scope all uses that were excluded from control in prior media.

Fair Use Narrowed. Fair use in copyright was always a judicially created concept with a large degree of uncertainty in its application. This uncertainty, coupled with a broader interpretation of what counts as a commercial use, a restrictive judicial view of what counts as fair, and increased criminalization have narrowed its practical scope.

First, it is important to recognize that the theoretical availability of the fair-use doctrine does not, as a practical matter, help most productions. This is due to a combination of two factors: (1) fair-use doctrine is highly fact specific and uncertain in application, and (2) the Copyright Act provides

— 1
— 0
— 1

large fixed statutory damages, even if there is no actual damage to the copyright owner. Lessig demonstrated this effect most clearly by working through an example of a documentary film.²⁵ A film will not be distributed without liability insurance. Insurance, in turn, will not be issued without formal clearance, or permission, from the owner of each copyrighted work, any portion of which is included in the film, even if the amount used is trivially small and insignificant to the documentary. A five-second snippet of a television program that happened to play on a television set in the background of a sequence captured in documentary film can therefore prevent distribution of the film, unless the filmmaker can persuade the owner of that program to grant rights to use the materials. Copyright owners in such television programs may demand thousands of dollars for even such a minimal and incidental use of “their” images. This is not because a court would ultimately find that using the image as is, with the tiny fraction of the television program in the background, was not covered by fair use. It probably would be a fair use. It is because insurance companies and distributors would refuse to incur the risk of litigation.

Second, in the past few years, even this uncertain scope has been constricted by expanding the definitions of what counts as interference with a market and what counts as a commercial use. Consider the *Free Republic* case. In that case, a political Web site offered a forum for users to post stories from various newspapers as grist for a political discussion of their contents or their slant. The court held that because newspapers may one day sell access to archived articles, and because some users may read some articles on the Web forum instead of searching and retrieving them from the newspapers’ archive, the use interfered with a potential market. Moreover, because Free Republic received donations from users (although it did not require them) and exchanged advertising arrangements with other political sites, the court treated the site as a “commercial user,” and its use of newspaper articles to facilitate political discussion of them “a commercial use.” These factors enabled the court to hold that posting an article from a medium—daily newspapers—whose existence does not depend on copyright, in a way that may one day come to have an effect on uncertain future revenues, which in any case would be marginal to the business model of the newspapers, was not a fair use even when done for purposes of political commentary.

Criminalization. Copyright enforcement has also been substantially criminalized in the past few years. Beginning with the No Electronic Theft Act

— 1
— 0
— 1

(NET Act) in 1997 and later incorporated into the DMCA, criminal copyright has recently become much more expansive than it was until a few years ago. Prior to passage of the NET Act, only commercial pirates—those that slavishly made thousands of copies of video or audiocassettes and sold them for profit—would have qualified as criminal violators of copyright. Criminal liability has now been expanded to cover private copying and free sharing of copyrighted materials whose cumulative nominal price (irrespective of actual displaced demand) is quite low. As criminal copyright law is currently written, many of the tens of millions using p2p networks are felons. It is one thing when the recording industry labels tens of millions of individuals in a society “pirates” in a rhetorical effort to conform social norms to its members’ business model. It is quite another when the state brands them felons and fines or imprisons them. Litman has offered the most plausible explanation of this phenomenon.²⁶ As the network makes low-cost production and exchange of information and culture easier, the large-scale commercial producers are faced with a new source of competition—volunteers, people who provide information and culture for free. As the universe of people who can threaten the industry has grown to encompass more or less the entire universe of potential customers, the plausibility of using civil actions to force individuals to buy rather than share information goods decreases. Suing all of one’s intended customers is not a sustainable business model. In the interest of maintaining the business model that relies on control over information goods and their sale as products, the copyright industry has instead enlisted criminal enforcement by the state to prevent the emergence of such a system of free exchange. These changes in formal law have, in what is perhaps a more important development, been coupled with changes in the Justice Department’s enforcement policy, leading to a substantial increase in the shadow of criminal enforcement in this area.²⁷

Term Extension. The change in copyright law that received the most widespread public attention was the extension of copyright term in the Sonny Bono Copyright Term Extension Act of 1998. The statute became cause celebre in the early 2000s because it was the basis of a major public campaign and constitutional challenge in the case of *Eldred v. Ashcroft*.²⁸ The actual marginal burden of this statute on use of existing materials could be seen as relatively small. The length of copyright protection was already very long—seventy-five years for corporate-owned materials, life of the author plus fifty

— 1
— 0
— 1

Term Extension Act increased these two numbers to ninety-five and life plus seventy, respectively. The major implication, however, was that the Act showed that retroactive extension was always available. As materials that were still valuable in the stocks of Disney, in particular, came close to the public domain, their lives would be extended indefinitely. The legal challenge to the statute brought to public light the fact that, as a practical matter, almost the entire stock of twentieth-century culture and beyond would stay privately owned, and its copyright would be renewed indefinitely. For video and sound recordings, this meant that almost the entire universe of materials would never become part of the public domain; would never be available for free use as inputs into nonproprietary production. The U.S. Supreme Court upheld the retroactive extension. The inordinately long term of protection in the United States, initially passed under the pretext of “harmonizing” the length of protection in the United States and in Europe, is now being used as an excuse to “harmonize” the length of protection for various kinds of materials—like sound recordings—that actually have shorter terms of protection in Europe or other countries, like Australia. At stake in all these battles is the question of when, if ever, will Errol Flynn’s or Mickey Mouse’s movies, or Elvis’s music, become part of the public domain? When will these be available for individual users on the same terms that Shakespeare or Mozart are available? The implication of *Eldred* is that they may never join the public domain, unless the politics of term-extension legislation change.

No de Minimis Digital Sampling. A narrower, but revealing change is the recent elimination of digital sampling from the universe of *ex ante* permissible actions, even when all that is taken is a tiny snippet. The case is recent and has not been generalized by other courts as of this writing. However, it offers insight into the mind-set of judges who are confronted with digital opportunities, and who in good faith continue to see the stakes as involving purely the organization of a commercial industry, rather than defining the comparative scope of commercial industry and nonmarket commons-based creativity. Courts seem blind to the effects of their decisions on the institutional ecology within which nonproprietary, individual, and social creation must live. In *Bridgeport Music, Inc.*, the Sixth Circuit was presented with the following problem: The defendant had created a rap song.²⁹ In making it, he had digitally copied a two-second guitar riff from a digital recording of a 1970s song, and then looped and inserted it in various places to create a completely different musical effect than the original. The district court

— 1
— 0
— 1

had decided that the amount borrowed was so small as to make the borrowing de minimis—too little for the law to be concerned with. The Court of Appeals, however, decided that it would be too burdensome for courts to have to decide, on a case-by-case basis, how much was too little for law to be concerned with. Moreover, it would create too much uncertainty for recording companies; it is, as the court put it, “cheaper to license than to litigate.”³⁰ The court therefore held that any digital sampling, no matter how trivial, could be the basis of a copyright suit. Such a bright-line rule that makes all direct copying of digital bits, no matter how small, an infringement, makes digital sound recordings legally unavailable for noncommercial, individually creative mixing. There are now computer programs, like Garage Band, that allow individual users to cut and mix existing materials to create their own music. These may not result in great musical compositions. But they may. That, in any event, is not their point. They allow users to have a very different relationship to recorded music than merely passively listening to finished, unalterable musical pieces. By imagining that the only parties affected by copyright coverage of sampling are recording artists who have contracts with recording studios and seek to sell CDs, and can therefore afford to pay licensing fees for every two-second riff they borrow, the court effectively outlawed an entire model of user creativity. Given how easy it is to cut, paste, loop, slow down, and speed up short snippets, and how creatively exhilarating it is for users—young and old—to tinker with creating musical compositions with instruments they do not know how to play, it is likely that the opinion has rendered illegal a practice that will continue, at least for the time being. Whether the social practice will ultimately cause the law to change or vice versa is more difficult to predict.

**Contractual Enclosure: Click-Wrap Licenses
and the Uniform Computer Information
Transactions Act (UCITA)**

Practically all academic commentators on copyright law—whether critics or proponents of this provision or that—understand copyright to be a public policy accommodation between the goal of providing incentives to creators and the goal of providing efficiently priced access to both users and downstream creators. Ideally, it takes into consideration the social costs and benefits of one settlement or another, and seeks to implement an optimal trade-off. Beginning in the 1980s, software and other digital goods were sold with “shrink-wrap licenses.” These were licenses to use the software, which pur-

— 1
— 0
— 1

ported to apply to mass-market buyers because the buyer would be deemed to have accepted the contract by opening the packaging of the software. These practices later transmuted online into click-wrap licenses familiar to most anyone who has installed software and had to click “I Agree” once or more before the software would install. Contracts are not bound by the balance struck in public law. Licensors can demand, and licensees can agree to, almost any terms. Among the terms most commonly inserted in such licenses that restrict the rights of users are prohibitions on reverse engineering, and restrictions on the use of raw data in compilations, even though copyright law itself does not recognize rights in data. As Mark Lemley showed, most courts prior to the mid-1990s did not enforce such terms.³¹ Some courts refused to enforce shrink-wrap licenses in mass-market transactions by relying on state contract law, finding an absence of sufficient consent or an unenforceable contract of adhesion. Others relied on federal preemption, stating that to the extent state contract law purported to enforce a contract that prohibited fair use or otherwise protected material in the public domain—like the raw information contained in a report—it was preempted by federal copyright law that chose to leave this material in the public domain, freely usable by all. In 1996, in *ProCD v. Zeidenberg*, the Seventh Circuit held otherwise, arguing that private ordering would be more efficient than a single public determination of what the right balance was.³²

The following few years saw substantial academic debate as to the desirability of contractual opt-outs from the public policy settlement. More important, the five years that followed saw a concerted effort to introduce a new part to the Uniform Commercial Code (UCC)—a model commercial law that, though nonbinding, is almost universally adopted at the state level in the United States, with some modifications. The proposed new UCC Article 2B was to eliminate the state law concerns by formally endorsing the use of standard shrink-wrap licenses. The proposed article generated substantial academic and political heat, ultimately being dropped by the American Law Institute, one of the main sponsors of the UCC. A model law did ultimately pass under the name of the Uniform Computer Information Transactions Act (UCITA), as part of a less universally adopted model law effort. Only two states adopted the law—Virginia and Maryland. A number of other states then passed anti-UCITA laws, which gave their residents a safe harbor from having UCITA applied to their click-wrap transactions.

The reason that *ProCD* and UCITA generated so much debate was the concern that click-wrap licenses were operating in an inefficient market, and

___ 1
 ___ 0
 ___ 1

that they were, as a practical matter, displacing the policy balance represented by copyright law. Mass-market transactions do not represent a genuine negotiated agreement, in the individualized case, as to what the efficient contours of permissions are for the given user and the given information product. They are, rather, generalized judgments by the vendor as to what terms are most attractive for it that the market will bear. Unlike rival economic goods, information goods sold at a positive price in reliance on copyright are, by definition, priced above marginal cost. The information itself is non-rival. Its marginal cost is zero. Any transaction priced above the cost of communication is evidence of some market power in the hands of the provider, used to price based on value and elasticity of demand, not on marginal cost. Moreover, the vast majority of users are unlikely to pay close attention to license details they consider to be boilerplate. This means there is likely significant information shortfall on the part of consumers as to the content of the licenses, and the sensitivity of demand to overreaching contract terms is likely low. This is not because consumers are stupid or slothful, but because the probability that either they would be able to negotiate out from under a standard provision, or a court would enforce against them a truly abusive provision is too low to justify investing in reading and arguing about contracts for all but their largest purchases. In combination, these considerations make it difficult to claim as a general matter that privately set licensing terms would be more efficient than the publicly set background rules of copyright law.³³ The combination of mass-market contracts enforced by technical controls over use of digital materials, which in turn are protected by the DMCA, threatens to displace the statutorily defined public domain with a privately defined realm of permissible use.³⁴ This privately defined settlement would be arrived at in non-negotiated mass-market transactions, in the presence of significant information asymmetries between consumers and vendors, and in the presence of systematic market power of at least some degree.

Trademark Dilution

As discussed in chapter 8, the centrality of commercial interaction to social existence in early-twenty-first-century America means that much of our core iconography is commercial in origin and owned as a trademark. Mickey, Barbie, Playboy, or Coke are important signifiers of meaning in contemporary culture. Using iconography is a central means of creating rich, culturally situated expressions of one's understanding of the world. Yet, as Boyle

— 1
— 0
— 1

has pointed out, now that we treat flag burning as a constitutionally protected expression, trademark law has made commercial icons the sole remaining venerable objects in our law. Trademark law permits the owners of culturally significant images to control their use, to squelch criticism, and to define exclusively the meaning that the symbols they own carry.

Three factors make trademark protection today more of a concern as a source of enclosure than it might have been in the past. First is the introduction of the federal Anti-Dilution Act of 1995. Second is the emergence of the brand as the product, as opposed to a signifier for the product. Third is the substantial reduction in search and other information costs created by the Net. Together, these three factors mean that owned symbols are becoming increasingly important as cultural signifiers, are being enclosed much more extensively than before precisely as cultural signifiers, and with less justification beyond the fact that trademarks, like all exclusive rights, are economically valuable to their owners.

In 1995, Congress passed the first federal Anti-Dilution Act. Though treated as a trademark protection law, and codifying doctrines that arose in trademark common law, antidilution is a fundamentally different economic right than trademark protection. Traditional trademark protection is focused on preventing consumer confusion. It is intended to assure that consumers can cheaply tell the difference between one product and another, and to give producers incentives to create consistent quality products that can be associated with their trademark. Trademark law traditionally reflected these interests. Likelihood of consumer confusion was the sine qua non of trademark infringement. If I wanted to buy a Coca-Cola, I did not want to have to make sure I was not buying a different dark beverage in a red can called Coca-Gola. Infringement actions were mostly limited to suits among competitors in similar relevant markets, where confusion could occur. So, while trademark law restricted how certain symbols could be used, it was so only as among competitors, and only as to the commercial, not cultural, meaning of their trademark. The antidilution law changes the most relevant factors. It is intended to protect famous brand names, irrespective of a likelihood of confusion, from being diluted by use by others. The association between a particular corporation and a symbol is protected for its value to that corporation, irrespective of the use. It no longer regulates solely competitors to the benefit of competition. It prohibits many more possible uses of the symbol than was the case under traditional trademark law. It applies even to noncommercial users where there is no possibility of confusion. The emer-

— 1
— 0
— 1

gence of this antidilution theory of exclusivity is particularly important as brands have become the product itself, rather than a marker for the product. Nike and Calvin Klein are examples: The product sold in these cases is not a better shoe or shirt—the product sold is the brand. And the brand is associated with a cultural and social meaning that is developed purposefully by the owner of the brand so that people will want to buy it. This development explains why dilution has become such a desirable exclusive right for those who own it. It also explains the cost of denying to anyone the right to use the symbol, now a signifier of general social meaning, in ways that do not confuse consumers in the traditional trademark sense, but provide cultural criticism of the message signified.

Ironically, the increase in the power of trademark owners to control uses of their trademark comes at a time when its functional importance as a mechanism for reducing search costs is declining. Traditional trademark's most important justification was that it reduced information collection costs and thereby facilitated welfare-enhancing trade. In the context of the Internet, this function is significantly less important. General search costs are lower. Individual items in commerce can provide vastly greater amounts of information about their contents and quality. Users can use machine processing to search and sift through this information and to compare views and reviews of specific items. Trademark has become less, rather than more, functionally important as a mechanism for dealing with search costs. When we move in the next few years to individual-item digital marking, such as with RFID (radio frequency identification) tags, all the relevant information about contents, origin, and manufacture down to the level of the item, as opposed to the product line, will be readily available to consumers in real space, by scanning any given item, even if it is not otherwise marked at all. In this setting, where the information qualities of trademarks will significantly decline, the antidilution law nonetheless assures that owners can control the increasingly important cultural meaning of trademarks. Trademark, including dilution, is subject to a fair use exception like that of copyright. For the same reasons as operated in copyright, however, the presence of such a doctrine only ameliorates, but does not solve, the limits that a broad exclusive right places on the capacity of nonmarket-oriented creative uses of materials—in this case, culturally meaningful symbols.

— 1
— 0
— 1

Database Protection

In 1991, in *Feist Publications, Inc. v. Rural Tel. Serv. Co.*, the Supreme Court held that raw facts in a compilation, or database, were not covered by the Copyright Act. The constitutional clause that grants Congress the power to create exclusive rights for authors, the Court held, required that works protected were original with the author. The creative element of the compilation—its organization or selectivity, for example, if sufficiently creative—could therefore be protected under copyright law. However, the raw facts compiled could not. Copying data from an existing compilation was therefore not “piracy”; it was not unfair or unjust; it was purposefully privileged in order to advance the goals of the constitutional power to make exclusive grants—the advancement of progress and creative uses of the data.³⁵ A few years later, the European Union passed a Database Directive, which created a discrete and expansive right in raw data compilations.³⁶ The years since the Court decided *Feist* have seen repeated efforts by the larger players in the database publishing industry to pass similar legislation in the United States that would, as a practical matter, overturn *Feist* and create exclusive private rights in the raw data in compilations. “Harmonization” with Europe has been presented as a major argument in favor of this law. Because the *Feist* Court based its decision on limits to the constitutional power to create exclusive rights in raw information, efforts to protect database providers mostly revolved around an unfair competition law, based in the Commerce Clause, rather than on precisely replicating the European right. In fact, however, the primary draft that has repeatedly been introduced walks, talks, and looks like a property right.

Sustained and careful work, most prominently by Jerome Reichman and Paul Uhler, has shown that the proposed database right is unnecessary and detrimental, particularly to scientific research.³⁷ Perhaps no example explains this point better than the “natural experiment” that Boyle has pointed to, and which the United States and Europe have been running over the past decade or so. The United States has formally had no exclusive right in data since 1991. Europe has explicitly had such a right since 1996. One would expect that both the European Union and the United States would look to the comparative effects on the industries in both places when the former decides whether to keep its law, and the latter decides whether to adopt one like it. The evidence is reasonably consistent and persuasive. Following the *Feist* decision, the U.S. database industry continued to grow steadily, without

— 1
— 0
— 1

a blip. The “removal” of the property right in data by *Feist* had no effect on growth. Europe at the time had a much smaller database industry than did the United States, as measured by the number of databases and database companies. Maurer, Hugenholtz, and Onsrud showed that, following the introduction of the European *sui generis* right, each country saw a one-time spike in the number of databases and new database companies, but this was followed within a year or two by a decline to the levels seen before the Directive, which have been fairly stagnant since the early 1990s.³⁸ Another study, more specifically oriented toward the appropriate policy for government-collected data, compared the practices of Europe—where government agencies are required to charge what the market will bear for access to data they collect—and the United States, where the government makes data it collects freely available at the cost of reproduction, as well as for free on the Web. That study found that the secondary uses of data, including commercial- and noncommercial-sector uses—such as, for example, markets in commercial risk management and meteorological services—contributed vastly more to the economy of the United States because of secondary uses of freely accessed government weather data than equivalent market sectors in Europe were able to contribute to their respective economies.³⁹ The evidence suggests, then, that the artificial imposition of rents for proprietary data is suppressing growth in European market-based commercial services and products that rely on access to data, relative to the steady growth in the parallel U.S. markets, where no such right exists. It is trivial to see that a cost structure that suppresses growth among market-based entities that would at least partially benefit from being able to charge more for their outputs would have an even more deleterious effect on nonmarket information production and exchange activities, which are burdened by the higher costs and gain no benefit from the proprietary rights.

There is, then, mounting evidence that rights in raw data are unnecessary to create a basis for a robust database industry. Database manufacturers rely on relational contracts—subscriptions to continuously updated databases—rather than on property-like rights. The evidence suggests that, in fact, exclusive rights are detrimental to various downstream industries that rely on access to data. Despite these fairly robust observations from a decade of experience, there continues to be a threat that such a law will pass in the U.S. Congress. This continued effort to pass such a law underscores two facts. First, much of the legislation in this area reflects rent seeking, rather than reasoned policy. Second, the deeply held belief that “more property-

— 1
— 0
— 1

like rights will lead to more productivity” is hard to shake, even in the teeth of both theoretical analysis and empirical evidence to the contrary.

Linking and Trespass to Chattels:

New Forms of Information Exclusivity

Some litigants have turned to state law remedies to protect their data indirectly, by developing a common-law, trespass-to-server form of action. The primary instance of this trend is *eBay v. Bidder's Edge*, a suit by the leading auction site against an aggregator site. Aggregators collect information about what is being auctioned in multiple locations, and make the information about the items available in one place so that a user can search eBay and other auction sites simultaneously. The eventual bidding itself is done on the site that the item's owner chose to make his or her item available, under the terms required by that site. The court held that the automated information collection process—running a computer program that automatically requests information from the server about what is listed on it, called a spider or a bot—was a “trespass to chattels.”⁴⁰ This ancient form of action, originally intended to apply to actual taking or destruction of goods, mutated into a prohibition on unlicensed automated searching. The injunction led to Bidder's Edge closing its doors before the Ninth Circuit had an opportunity to review the decision. A common-law decision like *eBay v. Bidder's Edge* creates a common-law exclusive private right in information by the back door. In principle, the information itself is still free of property rights. Reading it mechanically—an absolute necessity given the volume of the information and its storage on magnetic media accessible only by mechanical means—can, however, be prohibited as “trespass.” The practical result would be equivalent to some aspects of a federal exclusive private right in raw data, but without the mitigating attributes of any exceptions that would be directly introduced into legislation. It is still too early to tell whether cases such as these ultimately will be considered preempted by federal copyright law,⁴¹ or perhaps would be limited by first amendment law on the model of *New York Times v. Sullivan*.⁴²

Beyond the roundabout exclusivity in raw data, trespass to chattels presents one instance of a broader question that is arising in application of both common-law and statutory provisions. At stake is the legal control over information about information, like linking and other statements people make about the availability and valence of some described information. Linking—the mutual pointing of many documents to each other—is the very

— 1
— 0
— 1

core idea of the World Wide Web. In a variety of cases, parties have attempted to use law to control the linking practices of others. The basic structure of these cases is that A wants to tell users M and N about information presented by B. The meaning of a link is, after all, “here you can read information presented by someone other than me that I deem interesting or relevant to you, my reader.” Someone, usually B, but possibly some other agent C, wants to control what M and N know or do with regard to the information B is presenting. B (or C) then sues A to prevent A from linking to the information on B’s site.

The simplest instance of such a case involved a service that Microsoft offered—sidewalk.com—that provided access to, among other things, information on events in various cities. If a user wanted a ticket to the event, the sidewalk site linked that user directly to a page on ticketmaster.com where the user could buy a ticket. Ticketmaster objected to this practice, preferring instead that sidewalk.com link to its home page, in order to expose the users to all the advertising and services Ticketmaster provided, rather than solely to the specific service sought by the user referred by sidewalk.com. At stake in these linking cases is who will control the context in which certain information is presented. If deep linking is prohibited, Ticketmaster will control the context—the other movies or events available to be seen, their relative prominence, reviews, and so forth. The right to control linking then becomes a right to shape the meaning and relevance of one’s statements for others. If the choice between Ticketmaster and Microsoft as controllers of the context of information may seem of little normative consequence, it is important to recognize that the right to control linking could easily apply to a local library, or church, or a neighbor as they participate in peer-producing relevance and accreditation of the information to which they link.

The general point is this: On the Internet, there are a variety of ways that some people can let others know about information that exists somewhere on the Web. In doing so, these informers loosen someone else’s control over the described information—be it the government, a third party interested in limiting access to the information, or the person offering the information. In a series of instances over the past half decade or more we have seen attempts by people who control certain information to limit the ability of others to challenge that control by providing information about the information. These are not cases in which a person without access to information is seeking affirmative access from the “owner” of information. These are

— 1
— 0
— 1

cases where someone who dislikes what another is saying about particular information is seeking the aid of law to control what other parties can say to each other about that information. Understood in these terms, the restrictive nature of these legal moves in terms of how they burden free speech in general, and impede the freedom of anyone, anywhere, to provide information, relevance, and accreditation, becomes clear. The *eBay v. Bidder's Edge* case suggests one particular additional aspect. While much of the political attention focuses on formal “intellectual property”-style statutes passed by Congress, in the past few years we have seen that state law and common-law doctrine are also being drafted to create areas of exclusivity and boundaries on the free use of information. These efforts are often less well informed, and because they were arrived at ad hoc, often without understanding that they are actually forms of regulating information production and exchange, they include none of the balancing privileges or limitations of rights that are so common in the formal statutory frameworks.

International “Harmonization”

One theme that has repeatedly appeared in the discussion of databases, the DMCA, and term extension, is the way in which “harmonization” and internationalization of exclusive rights are used to ratchet up the degree of exclusivity afforded rights holders. It is trite to point out that the most advanced economies in the world today are information and culture exporters. This is true of both the United States and Europe. Some of the cultural export industries—most notably Hollywood, the recording industry, some segments of the software industry, and pharmaceuticals—have business models that rely on the assertion of exclusive rights in information. Both the United States and the European Union, therefore, have spent the past decade and a half pushing for ever-more aggressive and expansive exclusive rights in international agreements and for harmonization of national laws around the world toward the highest degrees of protection. Chapter 9 discusses in some detail why this was not justified as a matter of economic rationality, and why it is deleterious as a matter of justice. Here, I only note the characteristic of internationalization and harmonization as a one-way ratchet toward ever-expanding exclusivity.

Take a simple provision like the term of copyright protection. In the mid-1990s, Europe was providing for many works (but not all) a term of life of the author plus seventy years, while the United States provided exclusivity for the life of the author plus fifty. A central argument for the Sonny Bono

___ 1
___ 0
___ 1

Copyright Term Extension Act of 1998 was to “harmonize” with Europe. In the debates leading up to the law, one legislator actually argued that if our software manufacturers had a shorter term of copyright, they would be disadvantaged relative to the European firms. This argument assumes, of course, that U.S. software firms could stay competitive in the software business by introducing nothing new in software for seventy-five years, and that it would be the loss of revenues from products that had not been sufficiently updated for seventy-five years to warrant new copyright that would place them at a disadvantage. The newly extended period created by the Sonny Bono Copyright Term Extension Act is, however, longer in some cases than the protection afforded in Europe. Sound recordings, for example, are protected for fifty years in Europe. The arguments are now flowing in the opposite direction—harmonization toward the American standard for all kinds of works, for fear that the recordings of Elvis or the Beatles will fall into the European public domain within a few paltry years. “Harmonization” is never invoked to de-escalate exclusivity—for example, as a reason to eliminate the European database right in order to harmonize with the obviously successful American model of no protection, or to shorten the length of protection for sound recordings in the United States.

International agreements also provide a fertile forum for ratcheting up protection. Lobbies achieve a new right in a given jurisdiction—say an extension of term, or a requirement to protect technological protection measures on the model of the DMCA. The host country, usually the United States, the European Union, or both, then present the new right for treaty approval, as the United States did in the context of the WIPO treaties in the mid-1990s. Where this fails, the United States has more recently begun to negotiate bilateral free trade agreements (FTAs) with individual nations. The structure of negotiation is roughly as follows: The United States will say to Thailand, or India, or whoever the trading partner is: If you would like preferential treatment of your core export, say textiles or rice, we would like you to include this provision or that in your domestic copyright or patent law. Once this is agreed to in a number of bilateral FTAs, the major IP exporters can come back to the multilateral negotiations and claim an emerging international practice, which may provide more exclusivity than their then applicable domestic law. With changes to international treaties in hand, domestic resistance to legislation can be overcome, as we saw in the United States when the WIPO treaties were used to push through Congress the DMCA anticircumvention provisions that had failed to pass two years

— 1
 — 0
 — 1

earlier. Any domestic efforts to reverse and limit exclusivity then have to overcome substantial hurdles placed by the international agreements, like the agreement on Trade Related Aspects of Intellectual Property (TRIPS). The difficulty of amending international agreements to permit a nation to decrease the degree of exclusivity it grants copyright or patent holders becomes an important one-way ratchet, preventing de-escalation.

Countervailing Forces

As this very brief overview demonstrates, most of the formal institutional moves at the content layer are pushing toward greater scope and reach for exclusive rights in the universe of existing information, knowledge, and cultural resources. The primary countervailing forces in the content layer are similar to the primary countervailing forces in the logical layer—that is, social and cultural push-back against exclusivity. Recall how central free software and the open, cooperative, nonproprietary standard-setting processes are to the openness of the logical layer. In the content layer, we are seeing the emergence of a culture of free creation and sharing developing as a countervailing force to the increasing exclusivity generated by the public, formal lawmaking system. The Public Library of Science discussed in chapter 9 is an initiative of scientists who, frustrated with the extraordinarily high journal costs for academic journals, have begun to develop systems for scientific publication whose outputs are immediately and freely available everywhere. The Creative Commons is an initiative to develop a series of licenses that allow individuals who create information, knowledge, and culture to attach simple licenses that define what others may, or may not, do with their work. The innovation represented by these licenses relative to the background copyright system is that they make it trivial for people to give others permission to use their creations. Before their introduction, there were no widely available legal forms to make it clear to the world that it is free to use my work, with or without restrictions. More important than the institutional innovation of Creative Commons is its character as a social movement. Under the moniker of the “free culture” movement, it aims to encourage widespread adoption of sharing one’s creations with others. What a mature movement like the free software movement, or nascent movements like the free culture movement and the scientists’ movement for open publication and open archiving are aimed at is the creation of a legally self-reinforcing domain of open cultural sharing. They do not negate property-like rights in information, knowledge, and culture. Rather, they represent a

— 1
— 0
— 1

self-conscious choice by their participants to use copyrights, patents, and similar rights to create a domain of resources that are free to all for common use.

Alongside these institutionally instantiated moves to create a self-reinforcing set of common resources, there is a widespread, global culture of ignoring exclusive rights. It is manifest in the widespread use of file-sharing software to share copyrighted materials. It is manifest in the widespread acclaim that those who crack copy-protection mechanisms receive. This culture has developed a rhetoric of justification that focuses on the overreaching of the copyright industries and on the ways in which the artists themselves are being exploited by rights holders. While clearly illegal in the United States, there are places where courts have sporadically treated participation in these practices as copying for private use, which is exempted in some countries, including a number of European countries. In any event the sheer size of this movement and its apparent refusal to disappear in the face of lawsuits and public debate present a genuine countervailing pressure against the legal tightening of exclusivity. As a practical matter, efforts to impose perfect private ordering and to limit access to the underlying digital bits in movies and songs through technical means have largely failed under the sustained gaze of the community of computer scientists and hackers who have shown its flaws time and again. Moreover, the mechanisms developed in response to a large demand for infringing file-sharing utilities were the very mechanisms that were later available to the Swarthmore students to avoid having the Diebold files removed from the Internet and that are shared by other censorship-resistant publication systems. The tools that challenge the “entertainment-as-finished-good” business model are coming into much wider and unquestionably legitimate use. Litigation may succeed in dampening use of these tools for copying, but also creates a heightened political awareness of information-production regulation. The same students involved in the Diebold case, radicalized by the lawsuit, began a campus “free culture” movement. It is difficult to predict how this new political awareness will play out in a political arena—the making of copyrights, patents, and similar exclusive rights—that for decades has functioned as a technical backwater that could never invoke a major newspaper editorial, and was therefore largely controlled by the industries whose rents it secured.

— 1
— 0
— 1

THE PROBLEM OF SECURITY

This book as a whole is dedicated to the emergence of commons-based information production and its implications for liberal democracies. Of necessity, the emphasis of this chapter too is on institutional design questions that are driven by the conflict between the industrial and networked information economies. Orthogonal to this conflict, but always relevant to it, is the perennial concern of communications policy with security and crime. Throughout much of the 1990s, this concern manifested primarily as a conflict over encryption. The “crypto-wars,” as they were called, revolved around the FBI’s efforts to force industry to adopt technology that had a backdoor—then called the “Clipper Chip”—that would facilitate wiretapping and investigation. After retarding encryption adoption in the United States for almost a decade, the federal government ultimately decided that trying to hobble security in most American systems (that is, forcing everyone to adopt weaker encryption) in order to assure that the FBI could better investigate the failures of security that would inevitably follow use of such weak encryption was a bad idea. The fact that encryption research and business was moving overseas—giving criminals alternative sources for obtaining excellent encryption tools while the U.S. industry fell behind—did not help the FBI’s cause. The same impulse is to some extent at work again, with the added force of the post-9/11 security mind-set.

One concern is that open wireless networks are available for criminals to hide their tracks—the criminal uses someone else’s Internet connection using their unencrypted WiFi access point, and when the authorities successfully track the Internet address back to the WiFi router, they find an innocent neighbor rather than the culprit. This concern has led to some proposals that manufacturers of WiFi routers set their defaults so that, out of the box, the router is encrypted. Given how “sticky” defaults are in technology products, this would have enormously deleterious effects on the development of open wireless networks. Another concern is that free and open-source software reveals its design to anyone who wants to read it. This makes it easier to find flaws that could be exploited by attackers and nearly impossible to hide purposefully designed weaknesses, such as susceptibility to wiretapping. A third is that a resilient, encrypted, anonymous peer-to-peer network, like FreeNet or some of the major p2p architectures, offers the criminals or terrorists communications systems that are, for all practical purposes, beyond the control of law enforcement and counterterrorism efforts. To the extent

— 1
— 0
— 1

that they take this form, security concerns tend to support the agenda of the proprietary producers.

However, security concerns need not support proprietary architectures and practices. On the wireless front, there is a very wide range of anonymization techniques available for criminals and terrorists who use the Internet to cover their tracks. The marginally greater difficulty that shutting off access to WiFi routers would impose on determined criminals bent on covering their tracks is unlikely to be worth the loss of an entire approach toward constructing an additional last-mile loop for local telecommunications. One of the core concerns of security is the preservation of network capacity as a critical infrastructure. Another is assuring communications for critical security personnel. Open wireless networks that are built from ad hoc, self-configuring mesh networks are the most robust design for a local communications loop currently available. It is practically impossible to disrupt local communications in such a network, because these networks are designed so that each router will automatically look for the next available neighbor with which to make a network. These systems will self-heal in response to any attack on communications infrastructure as a function of their basic normal operational design. They can then be available both for their primary intended critical missions and for first responders as backup data networks, even when main systems have been lost—as they were, in fact, lost in downtown Manhattan after the World Trade Center attack. To imagine that security is enhanced by eliminating the possibility that such a backup local communications network will emerge in exchange for forcing criminals to use more anonymizers and proxy servers instead of a neighbor's WiFi router requires a very narrow view of security. Similarly, the same ease of study that makes flaws in free software observable to potential terrorists or criminals makes them available to the community of developers, who quickly shore up the defenses of the programs. Over the past decade, security flaws in proprietary programs, which are not open to inspection by such large numbers of developers and testers, have been much more common than security breaches in free software. Those who argue that proprietary software is more secure and allows for better surveillance seem to be largely rehearsing the thought process that typified the FBI's position in the Clipper Chip debate.

More fundamentally, the security concerns represent a lack of ease with the great freedom enabled by the networked information environment. Some of the individuals who can now do more alone and in association with others want to do harm to the United States in particular, and to advanced liberal

— 1
— 0
— 1

market-based democracies more generally. Others want to trade Nazi memorabilia or child pornography. Just as the Internet makes it harder for authoritarian regimes to control their populations, so too the tremendous openness and freedom of the networked environment requires new ways of protecting open societies from destructive individuals and groups. And yet, particularly in light of the systematic and significant benefits of the networked information economy and its sharing-based open production practices to the core political commitments of liberal democracies, preserving security in these societies by eliminating the technologies that can support improvements in the very freedom being protected is perverse. Given Abu Ghraib and Guantanamo Bay, however, squelching the emergence of an open networked environment and economy hardly seems to be the most glaring of self-defeating moves in the war to protect freedom and human dignity in liberal societies. It is too early to tell whether the security urge will ultimately weigh in on the side of the industrial information economy incumbents, or will instead follow the path of the crypto-wars, and lead security concerns to support the networked information economy's ability to provide survivable, redundant, and effective critical infrastructures and information production and exchange capabilities. If the former, this impulse may well present a formidable obstacle to the emergence of an open networked information environment.

— 1
— 0
— 1

- Social Ties in Two Suburban Localities,” *City & Community* 2, no. 4 (December 2003): 335.
14. Useful surveys include: Paul DiMaggio et al., “Social Implications of the Internet,” *Annual Review of Sociology* 27 (2001): 307–336; Robyn B. Driskell and Larry Lyon, “Are Virtual Communities True Communities? Examining the Environments and Elements of Community,” *City & Community* 1, no. 4 (December 2002): 349; James E. Katz and Ronald E. Rice, *Social Consequences of Internet Use: Access, Involvement, Interaction* (Cambridge, MA: MIT Press, 2002).
 15. Barry Wellman, “Computer Networks as Social Networks,” *Science* 293, issue 5537 (September 2001): 2031.
 16. Jeffery I. Cole et al., “The UCLA Internet Report: Surveying the Digital Future, Year Three” (UCLA Center for Communication Policy, January 2003), 33, 55, 62, <http://www.ccp.ucla.edu/pdf/UCLA-Internet-Report-Year-Three.pdf>.
 17. Pew Internet and Daily Life Project (August 11, 2004), report available at http://www.pewinternet.org/PPF/r/131/report_display.asp.
 18. See Barry Wellman, “The Social Affordances of the Internet for Networked Individualism,” *Journal of Computer Mediated Communication* 8, no. 3 (April 2003); Gustavo S. Mesch and Yael Levanon, “Community Networking and Locally-Based Social Ties in Two Suburban Localities,” *City & Community* 2, no. 4 (December 2003): 335.
 19. Barry Wellman, “The Social Affordances of the Internet.”
 20. A review of Ito’s own work and that of other scholars of Japanese techno-youth culture is Mizuko Ito, “Mobile Phones, Japanese Youth, and the Re-Placement of Social Contact,” forthcoming in *Mobile Communications: Re-negotiation of the Social Sphere*, ed., Rich Ling and P. Pedersen (New York: Springer, 2005).
 21. Dana M. Boyd, “Friendster and Publicly Articulated Social Networking,” *Conference on Human Factors and Computing Systems (CHI 2004)* (Vienna: ACM, April 24–29, 2004).
 22. James W. Carrey, *Communication as Culture: Essays on Media and Society* (Boston: Unwin Hyman, 1989).
 23. Clay Shirky, “A Group Is Its Own Worst Enemy,” published first in *Networks, Economics and Culture* mailing list July 1, 2003.

PART III. Policies of Freedom at a Moment of Transformation

1. For a review of the literature and a substantial contribution to it, see James Boyle, “The Second Enclosure Movement and the Construction of the Public Domain,” *Law and Contemporary Problems* 66 (Winter-Spring 2003): 33–74.
2. Early versions in the legal literature of the skepticism regarding the growth of exclusive rights were Ralph Brown’s work on trademarks, Benjamin Kaplan’s caution over the gathering storm that would become the Copyright Act of 1976, and Stephen Breyer’s work questioning the economic necessity of copyright in many industries. Until, and including the 1980s, these remained, for the most part, rare voices—joined in the 1980s by David Lange’s poetic exhortation for the public domain; Pamela

___ 1
 ___ 0
 ___ 1

Samuelson's systematic critique of the application of copyright to computer programs, long before anyone was paying attention; Jessica Litman's early work on the political economy of copyright legislation and the systematic refusal to recognize the public domain as such; and William Fisher's theoretical exploration of fair use. The 1990s saw a significant growth of academic questioning of enclosure: Samuelson continued to press the question of copyright in software and digital materials; Litman added a steady stream of prescient observations as to where the digital copyright was going and how it was going wrong; Peter Jaszi attacked the notion of the romantic author; Ray Patterson developed a user-centric view of copyright; Diane Zimmerman revitalized the debate over the conflict between copyright and the first amendment; James Boyle introduced erudite criticism of the theoretical coherence of the relentless drive to propertization; Niva Elkin Koren explored copyright and democracy; Keith Aoki questioned trademark, patents, and global trade systems; Julie Cohen early explored technical protection systems and privacy; and Eben Moglen began mercilessly to apply the insights of free software to hack at the foundations of intellectual property apologia. Rebecca Eisenberg, and more recently, Arti Rai, questioned the wisdom of patents on research tools to biomedical innovation. In this decade, William Fisher, Larry Lessig, Litman, and Siva Vaidhyanathan have each described the various forms that the enclosure movement has taken and exposed its many limitations. Lessig and Vaidhyanathan, in particular, have begun to explore the relations between the institutional battles and the freedom in the networked environment.

CHAPTER 11. The Battle Over the Institutional Ecology of the Digital Environment

1. Paul Starr, *The Creation of the Media: Political Origins of Modern Communications* (New York: Basic Books, 2004).
2. Ithiel de Sola-Pool, *Technologies of Freedom* (Cambridge, MA: Belknap Press, 1983), 91–100.
3. *Bridgeport Music, Inc. v. Dimension Films*, 2004 U.S. App. LEXIS 26877.
4. Other layer-based abstractions have been proposed, most effectively by Lawrence Solum and Minn Chung, *The Layers Principle: Internet Architecture and the Law*, University of San Diego Public Law Research Paper No. 55. Their model more closely hews to the OSI layers, and is tailored to being more specifically usable for a particular legal principle—never regulate at a level lower than you need to. I seek a higher-level abstraction whose role is not to serve as a tool to constrain specific rules, but as a map for understanding the relationships between diverse institutional elements as they relate to the basic problem of how information is produced and exchanged in society.
5. The first major treatment of this phenomenon was Michael Froomkin, "The Internet as a Source of Regulatory Arbitrage" (1996), <http://www.law.miami.edu/froomkin/articles/arbitr.htm>.
6. Jonathan Krim, "AOL Blocks Spammers' Web Sites," *Washington Post*, March 20,

— 1
 — 0
 — 1

- 2004, p. A01; also available at <http://www.washingtonpost.com/ac2/wp-dyn?page=article&contentId=A9449-2004Mar19¬Found=true>.
7. FCC Report on High Speed Services, December 2003 (Appendix to Fourth 706 Report NOI).
 8. 216 F.3d 871 (9th Cir. 2000).
 9. *National Cable and Telecommunications Association v. Brand X Internet Services* (decided June 27, 2005).
 10. *Turner Broad. Sys. v. FCC*, 512 U.S. 622 (1994) and *Turner Broad. Sys. v. FCC*, 520 U.S. 180 (1997).
 11. *Chesapeake & Potomac Tel. Co. v. United States*, 42 F.3d 181 (4th Cir. 1994); *Comcast Cablevision of Broward County, Inc. v. Broward County*, 124 F. Supp. 2d 685, 698 (D. Fla., 2000).
 12. The locus classicus of the economists' critique was Ronald Coase, "The Federal Communications Commission," *Journal of Law and Economics* 2 (1959): 1. The best worked-out version of how these property rights would look remains Arthur S. De Vany et al., "A Property System for Market Allocation of the Electromagnetic Spectrum: A Legal-Economic-Engineering Study," *Stanford Law Review* 21 (1969): 1499.
 13. *City of Abilene, Texas v. Federal Communications Commission*, 164 F.3d 49 (1999).
 14. *Nixon v. Missouri Municipal League*, 541 U.S. 125 (2004).
 15. Bill Number S. 2048, 107th Congress, 2nd Session.
 16. *Felten v. Recording Indust. Assoc. of America Inc.*, No. CV- 01-2669 (D.N.J. June 26, 2001).
 17. *Metro-Goldwyn-Mayer v. Grokster, Ltd.* (decided June 27, 2005).
 18. See Felix Oberholzer and Koleman Strumpf, "The Effect of File Sharing on Record Sales" (working paper), http://www.unc.edu/cigar/papers/FileSharing_March2004.pdf.
 19. Mary Madden and Amanda Lenhart, "Music Downloading, File-Sharing, and Copyright" (Pew, July 2003), http://www.pewinternet.org/pdfs/PIP_Copyright_Memo.pdf/.
 20. Lee Rainie and Mary Madden, "The State of Music Downloading and File-Sharing Online" (Pew, April 2004), http://www.pewinternet.org/pdfs/PIP_Filesharing_April_04.pdf.
 21. See 111 F.Supp.2d at 310, fns. 69–70; *PBS Frontline* report, <http://www.pbs.org/wgbh/pages/frontline/shows/hollywood/business/windows.html>.
 22. A. M. Froomkin, "Semi-Private International Rulemaking: Lessons Learned from the WIPO Domain Name Process," <http://www.personal.law.miami.edu/froomkin/articles/TPRC99.pdf>.
 23. Jessica Litman, "The Exclusive Right to Read," *Cardozo Arts and Entertainment Law Journal* 13 (1994): 29.
 24. *MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1993).
 25. Lawrence Lessig, *Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity* (New York: Penguin Press, 2004).
 26. Jessica Litman, "Electronic Commerce and Free Speech," *Journal of Ethics and Information Technology* 1 (1999): 213.

___ 1
 ___ 0
 ___ 1

27. See Department of Justice Intellectual Property Policy and Programs, <http://www.usdoj.gov/criminal/cybercrime/ippolicy.htm>.
28. *Eldred v. Ashcroft*, 537 U.S. 186 (2003).
29. *Bridgeport Music, Inc. v. Dimension Films*, 383 F.3d 390 (6th Cir.2004).
30. 383 F.3d 390, 400.
31. Mark A. Lemley, "Intellectual Property and Shrinkwrap Licenses," *Southern California Law Review* 68 (1995): 1239, 1248–1253.
32. 86 F.3d 1447 (7th Cir. 1996).
33. For a more complete technical explanation, see Yochai Benkler, "An Unhurried View of Private Ordering in Information Transactions," *Vanderbilt Law Review* 53 (2000): 2063.
34. James Boyle, "Cruel, Mean or Lavish? Economic Analysis, Price Discrimination and Digital Intellectual Property," *Vanderbilt Law Review* 53 (2000); Julie E. Cohen, "Copyright and the Jurisprudence of Self-Help," *Berkeley Technology Law Journal* 13 (1998): 1089; Niva Elkin-Koren, "Copyright Policy and the Limits of Freedom of Contract," *Berkeley Technology Law Journal* 12 (1997): 93.
35. *Feist Publications, Inc. v. Rural Telephone Service Co., Inc.*, 499 U.S. 340, 349–350 (1991).
36. Directive No. 96/9/EC on the legal protection of databases, 1996 O.J. (L 77) 20.
37. J. H. Reichman and Paul F. Uhler, "Database Protection at the Crossroads: Recent Developments and Their Impact on Science and Technology," *Berkeley Technology Law Journal* 14 (1999): 793; Stephen M. Maurer and Suzanne Scotchmer, "Database Protection: Is It Broken and Should We Fix It?" *Science* 284 (1999): 1129.
38. See Stephen M. Maurer, P. Bernt Hugenholtz, and Harlan J. Onsrud, "Europe's Database Experiment," *Science* 294 (2001): 789; Stephen M. Maurer, "Across Two Worlds: Database Protection in the U.S. and Europe," paper prepared for Industry Canada's Conference on Intellectual Property and Innovation in the Knowledge-Based Economy, May 23–24 2001.
39. Peter Weiss, "Borders in Cyberspace: Conflicting Public Sector Information Policies and their Economic Impacts" (U.S. Dept. of Commerce, National Oceanic and Atmospheric Administration, February 2002).
40. *eBay, Inc. v. Bidder's Edge, Inc.*, 2000 U.S. Dist. LEXIS 13326 (N.D.Cal. 2000).
41. The preemption model could be similar to the model followed by the Second Circuit in *NBA v. Motorola*, 105 F.3d 841 (2d Cir. 1997), which restricted state misappropriation claims to narrow bounds delimited by federal policy embedded in the Copyright Act. This might require actual proof that the bots have stopped service, or threaten the service's very existence.
42. *New York Times v. Sullivan*, 376 U.S. 254, 266 (1964).

— 1
— 0
— 1