8

Rethinking "Unauthorized Access"

As we saw in Chapter 7, institutional and technological changes driven by the perceived imperatives of piracy and security are reshaping the networked information environment, leading to the emergence of architectures of control. Efforts to develop a framework for determining whether and how law should concern itself with these developments have been only partly successful, for reasons that reflect the analytical limitations of the model of regulation developed in *Code*. Meanwhile, the everyday practice of individuals and communities in the networked information society follows its own rhythms. The mismatch between institutional regimes organized around architectures of control and the tactical behaviors of situated subjects sets the stage for recurring conflict over the conditions of access to networked resources and spaces. It is not surprising, then, that such conflict has been a defining feature of the legal landscape for the past two decades.

In this chapter, I lay the groundwork for a different way of thinking about the architecture of the networked information environment: one that takes into account both emerging social and institutional patterns and the everyday practice of network users. The starting point is a deceptively simple question: what if we inverted the analysis suggested by the *Code* framework? Rather than asking what architectures of control do, what if we asked how users experience the accessibility of information networks and resources, and then considered how architectures of control reshape that experience? *Code*'s implicit orientation toward the liberal subject—the solitary, unknowable dot at the heart of the regulatory matrix—results in relative indifference to the first question. How might foregrounding the experience of situated, embodied users affect our understanding of both network architectures and the institutional and social patterns within which they are embedded?

The analysis proceeds in three parts. First, I consider the accessibility of information networks and resources from the perspective of the situated user. Although the analysis roughly follows the pattern begun in Chapters 4 and 6, it is also different. Those chapters sought to "decenter" understandings of creativity and subjectivity, detaching them from individualist and intentionalist perspectives on creativity and self-formation. In the context of disputes about access, it has become vitally important to recover an individualist perspective, albeit a reconfigured one, to provide a baseline for evaluating the institutional and technological changes now underway. Accordingly, this chapter develops a "recentered" model of accessibility that considers the ways in which networked

information technologies, including both technologies of control and technologies of more general application, structure the experienced accessibility of network resources. Networked information technologies have some features that empower users and other features that create new challenges for everyday practice. We saw in Chapter 2 that technologies and artifacts mediate our perceptions of the possible; we use them to remake our world, but we also take the world they present to us as given. For some time now, networked information technologies have been evolving in a direction that reinforces the latter process, rendering the operation of the networked information environment increasingly opaque.

Next, I explore the ways in which the emergence of architectures of control alters the experienced accessibility of networked resources and spaces. Architectures of control and the institutional arrangements within which they are embedded do not simply aim to define the boundaries of legal entitlements, nor to create and rationalize information flows within markets and government information systems. They reflect a fundamental shift in our political economy, toward a system of governance based on precisely defined, continually updated authorization of access by and to actors, resources, and devices. Within the emerging regimes of authorization, discourses of national security, economic security, and technical authority work to reinforce a system of differential accessibility to information about the network's operation. Paradoxically, those discourses derive enormous power from the fact that they have taken root within an ideology of openness in which precepts about open government and open markets function both as received truths and as cardinal aspirations. Although regimes of authorization have no necessary connection to authoritarian political forms, they work to instantiate a system of governance that is authoritarian in the generic sense: one that favors compliant submission to authority. They seek to produce not only willing vendors, consumers, and citizens, but also tractable ones, and they seek these changes not merely at the behavioral level, but at the infrastructural level as well.

Finally, I consider regimes of authorization in relation to the theory of information rights and human flourishing developed in this book. The topic of accessibility presents difficult problems for law, policy, and theory. Limits on access to technical protocols and networked resources can be enormously important to social welfare; therefore, the law sometimes must reinforce such limits. But flexibility in the conditions of access to technical protocols and networked resources is also vital to human flourishing; therefore, the law should not reinforce regimes of authorization wherever they are asserted, and sometimes should seek to limit the reach of such regimes. Like the rules and institutions that confer and enforce copyright entitlements and those that confer or withhold privacy protection, the rules and institutions that regulate the network's accessibility should acknowledge and accommodate the play of everyday practice.

A Recentered Model of Accessibility

In legal theory, discussions about the conditions of accessibility tend to become discussions of ownership status. Here, however, I am not concerned with ownership, but rather with the practical accessibility of network resources.

It is useful to approach that topic by jettisoning the conventional, ownership-related categories of public/private and property/commons in favor of a more open-ended conceptual analysis of the geographies now emerging within networked space. I begin by sketching some alternate formulations of the ways in which networked information technologies create, disrupt, and regulate geographies of accessibility. Next, I consider how situated users experience the accessibility of the network and its constituent resources, both informational and technical. Finally, I explore the complex relationship between the design of networked information technologies and the everyday practice of network users.

Geographies of Accessibility in Networked Space

Experientially, accessibility has spatial, material, and temporal dimensions. A given resource may be theoretically accessible but geographically remote, technically or practically difficult to acquire, or old and hard to find. Although accessibility works differently, and sometimes more easily, in networked space than it does in real space, considerations of space, materiality, and time remain important in determining whether, how, and by whom particular resources will be found. Accessibility in networked space has geographic patterns of its own. Those patterns highlight the importance of technical protocols and processes in mediating the accessibility of networked resources.

As Chapter 2 explained, networked space is constituted by flows of information and communication that are layered over real-space geographies. The geography of networked space is defined by those flows—and, importantly, by their borders. In general, the borders of networked space are not tightly linked to national borders, but this does not mean that flows of networked information are unbounded. We are accustomed to thinking of borders as signaling fixed, binary points of demarcation, but geographers and scholars of human migration have long recognized that borders depend importantly on socially constructed rules. For example, applicants for a visa to travel to the United States encounter the national "border" while still in their home countries; the duty-free section of Charles de Gaulle Airport is decreed to be borderless for some purposes while remaining subject to French law for others. Saskia Sassen argues that borders are more accurately described as analytic "borderlands," the sets of conditions that govern passage from one domain to another. Those conditions are discursive as well as physical, and derive much of their power from the extent to which their foundational assumptions—about sovereignty, legal authority, and so on—are taken for granted.[1] So too with networked space, which has analytic borderlands of its own.

Networked space makes the discursive aspect of borders manifest; even its physical boundaries derive from semantic conditions—from rules instantiated in code that could be arranged in some other way. Yet the practical operation of network borders reminds us that discursive boundaries are no less powerful than physical ones. Flows of information, communication, and commerce move in patterns structured by both technical protocols and rules of network behavior. Technical protocols such as search algorithms and automated filters determine which information is shown to particular users and how it is shown. Often, decisions about the provision of information are based on information automatically collected from and about users. The rules that determine the distance between networked resources are constituted dynamically by the linking

practices of network users and the indexing practices of search engines, which together determine the paths that connect one resource to the next.[2] The resulting patterns establish the topologies that network users must negotiate.

Technical protocols determine not only the direction and boundaries of information flows, but also the scale of the economic, social, and cultural processes to which they relate. In real space, we intuitively grasp the significance of scale in shaping the patterns of everyday practice. Some processes are local, others citywide, others national, and the scale of a particular process or institution affects the way that both participants and bystanders experience it. So too with the geographies of networked space. Some processes in networked space, such as auctions for collectibles on eBay or discussion boards on CNN.com, take place on a grand scale. Others, such as dedicated members-only listservs, operate on a scale that is smaller and more intimate.

The emergence of networked space, however, has also changed the scale on which many social processes occur. The social science literature on globalization identifies the emergence of a new sense of space as simultaneously global and local, without mediating levels in between. Geographers have deployed the term "glocal" to describe this space, which simultaneously collapses some scales and renders others inconceivably large.[3] Glocal space is a by-product of the emergence of networked space: it is produced by the extension of information and communication networks throughout real space, and by the interpenetration of the real and the virtual. The space that results from this process increasingly is characterized by the technologically mediated disappearance of intermediate levels of scale between local and global.

Within legal and policy discussions about the networked information society, scale is often understood as a purely technical phenomenon, while scalability and interconnectivity are assumed to be generally beneficial. Those assumptions are far too simple. Scalability furthers some goals that are worth pursuing, such as communication and competition, but undermines others. The seamless interoperability that enables global communication also enables global data flows of personal information. The demise of "walled gardens" in social networking may enable easier networking across larger and larger communities, but also may increase the likelihood of unwanted information flows to community members and make communities too large to sustain certain types of interaction. Standardization in copyright law shapes cultural practices globally, but increasing globalization leaves less and less room for heterogeneity, contextual separation, and local variation.[4] The ostensibly technical question "Does it scale?" thus both crystallizes and masks questions that are fundamentally political. Like borders, scale depends in part on analytical constructs, this time relating to the appropriate scope of social, cultural, and economic activity.

Finally, accessibility has a temporal dimension. Other things being equal, information is more likely to be accessible to someone if it is stored in a relatively permanent, easily searchable form. With respect to both variables, a very odd dynamic is beginning to emerge. Artistic and intellectual culture is relatively inaccessible and ephemeral, while personal information is relatively ubiquitous and persistent. Those de facto policies are expressed and effectuated via the technical protocols that govern the storage, retention, and searchability of digital information, and via a wide range of associated institutional practices.

Within the domain of copyright, legal and technological developments are producing a world in which the conditions of access to cultural and informational resources are carefully controlled, and those resources are constantly at risk of disappearing. The archival practices of portals for proprietary content vary considerably, and many such portals use robot.txt files to block caching and archiving by search engines. Intermediaries such as libraries, booksellers, and search engines still play important roles in providing access to these resources, but an increasing number of copyright disputes seek to limit the types of access that intermediaries can offer. Confronted with shrinking budgets and shelf space, many libraries are dismantling their stacks and moving physical copies to remote storage. In place of physical texts, they offer patrons access to digital versions provided by proprietary subscription services that require continual payment streams. And "going digital" also creates new risks to cultural memory. Digital storage formats have proved to be far more unstable than paper over the long term. Ironically, then, there is a large risk that efforts to create comprehensive digital archives may hasten the processes of cultural forgetting that they seek to prevent.[5] In his 2006 novel, *Rainbows End*, Vernor Vinge described the spectacle of staff members at a large university library systematically ripping up physical books to scan them into a digital library. In the era of Google Book Search, Vinge's vision seems both otherworldly and mundane. Although Google does not destroy the rare books that it is archiving in partnership with university libraries, a key factor in Google's proposed settlement with the publishing industry is the effective disassembly, from the user's perspective, of archived materials as they appear in search results.[6]

Within the domain of privacy, the landscape of memory and absence is oddly inverted. Network architectures constitute social memory along with cultural memory. In the age of "Web 2.0" social-networking technologies and real-time Internet archiving, information about individuals, communities, and groups is increasingly distributed and persistent. Internet archivists and open-access activists may deplore the absence of, say, great books in open archives, but they have been less willing to consider the privacy-related consequences of the "store everything" mentality.[7] As a practical matter, of course, the refusal to make explicit value judgments about the relative merits of different categories of information is itself a judgment—that everything is worth storing for historical reasons, and that no other considerations are relevant. Increasingly, we lack what Michael Curry and Leah Lievrouw call "ecologies of forgetting"—information environments that afford anonymity and ephemerality for those who desire it.[8]

Access to the protocols and processes that regulate geographies of accessibility and inaccessibility in networked space ought to be a subject of paramount concern both for scholars studying the network and for ordinary network users. Yet, as we will see next, a growing constellation of factors—business models, legal doctrines, and accepted design practice—operates to diminish the technical accessibility of the network, obscuring important aspects of the structure and operation of the networked information environment from those who inhabit it. This is so both for technologies that legal scholars have recognized as implicated in architectures of control and for those that they have not.

Situated Users, Reconsidered

How do network users experience the accessibility of resources within networked space? The answer to that question is oddly self-contradictory. For situated users of network resources, networked information technologies enable access to an astonishing bounty of information resources, including technical and scientific information. Often, though, the information abundance of the network contrasts with technical inscrutability in the platforms, portals, and devices that mediate access to the network. The experience of networked space is both increasingly personalized and increasingly opaque.

Information networks offer users an unprecedented wealth of information and an equally unprecedented opportunity for collaboration with like-minded others. It is an oversimplification to say the network's resources are unlimited, or that anything "on the Internet" is instantly available to anyone who connects. Any habitual Internet user knows that although information resources made available via the network are, in theory, equally accessible to all network users, some resources are more available than others. Experientially, the accessibility of those resources is structured by our own inclinations and affinities—by the various human, cultural, and geographic networks within which we are situated. Here the analysis largely duplicates that in Chapters 4 and 6; the process of working through the cultural landscape is, increasingly, a process of working through the networked landscape. The "network of networks" makes boundaries more porous, but still we must begin where we are. Even so, the end result of that process is a qualitatively enormous increase in access to both information and people.

In this chapter, however, I am concerned not only with the accessibility of information resources made available via the network, but also with the accessibility of the network itself—with the technical processes by which it operates and with the ways that those processes shape both our settled routines and our far-ranging explorations. Here the picture becomes more complicated. For some time now, networked information technologies have been evolving in directions that make them simultaneously more convenient—more intuitive, more portable, more seamlessly integrated with our lives—and less accessible in their own right.

In contemporary debates about technology policy, questions about technical accessibility are often subsumed within the rubric of "network neutrality," a term that refers to the conditions under which third-party information providers can access proprietary networks and platforms to offer their services. The network neutrality debate has for the most part proceeded on the presumption that concerns about access to information can be satisfactorily resolved via open and nondiscriminatory treatment of information service providers. Some think market competition will produce that effect; others disagree. The U.S. Federal Communications Commission has called for transparency about network-management practices that affect the treatment of third-party providers, and has attempted to mandate neutrality for some (though not all) types of network providers.[9] For the most part, however, parties to the network neutrality debate do not express a comparable level of concern about the technical transparency to users of the processes that govern access to information.

In fact, neutral provision of access to third-party information providers and technical transparency of the network to users do not necessarily go hand in hand. For the technically trained, this point can be difficult to grasp. From a technical standpoint, the network does not exist as a single entity. Layered atop the Internet's basic protocols are a hodgepodge of applications and networked devices, some understood as "open" and some embedded within emerging architectures of control. From the network perspective, accessibility is determined by the rules that operate at every layer, and those rules can be disaggregated, examined, and chosen or avoided. From the perspective of the ordinary, situated user, though, things look different. Ordinary users experience not rules but effects; together, those effects determine the affordances of the network and its constituent applications—the possibilities for action that the network creates.[10] The rules that produce the effects need not be explained or disclosed, and increasingly are not.

Consider first the regimes of "trusted computing" that the copyright industries have sought to implement. Early models of DRM envisioned a set of atomized authorization processes, but that model collided with user expectations. In an age of increasing mobility, users want to take their content with them, place- and time-shifting it to suit their needs without constantly needing to obtain reauthorization. One proposed solution to these problems is an application of trusted computing sometimes called the personal digital network (PDN) or personal digital network environment (PDNE), which would extend throughout a designated space or across a designated set of consumer electronics equipment. The most important feature of the PDN is seamless plug-and-play capability; within a successfully designed PDN, the transitions between authorized devices should be effortless from the user's point of view.[11]

The seamless PDN is still a long way from implementation, but it is clear that portability of content does not equal transparency of operation. In addition, portability likely will go hand in hand with other changes in functionality that are less appealing to users. In major content-side initiatives, portability is highly leveraged, but only across authorized equipment, while both sharing and repurposing of media files are significantly restricted. The technologies being developed to produce those effects are held as secrets; "looking under the hood" to see how they work is expressly forbidden.[12] From the user perspective, the seamless PDN thus would operate both as an extension of the embodied self and as a revision of it. Trusted-computing technologies may provide increased access to some resources, but they will do it by limiting accessibility in a variety of other ways.

Now consider a group of technologies that is fast becoming integral to a variety of processes, some expressly linked to security and others not. Imagine a typical day in the life of a commuter in a major East Coast city. To get to work in the morning, she scans a smart card to use public transit or uses the transponder installed in her car to pay for tolls and parking. After work, she meets a friend for a drink, consulting the transponder in her car or an application on her mobile phone to find the bar her friend has suggested. On her way home, she stops at a supermarket and uses her debit card to buy groceries. When she returns home, energy-saving sensors in her home detect her presence, turn on the lights, and adjust the climate controls. These technologies are rudimentary versions of "ubiquitous computing" technologies: computing tech-

nologies built into the artifacts of everyday life to manage flows of goods, services, people, and energy in the physical environment. Those who design ubiquitous-computing technologies envision trajectories toward increasing convergence. Not long from now (or so technologists hope), our commuter will manage all of her daily transactions using a single device. Sensors in refrigerators will take the guesswork out of stops at the grocery store, while embedded RFID chips will enable grocers to manage retail inventories automatically.

The organizing concept for these endeavors is the notion of "unremarkable computing": a seamless web of networked, continually communicating artifacts that users experience as natural, if indeed they pause to think about it at all.[13] Engineers and policy makers have understood the shift toward unremarkable computing as presenting two principal problems. First, for the technologies to be most useful, their designers must identify the optimal balance between ease of use and complexity of function. Researchers in human-computer interaction seek to answer this question by modeling increasingly complex problems and building interfaces that embed and then simplify the complexities. Second, unremarkable computing raises concerns about the privacy and security of personal information that the ubiquitous sensors collect and exchange. Yet there is a third problem that is not reducible to either of the other two: what if users were to want access to the ways that the technologies of unremarkable computing work? There are many legitimate reasons for wanting such access; for example, one might want to know how one's personal information is being used, or to improve the ways that one's own devices interact.[14] To the extent that existing laws address this question, they do so from a completely different perspective, that of the trade-secret owner seeking to recruit authorized licensees and exclude competitors, or of the government agency seeking to maintain the secrecy of technical information in the interest of national security. Once again, then, the technologies of unremarkable computing offer new methods of access to some resources within networked space, but they do so in a way that limits access to information about the network's operation.

Similar effects are produced by technologies that most U.S. legal theorists have understood as exemplars of openness: the technologies of search and social networking. Consider the following incidents: in 2006, AOL released a database containing tens of thousands of search queries entered by its subscribers to the public for research purposes. Before releasing the database, AOL had "anonymized" the queries, removing some information to ensure that they could not be linked to any particular user. As it happened, the database contained enough information to enable some users to be identified with some not too difficult reverse engineering. In response to widespread public outcry, AOL disabled access to the database and confessed that it had given the matter insufficient thought.[15] Similar results followed a series of ill-advised decisions by the popular social-networking site Facebook. In 2007, Facebook added data feeds that kept its members updated, in real time, on every change in the status or activities of their online "friends." Also in 2007, it joined a commercial venture, the Beacon program, that would alert members to their friends' purchases. In both cases, the user response was swift and unequivocal. Many users didn't want their friends to receive real-time notifications of every change to their profiles, and didn't want to be turned into promotional agents for products they had purchased. Facebook redesigned its menu of options to give users greater con-

trol and later ended the program as part of a settlement of legal claims filed against it.[16]

The AOL and Facebook controversies represent only the tip of a very large iceberg, and users do not always rebel against new uses of information about their activities. Google's e-mail service, Gmail, mines the subject lines and the contents of e-mail messages for keywords and serves ads related to those keywords. When Google announced the launch of Gmail, and acknowledged that it would use e-mail content to target advertising, users flocked to the service, attracted by the unprecedented amounts of storage that it provided. Privacy advocates warned that Google had provided little real information about how the targeting would be done, but for many users, the possible harms felt too remote or indefinite to matter.[17] If anything, privacy advocates likely understated the extent of Google's data-mining activities. Gmail is but one of a number of linked Google services. Google Shopping stores information about online purchases and shopping preferences; Google Maps supplies satellite imagery and travel directions; Google Desktop encompasses an array of localized information-management services, including a file manager and a shareable calendar, and so on. When you are signed in to your Google account, all the different data streams are linked. Google's acquisition of Doubleclick gave it access to a large amount of data about commercial preferences with which to enhance its profiling algorithms, and the proposed Google Book Search settlement would give Google access to data about users' intellectual interests. Recently, Google announced that it would begin behavioral targeting of advertising to all users of its search engine.[18]

Among legal scholars, these developments are not typically described or understood as raising problems of technical accessibility. Privacy advocates argue that they involve unauthorized access to users and therefore raise questions about the nature and scope of privacy interests. We have already seen that existing privacy frameworks work poorly in such contexts, but my intent here is not to recast accessibility as a privacy issue. Rather, it is to argue that the technologies of search and social networking also raise a different problem, which relates squarely to both the accessibility of information resources and to the transparency of network processes. According to Frank Pasquale, the technical opacity of search threatens the ideal of equal access to information.[19] He is exactly right, but the problem extends both far beyond equal access to information and far beyond the domain of search.

Google's official mission statement promises "to organize the world's information and make it universally accessible and useful," but when its services are considered together, that mission can be reframed in a way that is both more personal and oddly more comprehensive: the management of individuals' entire networked existence.[20] In fact, the two missions are one and the same. Google uses information about and generated by users to create and manage the world of information that it reflects back to users. Its algorithms mediate flows of information, showing subscribers what Google predicts they will want to see. That business plan is noteworthy because of Google's dominant market position, not because the plan itself is an unusual one. AOL didn't disclose why users received the search results they did, and Facebook didn't specify how the Beacon program would work. "Google Everything" is but one example of a more general trend in the networking of everyday life to produce the "semantic

web"—"a Web in which machines mine mountains of metadata in order to automate a wide variety of transactions" and personalize the online experiences of network users.[21]

Like the PDN and ubiquitous computing, the semantic web promises many conveniences. Consider the notion of a "Coasean filter" for marketing-related communications. Such a filter would be tailored so precisely to individual preferences that it would admit only those offers that matched the preferences.[22] Who cannot claim to be intrigued by the promise of a networked future in which only relevant advertising will appear? Ultimately, however, the semantic web operates by separating personalization and control; information about how its constituent technologies channel content to (or away from) users is jealously guarded. Arguably, the public outrage that followed the AOL and Facebook episodes, and the lingering unease that some users feel about Gmail, is only partly about privacy and partly about the lack of operational transparency that characterizes the network as users experience it. Those controversies, and others like them, remind us that we are losing the ability to control the processes of personalized shaping or even to know much about them.

Perhaps, though, technical and cultural accessibility are not equally important. To understand why technical accessibility is important in its own right, we need to return to the accounts of embodied perception and everyday practice developed in Chapter 2 and reconsider the particularly intimate ways in which networked information technologies mediate the everyday practice of network users.

Autonomic Technologies and the Play of Everyday Practice

Chapter 2 explored the ways that networked information technologies mediate our perceptions of the world around us: we experience technologies and artifacts as altering our preexisting capabilities vis-à-vis the physical world, but technologies and artifacts also mediate our embodied perception of that world—of how it is organized and how it works. Because they are both tools for producing useful results and tools for representing the world, networked information technologies shape our perceptions of reality more comprehensively than simpler artifacts do. These points run orthogonally to the principal thrust of STS scholarship. Rejecting the cultural myth of "autonomous technology," STS scholars remind us that technologies do not have autonomous trajectories, but rather are socially shaped.[23] This important point about contingency is often assumed to mean that technologies have no power to shape us, but it should not be. Paths taken have consequences.

The technologies described above are designed to render the functioning of the networked information environment seamless by making complex processes of networked computing largely invisible to end users. Invisible does not mean neutral, though. The technologies of the PDN seek to reshape the embodied experience of the digital media environment. Ubiquitous-computing technologies seek to reorganize the relations between embodied users and their physical and social contexts. Semantic-computing technologies mediate the relations between embodied users and their (own?) preferences, organizing unruly flows of information into patterns that are more easily managed. Each of these design efforts succeeds most fully when users experience its operation as natural—as "just the way things are."

To the extent that we naturalize the built environment, the window for remaking it grows smaller. The tendency to naturalize the operation of technologies and artifacts—to take the world they present to us as given—makes it harder to formulate such a desire, much less implement it. Of course, that tendency is not itself a by-product of digital technologies; it predates the digital age. But because networked information technologies simultaneously mediate and represent the world around us, they have at least the potential to accelerate processes of naturalization. Each of the technologies described above possesses that potential. Ubiquitous computing defines an "Internet of things," DRM defines an "Internet of (proprietary) media," and the semantic web promises to define an "Internet of me"—a universe of relevant information sorted and managed by each person's personal information manager. As we incorporate these technologies more fully into the practice of everyday life, it can be increasingly difficult to identify the point where technology leaves off and the embodied self begins. From the perspective of embodied, situated users, new technological developments in the networked information society may lack visible trajectories, let alone autonomous ones.

Borrowing from biology, I will use the term "autonomic" to describe the relationships between these technologies and the networked self. IBM has used the term "autonomic computing" to refer to a philosophy of design for very complex systems. Its "Autonomic Computing Manifesto" envisions a future in which information and communication technologies mediate flows of information automatically via sophisticated feedback mechanisms. It invokes the model of the autonomic nervous system, which mediates essential biological processes automatically via feedback mechanisms that for the most part lie below the threshold of our conscious control.[24] I mean something related but slightly different, which concerns the way that networked information technologies—whether or not they have technically complex feedback mechanisms—are experienced by users. To an ever-increasing extent, networked information technologies operate automatically to mediate the activities of culture, self-, and community formation. It is no coincidence that the figure of the cyborg, discussed in Chapter 2, emerged in the work of a scholar trained in the life sciences. In the arena of the biomedical, the distinction between internal and external was already problematized by advanced, internally implanted prosthetics. But flows of information across interfaces between the body and a technologically enabled society are not confined to the domain of the biomedical, and the characteristics of those flows have profound implications for both self-development and the creation of social meaning.

The play of everyday practice is important precisely because it counters the innate tendency to naturalize—to take the current technological landscape as given—with the innate tendency to tinker, repurpose, and adapt. Everyday practice is the day-to-day process of negotiating the dialectical relationship between constraint and possibility. Within networked space, information flows are defined by semantic and technical structures. The play of everyday practice pushes against those structures, sometimes conforming to them and sometimes finding ways to work around them. Some users might want, or need, to know at least in a general sense what a networked digital product does. Others might want to find out how the product or network works "behind the scenes"—what is happening to the information that it collects, for example, or how particular search results came to be displayed. Still others might want the ability to repur-

pose the product or network—to make it do different things. In each case, the product resists, but everyday practice persists.

We can hypothesize that, generally speaking, the process of naturalization and the play of everyday practice exist in a sort of equilibrium—sometimes one is ascendant, and sometimes the other is. It is possible that even the new autonomic technologies would not alter that overall pattern. Because they operate so invisibly, autonomic technologies threaten to tilt the balance more heavily toward naturalization. It is harder to work around a set of protocols that has been designed to disappear. But the obverse is also true: the human tendency to tinker, repurpose, and adapt artifacts—to incorporate artifacts into the play of everyday practice—increases the likelihood that interesting facts about the network and its constituent devices will be discovered. The distributed, "unfinished" nature of networked information technologies amplifies the power of everyday practice. Everyday practice leverages both the distributed, democratic nature of networked information technologies and what Jonathan Zittrain has called their generativity—their extraordinary amenability to tinkering and revision.[25] Users build new tools, develop new "places," generate new communities, and create new cultural practices. While networked information technologies present everyday practice with large challenges, they also present it with large opportunities.

But aspirations toward seamless design are not the only factor in play. The equilibrium between naturalization and everyday practice also depends on larger social and institutional factors. Here we return to the linked architectural and institutional changes introduced in Chapter 7. As autonomic technologies morph into more carefully structured governance regimes organized around architectures of control, the activities that constitute the play of everyday practice are exactly the ones that those regimes seek to prevent.

The Networked Self in the Age of Authorization

As we saw in Chapter 7, U.S. legal scholars have examined emerging architectures of control principally through the lens of liberalism's foundational dichotomy between liberty and constraint. Because that framing encourages a focus on what technologies of control prohibit, legal scholars have paid far less attention to what those technologies do in the grey area where liberty and constraint mingle: they authorize. Emerging architectures of control operate within nascent institutional regimes that span both public and private sectors and that derive their power from a reconfiguration of the meaning and significance of "unauthorized access." The vehicle for this process is not the "appliance" Internet described by Zittrain; appliances do not engage in acts of authorization, nor do they recruit individuals and technology vendors into networks of authorized, and compliant, insiders.[26] It is something different and far more powerful: a new mode of governance for the networked information society. The emerging regimes of authorization work to produce both a configuration of networked space that is increasingly opaque to its users and users who are increasingly habituated to processes of authorization and their associated requirements of technical and operational secrecy.

The Shifting Meaning of Unauthorized Access

Let us begin by reexamining Chapter 7's account of the emergence of architectures of control, this time with authorization rather than prohibition in mind. The emerging technical and institutional regimes organized around architectures of control do not function simply to prohibit certain actions. Instead, they reconfigure networked space by extending and normalizing protocols for authorization of access to network resources. In the two decades since the enactment of the Computer Fraud and Abuse Act (CFAA), the prevailing conception of unauthorized access, and so of the appropriate domains of authorization, has changed almost beyond recognition. In the 1980s, "unauthorized access" described a group of relatively narrow, stand-alone problems capable of resolution within a single statute. In the twenty-first century, managing access has become the central regulatory problem of the networked information society. The principal purpose of emerging architectures of control is to define as precisely as possible the actions that are authorized and the persons or devices authorized to take them.

The drafters of the CFAA conceived of unauthorized access as a threat to a "computer," and understood a computer to be a fixed, discrete location to which one might gain access. Once inside that location, the extent of authorized access could be differentiated, but the principal boundary to be defended was that of the computer itself. That conception implied a correlative understanding of the default rules that obtain in the world outside the computer's boundaries. In that world, no special authorization of access would be required for most ordinary actions that a "user," or ordinary person, might wish to take.

The CFAA's conceptualization of the world as a large unregulated space surrounding small zones of authorized access also shaped the conceptualization of those labeled wrongdoers under the statute. Most often, it was assumed, those wishing to gain access would be highly skilled outsiders—hackers looking for the digital equivalent of a joyride in a stolen car, or "crackers" bent on more malevolent ends. Many scholars have argued that equating hackers with wrongdoers oversimplified an emerging subculture that was far more complex, and I have no quarrel with that position. My point here is different: whether or not the view of hackers embodied in the CFAA was accurate or appropriate, it was a view that excluded most of the general population. Anxiety about computer users remained largely confined to those "superusers" possessing both atypical skill and high levels of motivation to gain entry to purportedly secure systems.[27]

The relatively simple vision of a computing world comprising isolated fortresses under threat from malevolent outsiders was complicated by the problem of the unauthorized insider. When someone hacks into a protected computer or file from outside the system, that action is unauthorized both technically and legally. The situation changes when an insider—an employee, a contractor, or a customer—abuses a position of trust to access resources that he is not supposed to use. From a technical perspective, the actions might be considered authorized; for example, perhaps the wrongdoer supplied the required password. Defining the actions as unauthorized—or, in the CFAA's terms, actions that "exceed[]authorized access"—requires resort to nontechnical standards of proper conduct. Once articulated, such standards became vehicles for the CFAA's expansion to cover a variety of "unauthorized" actions with respect

to publicly available content on the internal pages of Web sites.[28] For a variety of reasons, however, most Web site owners did not choose to implement their preferences via technologies that precisely calibrated authorization of access, and so the melding of technical and normative authorization remained incomplete.

In the copyright context, the objects requiring protection against unauthorized access have no fixed location. To accommodate the idea of digital objects that carry restrictions with them, the conceptualization of unauthorized access underwent a dramatic shift. For such a system to work, authorization itself must become broadly distributed. The architectures of pervasively distributed copyright enforcement drive toward precisely that end. They seek to change the technical and legal parameters of content-related transactions, both online and offline, in a way that renders them fundamentally relational on two levels. For individual users, transactions over copyrighted content become processes characterized by the ongoing authorization of access and use. Those processes, in turn, will not work properly unless compliance by licensed equipment and service providers is mandatory and verifiable, and that necessitates realignments in the relationships between intermediaries and content providers. Effective implementation of pervasively distributed control requires ongoing authorization of intermediaries' access to and implementation of the relevant standards.

As both authorization and unauthorized access detached themselves from fixed locations, the identity of the presumed threat also shifted. The hacker remains a powerful figure in copyright's mythology because it is hackers who have the skill and (presumed) motivation to circumvent technical protections and release unprotected copies into darknets. Now, however, the figure of the hacker coexists uneasily with the idea that the real locus of distrust is the ordinary user, who cannot be relied upon to turn away from illegality when the opportunity presents itself.

At the same time, redefining "unauthorized access" to encompass circumvention of the protocols for access to widely distributed files has made it much more difficult to create legal exceptions that would shield a range of socially valuable activities. Law- and policy makers have tried several different methods of creating such exceptions. In formulating the DMCA's core prohibitions, Congress attempted to use "access" as a narrowing concept to safeguard user rights. The DMCA distinguishes between technical protection measures (TPMs) that function as access controls and those that protect against violation of the exclusive rights of copyright owners. It bans the manufacture and distribution of tools for circumventing both types of TPM, but prohibits only those individual acts of circumvention that are directed at access controls. Congress thought a ban on the circumvention of access controls appropriate and fair because otherwise users could circumvent to avoid payment. Meanwhile, Congress thought, users would remain free to devise means of their own choosing to circumvent rights controls as necessary to exercise the privileges afforded them under copyright law.[29] That strategy for safeguarding user rights, however, depended entirely on an interpretation of "access" as encompassing only a narrow domain of activity.

Litigation over the meaning of the DMCA's prohibitions has established that the new model of authorization-based access cannot be so easily ca-

cabined. Consider a TPM that allows the user to play a music or video file but prevents copying. According to the legislative rationale for the DMCA's bifurcated structure, this TPM is a rights control. Yet in litigation over circumvention of the CSS algorithm, which encrypts DVD movies to allow playback but not copying, courts acquiesced without question in the entertainment industries' classification of CSS as an access control because it prevents rendering the content on noncompliant devices.[30] That construction means that only authorized DVD *players*—as opposed to authorized *users*—may access the encrypted content. But if only authorized players can make authorized access, then two further conclusions follow. First, if every act of rendering protected content is an act of accessing the content, then the individual privilege to circumvent rights controls exists only in theory. Second, if "access" refers to devices and not to people, then the development of unauthorized media players violates the ban on tools for circumventing access controls. This rule grants far-reaching control over technology development to those who control the processes of authorization.

Efforts to define narrower legal shelters for certain types of unauthorized access have met with a similar fate. Software reverse engineering is a type of unauthorized access that copyright law allows on the grounds that it is essential to both innovation and competition. Seeking to preserve that privilege, Congress created an exception to the DMCA's prohibitions, allowing both circumvention of TPMs and the manufacture of circumvention tools "to achieve interoperability of an independently created computer program with other programs."[31] Since PC-based media players are also computer programs, in theory that exception should allow the unauthorized creation of interoperable media players. Courts have found a variety of ways to avoid reaching this result, however, and it would be hard to square with their conclusion that the statute's prohibitions encompass access to digital media content by unauthorized devices.

Taking a different approach, the Copyright Office has attempted to legitimize unauthorized access to a particular class of devices. Mobile phones released in U.S. markets typically are configured to work only on one or a few authorized networks; configuring a phone for use on another carrier's network requires an act of circumvention (or reverse engineering). The DMCA authorizes the Copyright Office to create exemptions from the rule forbidding circumvention of access controls when necessary to enable access to particular classes of works. The Copyright Office issued a rule allowing circumvention of access controls on mobile phone software that operate to restrict network access. Unlike the reverse-engineering exception, the mobile phone exemption brackets the question of what is or isn't a "computer program" and invokes consumer protection concerns.[32] But the device-based framework is no more coherent than a framework that distinguishes between computer programs and media players. Many mobile phones are also media players, and the two types of functionality can be made to intertwine. This flexibility allows the technology vendor to determine which set of rules will apply. For example, Apple Computer has used technical countermeasures to disable "liberated" iPhones, releasing firmware upgrades that turned the devices into useless "bricks."[33] If Apple released upgrades that selectively disabled iTunes, owners of hacked iPhones who attempted to fix the problem would risk violating the DMCA's access prohibition.

In the world of pervasively distributed security measures, the conceptualization of unauthorized access has begun to shift again, in a way that completely inverts the implicit presumptions that produced the CFAA. As more and more of the ordinary transactions that make up everyday life become processes characterized by the ongoing authorization of access and use, authorization becomes essential to the ordinary person's existence—necessary to get to work, pay bills, and access communication systems. Levels of access also become defining conditions of privilege; some users have more access than others, and that fact too structures the rhythms of everyday life.

In such a world, moreover, the target class is related to the class of putative wrongdoers only in the most notional sense. On their face, of course, security measures target wrongdoers. The need to catch the terrorist, the money launderer, or the identity thief is obvious and pressing. Yet when security measures are brought to bear on everyone, those individuals cannot plausibly be said to be the sole targets of the corrective measures any more than speeders can be said to be the sole intended audience for traffic signals. Pervasively distributed security measures target everyone because universal coverage is their raison d'etre. They operate on the presumption that security requires it.

As authorization of access become the norm, the ability of users to make authorized access increasingly depends on their agreeing to submit to invasive procedures for authentication. Network users have become accustomed to accepting without question automatic updates of software that, among other things, mediates authorization processes. Other security procedures may require the installation of cookies, tracking software, or biometric readers on users' devices. The outer boundaries of technology vendors' authority to install functionality for tracking, authentication, and authorization are poorly delineated. There is no generally agreed dividing line between spyware and authorized installation, and technology vendors have little to gain from drawing one.[34] In short, within the new political economics of precisely calibrated authorization, the conditions of authorized access to users do not seem to be precisely defined, or limited, at all.

The emerging regimes of authorization are not the work of some invisible, hitherto-concealed dictator or corporate cabal. They are the products of our ordinary institutions of governance: markets, property and contract rights, and legislation by democratically elected representatives. They depend for their success on two kinds of changes in our political culture. The first relates to political discourse; the second, to ingrained habits of behavior and thought.

Ideologies of Openness, Discourses of Authority

The emerging regimes of authorization require regimes of secrecy to sustain their operation. This hard reality creates insuperable difficulties for a legal system premised on an ideology of openness in government and in markets. One would expect societal commitment to an ideology of openness to prompt questions about regimes of technical secrecy, and many dedicated public-interest advocates have devoted their careers to raising such questions. Just as often, though, the process seems to work in reverse: the power of the ideology of openness operates to conceal the extent to which technical secrecy is reinforced by law. Regimes of technical secrecy derive additional force from moral panics that cast restrictions on access as a matter of social and cultural

survival, and from processes of technical mystification that position decisions about network architecture as purely technical matters best handled by expert elites.

In evaluating the role of secrecy in our political discourse, it is useful to return to Jodi Dean's critique of the "political economy of communicative capitalism," which we encountered at the end of Chapter 6. Dean argues that the political economy of the modern mass-communication society is characterized by an ideology of openness and antihegemony, but driven in fact by a mix of secrecy and spectacle. Within this political economy, she argues, secrecy becomes both a locus of economic value and the object of public desire. The desire to expose secrets feeds a public culture of the spectacle, which neither satiates the desire nor dislodges the power that secrets represent.[35] Remarkably for a study of the political economy of the networked information society, however, Dean's book devotes almost no attention to the politics of openness in technical contexts. To understand the political economy of openness in the networked information society, it is necessary to consider the treatment of specifically technical information as well. Discussions of technical information are characterized by a dialectic between secrecy and spectacle, but that dialectic has a slightly different flavor than the one Dean describes.

It is well recognized that governments can leverage secrecy to create structures of differential visibility that reinforce their own power, and it is commonly believed that such secrecy threatens core principles of democratic governance. Such assertions of government secrecy are increasingly routine. For example, many law enforcement experts believe that surveillance deters crime most effectively when the fact of surveillance is visible but the details of surveillance behavior are deliberately concealed. They apply similar reasoning to technical information about surveillance practices, arguing that secrecy serves both deterrence- and enforcement-related goals. Efforts to gain access to operational information about government profiling and data-mining practices are invariably met with assertions about the ways in which secrecy serves national security and about why disclosure would jeopardize essential state secrets.[36]

How, in this context, should one interpret statutory frameworks and underlying normative principles purporting to require government accountability in data processing? The U.S. Freedom of Information Act mandates far-reaching disclosure of information about government actions and processes, but exempts classified information, trade secret information, and information about law enforcement techniques and procedures if such disclosure would "risk circumvention of the law" or create risks to physical safety.[37] Although the FOIA is widely considered to be a keystone of open government, in reality the amount of secrecy those exceptions permit is indeterminate, and may be very great. Assertions of national security interests do not always persuade courts; the process of seeking access proceeds slowly; and the extent of publicly available information about such practices remains incomplete. In particular, the operations of the vaunted Foreign Intelligence Surveillance Act (FISA) court remain almost entirely secret. Ironically, in the wake of disclosures about widespread and wholly unauthorized government wiretapping, we have come to cling to its (presumed) procedural regularity—again, a case of partial disclosure used to

great effect.[38] (Better the devil who plays by secret rules than the one who follows no rules at all.)

In the private sector, secrets about the structure of privately administered components of the information society are a potent source of economic power. The basic Internet protocols remain open, but from the ordinary individual's perspective, that counts for much less than we are led to think. The individual experience of the network is shaped by a host of technical intermediaries, many of whom argue that maintaining the secrecy of technical protocols is a competitive necessity, essential to preserving robust and "open" competition. Efforts to gain access to information about the algorithms that determine the order of online search results typically have been stymied by assertions of trade secrecy, and digital content owners have used the trade-secret status of DRM protocols as one weapon in their litigation campaign against devices that enable unauthorized access.[39] Frameworks for ensuring private-sector accountability in the processing of personal data are focused principally on ensuring individuals the right of access to their "own" data—that is, data about the person, not data about the algorithms that will process it.[40]

Spectacle also plays an important role in discourses about technical secrecy in these government and private-sector processes, but the spectacles that capture public attention are not the banal tales of self-exposure that we encountered in Chapter 6. Instead, they involve a different sort of morality play, which revolves around the malevolent figures of the hacker, the "pirate," and the terrorist. Rather than rewarding the exposure of technical secrets, these morality plays tend to reinforce regimes of technical secrecy, aligning secrecy with political, economic, and cultural survival. Consider, for example, Judge Lewis Kaplan's characterization of the problem posed by the DeCSS litigation:

> In a common source epidemic, as where members of a population contract a non-contagious disease from a poisoned well, the disease spreads only by exposure to the common source. If one eliminates the source, or closes the contaminated well, the epidemic is stopped. In a propagated outbreak epidemic, on the other hand, the disease spreads from person to person. Hence, finding the initial source of the infection accomplishes little, as the disease continues to spread even if the initial source is eliminated. For obvious reasons, then, propagated outbreak epidemics, all other things beings equal, can be far more difficult to control.
>
> This disease metaphor is helpful here. The book infringement hypothetical is analogous to a common source outbreak. Shut down the printing press (poisoned well) and one ends the infringement (the disease outbreak). The spread of means of circumventing access to copyrighted works in digital form, however, is analogous to a propagated outbreak epidemic. Finding the original source of infection (e.g., the author of DeCSS or the person to misuse it) accomplishes nothing as the disease (infringement made possible by DeCSS, the resulting availability of decrypted DVDs) may continue to spread from one person who gains access to the circumvention program or decrypted DVD to another. And each is infected, i.e.,

> each is as capable of making perfect copies of the digital file containing the copyrighted work as the author of the program or the first person to use it for improper purposes.[41]

As Chapter 7 described, Judge Kaplan's elaboration of the disease metaphor for online copyright infringement is not a solitary occurrence, but rather adopts a persistent theme sounded by the copyright industries and echoed in media coverage of digital copyright issues. The rhetoric of contagion plays an analogous role in the security context. Addressing a joint session of the U.S. Congress several months after the U.S. invasion of Iraq, British prime minister Tony Blair called terrorism "a new and deadly virus" originating in "a fanatical strain of religious extremism . . . that is a mutation of the true and peaceful faith of Islam." Other public figures, including legislators from both political parties, describe terrorism as a "cancer" that must be "eradicated" before it destroys the health of the body politic.[42]

These statements are not simply window dressing for a substance that lies elsewhere—in reasoned debate about the nature of property or the appropriate extent of civil liberty. When rhetorics of crisis succeed, they create the perception of an existential threat to society that requires an immediate and drastic response. This process, which scholars have termed "securitization," urgently suggests that society must be reorganized to counter the threat.[43] In casting piracy and terrorism as threats to the health of the body politic, the metaphors of contagion and cancer work not only to mobilize public support for secrecy, but also to signal the range of appropriate and necessary corrective actions.

The classic societal response to an acute threat to public health is quarantine. Foucault described the methods developed by medieval city-states for managing outbreaks of the plague. As Foucault explained, authorities responded to a great threat that traveled by human contact in the only way possible—by eliminating contact. Although medieval physicians did not have the benefit of modern principles of microbiology and epidemiology, they understood that the plague spread by human-to-human contact. Therefore, during an outbreak, citizens were forbidden to leave their homes. Every evening, a designated corps of inspectors would go door-to-door and demand that each inhabitant of a household stand at the window to prove that he or she was still alive. If the inhabitants of a home were stricken, the home remained isolated until everyone in it had either died or shown immunity by surviving. Then the home was scoured and its contents were burned.[44] In the networked information society, some responses to acute security threats map more or less directly to the classic pattern; for example, antimalware programs "quarantine" infected files.

But most information-age "epidemics" are too complicated for quarantine to be a viable strategy, for two reasons. First, the understanding of acute danger as episodic does not translate well to the contexts of copyright infringement, terrorism, and identity theft. In the societies that originated the techniques of plague control, emergencies were temporary. As the plague passed, so did the ability to sustain the extreme measures it was thought to justify, which required both a massive expenditure of resources and near-complete suspension of ordinary activity. Second, the germs that cause the plague have no positive qualities, and there is no independent reason to disseminate them. Digital economies, in contrast, thrive on endless flows of all types of information. The

"propagated outbreak epidemic" to which Judge Kaplan referred is simply an example of a more general property of networks of all sorts; information must move for the network to exist.

Governance regimes predicated on technical, legal, and market strategies for separating authorized from unauthorized flows of information and communication solve both of these problems. Such regimes open up a middle ground between a state of quarantine and rules allowing the unrestricted movement of people, communications, and information. Within that middle ground, many possibilities exist for convergence between perceived security imperatives and the self-interest of information intermediaries.[45] As we saw in Chapter 5, flows of information in the emerging networked information society reflect a set of beliefs about the relationship between risk, information, and profit. For the institutions that participate in the network, information technologies promise systematized knowledge as an antidote to insecurity. At the same time, architectures designed to facilitate authorized movement may be more readily perceived by market actors as affording the potential for competitive leverage.

Understanding emerging regimes of authorization through the lens of securitization also explains the paradoxical stance toward openness exhibited by corporate and political actors. To serve both their competitive and regulatory functions, regimes of authorization must be buttressed by technical and procedural secrecy, but they also must demand more and more openness of individual citizens. The morality plays of the hacker, the pirate, and the terrorist serve both to induce more disclosure in exchange for more security and to convince network users that more security cannot be had in any other way.

Critically, the public discourse around secrecy and security is also unstable in important ways. Public interest advocates have generated a constant stream of cases in which secrecy has pernicious effects on concrete, identifiable people—people wrongly placed on the Transportation Security Administration's no-fly list and unable to clear their names, computer-ignorant grandmothers sued by the recording industry based on assertedly foolproof methods for tracking their downloads, and so on. In addition, scandals about electronic voting and identity theft have begun to generate narratives that are inconsistent with those that the morality plays seek to instill.[46]

On the other hand, as these examples suggest, technical processes also introduce a new kind of tension between ideologies of openness and discourses of secrecy, a tension revolving around technical authority and the appropriate roles of those who possess it. The emergence of technical standards as sites for the production of power constitutes new regulatory and political processes: the expert fora in which technical standards are defined and revised. In those processes, the patterns of accessibility typically associated with modern forms of democratic government are dramatically altered.

Standards processes for information networks and platforms tend to be conducted in ways that obscure network governance functions behind a veil of technical mystification. Most obviously, some standards processes are operated by private consortia of technology companies, pursuant to trade-secrecy regimes. Others are conducted by open-membership organizations or by government bodies, but even nominally open or public standards processes can be

opaque and mysterious. They are conducted in complex, technical language and unfold over lengthy time periods, and both factors can operate to prevent widespread public awareness of what is at stake. This tends to obscure the political implications of network standards and protocols, along with difficult and important questions about whether governance by elites trained predominantly in technical fields is normatively desirable.[47]

The emerging regimes of authorization contribute to the climate of technical mystification by restricting participation in their standards processes to authorized professionals. The DMCA's exceptions for reverse engineering, encryption research, and security testing are crafted in ways that preclude their invocation by members of the public.[48] In other contexts, regimes of trade secrecy and state secrecy that foreclose routine public access to information about surveillance systems produce similar results, operating to professionalize innovation by restricting technical access to authorized insiders.

Moral panics and technical mystification do not displace the ideology of openness that is so central to our political discourse; they depend centrally on ideologies about the value of certain kinds of openness in certain contexts. At the same time, however, they change the prevailing understanding of how openness is supposed to work. Together, moral panics and technical mystification facilitate the normalization of institutional ecologies predicated on differential accessibility to the technical operation of the emerging networked information society. Those ecologies have profound implications for our political culture.

Configuring Tractable Users

Regimes of authorization and accompanying discourses of authority work to establish technical and market path-dependencies—patterns of accessibility and inaccessibility—that themselves come to be seen as normal and natural. This reshapes the everyday experience of networked space in ways that the liberal binary of liberty and coercion does not encompass. The thrust of these strategies is to produce tractable users who comply with the requirements of authorization protocols and refrain from behaviors that are unauthorized or simply anomalous.

Consider, again, the problem of liberty and constraint that has preoccupied cyberlaw scholars. Within liberal political theory, the evil of paramount concern is coercion by an authoritarian government. Because information networks have evolved in ways that are relatively resistant to government control, cyberlaw scholars have viewed the rise of information networks as fundamentally incompatible with the propagation of authoritarianism.

The emerging political economies of authorization are quite different from authoritarian political regimes, and that difference has operated to conceal the magnitude of the cultural and political change that they represent. Regimes of authorization have no necessary connection to authoritarian political regimes; in fact, the opposite is more nearly true. Regimes of authorization thrive in market economies, which more reliably provide both the technical know-how and entrepreneurial initiative to fill apparent security needs. In addition, regimes of authorization may or may not concern themselves directly with the sorts of dissent that matter most within the liberal paradigm and that reliably mobilize authoritarian political regimes. Architectures of control need not pre-

vent people from setting up their own digital soapboxes, nor from purchasing access to listeners.

In place of authoritarian government, regimes of authorization offer a more generic model of authoritarian governance. Both models of regulation seek to instill habits of compliant submission to unquestioned authority, and to use their authority to generate and normalize new patterns of conduct. But authoritarian governance has a different goal and a correspondingly different modus operandi than authoritarian governments do.

Social theorists who study the networked information society argue that there is a mutually constituting relationship between the network's material affordances—the possibilities for action that it creates—and the forms of subjectivity that it enables, which I will call the network's "psychic affordances." These theorists offer different conceptions of self-formation, but each identifies a fundamental relationship between network structure and processes of self-formation. Manuel Castells argues that the emerging networked information society is constituted by a dialectical relationship between the Net, a new set of institutional arrangements organized around networked information and communication technologies, and the Self, a set of activities directed toward defining the meaning of identity. For Gilles Deleuze, the emerging "control society" provides very limited scope for self-differentiation. He characterizes the control society as signaling a shift from Foucauldian discipline via externally imposed normalizing frameworks to less crude but potentially more powerful "modulation" by continual streams of information to, from, and about individuals. Other theorists, such as Jean Baudrillard, argue that the distinguishing characteristic of the networked information society is not modulation but simulation: the networked presentation of alternate realities casts the self adrift, unable to distinguish reality from an endless series of simulacra.[49]

Although these theories are very different from one another, each directs our attention to the ways that the structure of the network mediates the formation of the networked selves who inhabit it. That process is material as well as informational. The geographies and architectures of networked space establish the material field for processes of self-constitution. Scholars of geography and urban planning have explored the ways that the design of public spaces shapes cultural and social life, and have argued that planned spaces risk achieving order at the expense of diversity, vibrancy, and social and cultural mobility. Drawing on this work, Michael Madison has observed that, just as early twentieth-century urban planning moved to eliminate visual chaos and replace it with order, so the technical and contractual mediation of information flows within information networks threatens to eliminate the diversity of textures and "feels" that flourishes under less restrictive architectures. Aesthetically and experientially, one might compare the controlled spaces that result from digitally mediated standardization to large shopping malls or gated communities.[50] This architectural shift recasts the options available to both ordinary and technically skilled network users, producing subtle but fundamental behavioral and cultural changes.

Experientially, the processes of standardization contemplated by emerging regimes of authorization work to produce a larger geography of information space that is increasingly standardized and that we increasingly come to take for granted. At the same time, the interpolation of regimes of authoriza-

tion into formerly private spaces redraws the boundary between private and public, producing at the intersection a third sort of space that is neither entirely private nor conventionally public. That space combines the exposure of behavior in public spaces (but not the mobility or expressive privilege) with the isolation of private spaces (but not the security against intrusion). Regimes of authorization invade, disrupt, and casually rearrange the boundaries of personal and social spaces and of the intellectual, cultural, and relational activities played out within those spaces.

Only some of these emerging architectural and institutional changes alter the scope for individual agency as conventionally understood by legal theorists. Most obviously, direct technical constraint on behavior—for example, a digital file that cannot be shared with anyone, or a tamper-resistant biometric authentication device—substitutes rule-governed behavior for individual judgment and responsibility. In many cases, we might conclude that looseness of fit between rules and behavior is itself a social good. Where the precise contours of legal rules are unclear, or the proper application of legal rules to particular facts is contested, imperfect control of individual conduct shields a range of experimentation that involves individuals and communities in the creation of law and furthers the value-balancing goals of a sound and inclusive public policy.

The more significant effects of regimes of authorization, however, are not so easily characterized as constraints on liberty. Recall, once again, that the momentum toward regimes of authorization is so strong precisely because we are not driven to embrace them by coercion. Our relationship to these developments is ambivalent, driven in equal parts by fear and desire, and cemented by growing habituation. For individuals, networked information technologies promise more immediate, accurate, and convenient fulfillment of their desires. The networked self in the age of authorization seeks safety, to be sure, but also the convenience that authentication and personalization bring. This is, again, the difference between prohibition and authorization; the control society can claim to have won broader acceptance in the marketplace because it offers commodities that people (learn to) want.[51]

In narrowing the horizons of individual desire, regimes of authorization also narrow social and architectural tolerances for the construction of difference. As Rosemary Coombe demonstrates in the context of intellectual property and John McGrath shows in the context of surveillance, the rules that govern the uses of information can expand or constrict the scope for creative appropriation—for play with the symbolisms embedded in cultural artifacts and attached to particular, culturally identified behaviors.[52] Regimes of authorization extend these effects throughout networked space, operating upon difference and unpredictability to produce more homogeneous, more carefully modulated behavior. As Chapter 6 discussed, even newly-emerging practices of self-exposure take on a standardized quality.

In sum, the networked self in the age of authorization is a different self, and the networked society a correspondingly different society. It may be that the psychic affordances of the emerging regimes of authorization are the ones we want; certainly, that is what conventional hedonic analysis would suggest. Before reaching that conclusion, though, we should take stock of their effects on a range of individual and social practices that we claim to value. In particu-

lar, we should consider more carefully the effects of regimes of authorization on the play of everyday practice.

Accessibility as Scope for Material Practice

Law plays an integral role in the emergence of regimes of authorization. With increasing frequency, legal prohibitions, incentives, and mandates are deployed unquestioningly to reinforce technical, commercial, and political regimes of differential accessibility. That is both a great mistake and a lost opportunity. Limitations on access to networked resources can be important, and even essential, for the networked information society to function in a way that promotes the well-being of its citizens. Legal rules that prohibit and punish unauthorized access to networked resources sometimes will be necessary. But only sometimes. The well-being of the networked selves who inhabit the emerging information society also depends importantly on the ability to find—or create—breathing room for everyday material practice. Regimes of authorization that operate systematically to diminish such breathing room therefore warrant careful, critical attention from law- and policy makers.

Recall the analysis of the relationship between processes of naturalization and the play of everyday practice that concluded the first half of this chapter. That discussion suggested that everyday material practice—including not only tinkering and reengineering by relatively skilled users, but also repurposing of artifacts and spaces by ordinary users—serves both instrumental and intrinsic goals that are far broader and more momentous than those typically acknowledged by lawmakers and legal commentators. Everyday material practice is the root cause of movement in material culture, the antidote to technical, spatial, and interpretative stagnation. It is what counteracts the innate tendency to naturalize the built environment—to take the configurations of spaces and the affordances of artifacts as givens, and to move obediently in the patterns they suggest. It is precisely the fluidity and unpredictability of everyday material practice that regimes of authorization treat as suspect and seek to contain. Law may side with rigidity sometimes, but to align with it always would be to jeopardize an essential dimension of cultural vibrancy.

As in the case of copyright, one might argue that attempting to define legal shelter for the play of everyday material practice would be both quixotic and unnecessary. Arguably, defined zones of legal protection are definitionally incompatible with play of everyday practice, which by its very nature resists technical and institutional limitations. For similar reasons, we might conclude that the everyday practice of situated users is a given and therefore something with which the law need not concern itself; within any regime of governance, some amount of diffuse, tactically driven behavior will occur.

Those conclusions, however, would be too hasty. The analysis in the second half of this chapter suggests that the everyday material practice of situated users is also a quantity that is contingent and extraordinarily vulnerable to environmental modulation. To the extent that habits of tractability instilled by the emerging regimes of authorization reinforce processes of naturalization already underway in the networked digital environment, they work to insulate that environment and its constituent protocols from challenge, critique, and re-

vision. More generally, the habits of tractability instilled by emerging regimes of authorization dampen the amplitude of everyday practice in contexts both technical and nontechnical, jeopardizing a broad range of other goals that the play of everyday practice promotes. The play of everyday practice forms the substrate out of which a mature and critical subjectivity, a vibrant artistic and intellectual culture, and a robust culture of technical innovation all emerge. If we are serious when we say that these are goals that our society values, then we need an information policy to match.

This analysis has important implications, first, for the legal treatment of hacking and tinkering by situated users. Attempts by legal theorists to justify a "right to hack" or a "freedom to tinker" have seemed unable to formulate a narrative that would capture the urgency of such a right. Attention to the play of everyday practice enables us to cast hacking and tinkering in a new and more compelling light. The process of tinkering with artifacts and tools is both mundane and extraordinary. Tinkering is an indispensable prerequisite for transformative innovation, but it is also what ordinary people do on a daily basis, and in everyday practice it is an indispensable prerequisite for the exercise of material and social agency. It enables users of technology to adapt standardized tools and interfaces to their more particular goals. That process in turn increases the likelihood that the fruits of innovation will be distributed broadly and adapted eclectically, in ways that promote the flourishing of disparately situated communities.

The constitutive importance of tinkering for human flourishing means that lawmakers cannot take the easy out by prohibiting all acts of "circumvention" or "unauthorized access" without regard to motives or consequences. Instead, the law has a dual role to play, proscribing some kinds of unauthorized access while preserving room for the acts of tactical evasion and situated creativity that make up the fabric of everyday life.

This chapter's exploration of the various dimensions of accessibility also demonstrates, however, that merely rolling back legal prohibitions on hacking and tinkering would be unlikely to guarantee all the kinds of accessibility or all of the kinds of breathing room that human flourishing demands. Some problems of accessibility and breathing room—particularly those that recur in copyright disputes—are readily amenable to resolution by determined tinkering. Other problems are not. For example, it is probably shortsighted to rely on tinkering and hacking to ensure the optimal mix of openness and privacy, including both informational privacy and adequate shelter for behavior in networked spaces, or to guarantee sufficient representation in expert standards processes. In those contexts and many others, preserving scope for everyday material and spatial practice requires a broader array of regulatory options.

Notably, many of the goals that I have just listed do not require simply increased accessibility, but rather a normatively informed recalibration of the balance between "open" and "closed." Put differently, the requirements of human flourishing place nonneutral, normative constraints on the design of network architectures. Again and again throughout this book, we have seen that interstitial flexibility serves important social purposes. The value of architectural and institutional constraints lies not only in the pattern of constraint and authorization that they impose, but also in the spaces left over for activities that are neither constrained nor authorized. Networked space can be a space of

dystopian domination or a space that affords breathing room for situated creativity and critical identity practice, depending significantly on the nature of its system of boundaries and permissions. Network-neutrality mandates, however they are crafted, simply do not speak to that question. We have also seen that technology markets may not—and in the current climate, likely will not—produce such a normatively informed recalibration "on their own."

It is worth emphasizing that identifying these needs is a long way from prescribing ways in which the law should attempt to pursue them. This point is too often lost in debates about information law and policy; partisans on both sides are apt to assume that calls for correction are calls for command-and-control forms of regulation. As we have seen, there are dangers in attempting to make either code or law all-powerful. The control fetishism of code-based regulation is in tension with the critical importance of indeterminacy in the linked realms of cultural creativity, evolving, socially situated subjectivity, and material practice. But law can descend into control fetishism as well. Considering how to shape information rights and associated technical architectures that promote human flourishing while avoiding the problem of control-fetishism is the subject of Part V.

Notes

[1] Sassen, *Territory, Authority, Rights*, 379-86.

[2] For a description of this process, see Barabási, *Linked*, 41-92.

[3] Swyngedouw, "Neither Global Nor Local," 140-42.

[4] On global standardization of copyright rules, see Birnhack, "Global Copyright, Local Speech." On convergence in social networking, see Ching-man Au Yeung, Ilaria Liccardi, Kanghao Lu, Oshani Senaviratne, & Tim Berners-Lee, "Decentralization: The Future of Online Social Networking," *W3C Workshop on the Future of Social Networking*, Jan. 2009, http://www.w3.org/2008/09/msnws/papers/decentralization.pdf; Keven Moffitt, "Facebook's Open Graph: Could It Be the End of the Walled Garden?" *E-Commerce Developer*, May 13, 2010, http://www.ecommercedeveloper.com/articles/1903-Facebook-s-Open-Graph-Could-It-Be-the-End-of-the-Walled-Garden-; Juan Carlos Perez, "Data Portability: Reasonable Goal or Impossible Dream?," *PCWorld*, Jan. 21, 2008, http://www.pcworld.com/businesscenter/article/141541/data_portability_reasonable_goal_or_impossible_dream.html.

[5] For a comprehensive discussion of the challenges of cultural preservation in the networked information environment, see Pessach, "[Networked] Memory Institutions."

[6] For a helpful summary of Google's policies regarding the display of books still under copyright, see Jonathan Band, "A Guide for the Perplexed: Libraries and the Google Library Project Settlement," American Library Association and the Association of Research Libraries, Nov. 13, 2008, 4-5, http://www.arl.org/bm~doc/google-settlement-13nov08.pdf.

[7] See Eric Bangeman, "Internet Archive Settles Suit over Wayback Machine," *Ars Technica*, August 31, 2006, http://arstechnica.com/old/content/2006/08/7634.ars; Steve Lohr, "It's History, So Be Careful Using Twitter," *New York Times*, Apr. 15, 2010.

[8] See Curry & Lievrouw, "Places to Read Anonymously." On the geographies of digital memory and forgetting, see also Blanchette & Johnson, "Data Retention and the Panoptic Society"; Mayer-Schonberger, *Delete*.

[9] See U.S. Federal Communications Commission, "In the Matter of Preserving the Open Internet: Broadband Industry Practices," No. 10-201, Dec. 21, 2010, Appendix A, http://www.fcc.gov/Daily_Releases/Daily_Business/2010/db1223/FCC-10-201A1.pdf; U.S. Federal Communications Commission, "In the Matter of Preserving the Open Internet: Broadband Industry Practices," No. 09–93, Oct. 22, 2009, ¶¶ 118-132, http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-09-93A1.pdf. As of this writing, Congress may block the 2010 regulation from taking effect. See Paul Barbaglio, "House Commerce Adopts Resolution to Overturn FCC's Net Neutrality Rules," *BNA Electronic Commerce & Law Report*, Mar. 16, 2011, 420.

[10] On affordances, see Norman, *The Design of Everyday Things*, 9-11, 87-104; Pfaffenberger, "Social Anthropology of Technology," 503-07.

[11] See, for example, U.S. Federal Communications Commission, "Digital Broadcast Content Protection: Notice of Proposed Rulemaking," 68 Fed. Reg. 67,624, 67,625 (Dec. 3, 2003); U.S. Federal Communications Commission, "Report and Order and Further Notice of Proposed Rulemaking: In the Matter of Digital Broadcast Content Protection," No. 03–273, Nov. 4, 2003, ¶ 63. For an early model of digital rights management contemplating atomized authorization, see Stefik, "Letting Loose the Light," 226-34.

[12] See Gillespie, *Wired Shut*, 236-40.

[13] Weiser, "Creating the Invisible Interface." A fuller exposition of Weiser's vision of computing appears in Weiser, "The Computer for the 21st Century."

[14] In a provocative article, Jerry Kang and Dana Cuff suggest that users might employ pervasive computing capabilities to bring the public sphere into the shopping mall, tagging places and products with persistent, user-generated commentary and critique; see Kang & Cuff, "Pervasive Computing." In a similar vein, see Anne Galloway, "Intimations of Everyday Life."

[15] See Saul Hansell, "AOL Removes Search Data on Vast Group of Web Users," *New York Times*, Aug. 8, 2006; Michael Barbaro & Tom Zeller, Jr., "A Face Is Exposed for AOL Searcher No. 4417749," *New York Times*, Aug. 9, 2006.

[16] See Louise Story and Brad Stone, "Facebook Retreats on Online Tracking," *New York Times*, Nov. 30, 2007; Caroline McCarthy, "Facebook Beacon Has Poked Its Last," *CNet News*, Sept. 18, 2009, http://news.cnet.com/8301-13577_3-10357107-36.html; Tomio Geron, "Judge Approves Facebook's Privacy Settlement," *Wall Street Journal*, Mar. 19, 2010, Tech, http://online.wsj.com/article/SB10001424052748703580904575131742105971382.html.

[17] See Mike Musgrove, "Google E-Mail Ad Plans Raise Fears About Privacy," *Washington Post*, Apr. 2, 2004; John Markoff, "Google Sends a Message to Competitors," *New York Times*, Apr. 1, 2004.

[18] See Google Privacy Policy ("Information We Collect and How We Use It"), revised March 11, 2009, http://www.google.com/privacypolicy.html; Louise Story and Miguel Helft, "Google Buys Online Ad Firm for $3.1 Billion," *New York Times*, Apr. 14, 2007; Miguel Helft, "Google to Offer Ads Based on Interests," *New York Times*, Mar. 11, 2009.

[19] Pasquale, "Beyond Competition and Innovation"; see also Introna & Nissenbaum, "Shaping the Web."

[20] Google Corporate Information, "Company Overview," http//www.google.com/corporate/index.html.

[21] Carroll, "Creative Commons and the New Intermediaries," 59. The "semantic web" nomenclature originates with Tim Berners-Lee. See Berners-Lee, Hendler, and Lassila, "The Semantic Web."

[22] See Goldman, "A Coasean Analysis of Marketing."

[23] The classic statement of this argument is Winner, *Autonomous Technology*.

[24] See Kephart & Chess, "The Vision of Autonomic Computing"; IBM, *Autonomic Computing: IBM's Perspective on the State of Information Technology*, http://www.research.ibm.com/autonomic/manifesto/autonomic_computing.pdf. For a set of thought-provoking mediations on the philosophical and legal implications of IBM's project, see Hildebrandt & Rouvroy, *Law, Human Agency, and Autonomic Computing*.

[25] Zittrain, *The Future of the Internet*, 67-74.

[26] See ibid., 104-26.

[27] Ohm, "The Myth of the Superuser." For a representative analysis of the different subvarieties of hacking, see Skibell, "Cybercrimes and Misdemeanors."

[28] For perceptive accounts of this evolution, see Kerr, "Cybercrime's Scope"; Winn, "The Guilty Eye." The relevant provisions of the CFAA are 18 U.S.C. §1030(2) and (4).

[29] The access-control protections are codified at 17 U.S.C. §1201(a)(1)-(2); the prohibition on trafficking in devices for circumventing rights controls is codified at 17 U.S.C. §1201(b). For the legislative history, see House of Representatives Report No. 105–551, part 1, 17-19 (1998), reprinted in Melville B. Nimmer & David Nimmer (2000), *Nimmer on Copyright: Congressional Committee Reports on the Digital Millennium Copyright Act and Concurrent Amendments*, 5-1, 5-24 to 5-26; Senate Report No. 105-190, at 28-30 (1998), reprinted in Nimmer & Nimmer, ibid., 4-1, 4-33 to 4-35.

[30] See Universal City Studios, Inc., v. Reimerdes, 111 F. Supp. 2d 294, 317-19 (S.D.N.Y. 2000), *affirmed*, Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001).

[31] Digital Millennium Copyright Act, Pub. L. No. 105–304, 112 Stat. 2866 (codified at 17 U.S.C. §1201(f)). For examples of cases rejecting the interoperability defense for unauthorized media and game players, see Reimerdes, 111 F. Supp. 2d at 320; Davidson & Associates v. Jung, 422 F.3d 630, 641-42 (8th Cir. 2005).

[32] See U.S. Copyright Office, "Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies: Final Rule," 71 Fed. Reg. 68,472, 68, 476 (Nov. 27, 2006) (codified at 37 C.F.R. §201.40(b)(5)).

[33] See Katie Hafner, "Altered iPhones Freeze Up," *New York Times*, Sept. 29, 2007.

[34] See, for example, U.S. Federal Trade Commission, Staff Report, *Monitoring Software on Your PC: Spyware, Adware, and Other Software*, Mar. 2005, 2-4, http://www.ftc.gov/os/2005/03/050307spywarerept.pdf; Dave Morgan, Interactive Advertising Bureau, Testimony Before the Subcommittee on Commerce, Trade, and Consumer Protection on H.R. 964, "Securely Protect Yourself Against Cyber Trespass Act," U.S. House of Representatives, Committee on Energy & Commerce, Mar. 17, 2007, http://energycommerce.house.gov/images/stories/Documents/Hearings/PDF/110-ctcp-hrg.031507.Morgan-testimony.pdf.

[35] Dean, *Publicity's Secret*.

[36] See, for example, New York Times Co. v. U.S. Department of Defense, 499 F. Supp. 2d 501 (S.D.N.Y. 2007); American Civil Liberties Union v. F.B.I., 429 F. Supp. 2d 179 (D.D.C. 2006); American Civil Liberties Union v. U.S. Department of Justice, 265 F. Supp. 2d 20 (D.D.C. 2003).

[37] Freedom of Information Act, Pub. L. No. 89–554 , 80, Stat. 383 (codified as amended at 5 U.S.C §552(b)(1)-(7)).

[38] The statute authorizing the court is the Foreign Intelligence Surveillance Act, Pub. L. No. 95–511, 92 Stat. 1783 (codified at 50 U.S.C. §1801 *et seq*.). For the secrecy provisions, see 50 U.S.C. §1803(b). For examples of post-9/11 press coverage relatively critical of the secrecy surrounding the FISA court, see John Lancaster & Walter Pincus, "Proposed Anti-Terrorism Laws Draw Tough Questions," *Washington Post*, Sept. 25, 2001; Philip Shenon, "Secret Court Says F.B.I. Aides Misled Judges in 75 Cases," *New York Times*, Aug. 23, 2002. For examples of coverage more favorable to FISA following discovery of the Bush Administration's warrantless wiretapping program, see James Risen & Eric Lichtblau, "Bush Lets U.S. Spy on Callers without Courts," *New York Times*, Dec. 16, 2005; Neil King, Jr., "Senators Focus on Wiretapping Program," *Wall Street Journal*, Jan. 18, 2006.

[39] For decisions according trade-secret protection to search algorithms, see Viacom Intern. Inc. v. YouTube Inc., 253 F.R.D. 256, 259-60 (S.D.N.Y. 2008); Gonzales v. Google, Inc. 234 F.R.D. 674, 684-86 (N.D. Cal. 2006). On trade-secret protection for DRM protocols, see DVD Copy Control Association, Inc. v. Bunner, 31 Cal. 4th 864 (2003); and DVD Copy Control Association, Inc. v. Bunner, 116 Cal. App. 4th 241 (2004). The California Supreme Court ruled that enjoining defendant from distributing DeCSS over the Internet did not violate the First Amendment; on remand, however, the Court of Appeal vacated the injunction because the evidence showed that DeCSS already had been widely distributed to the public at the time the defendant posted it.

[40] The leading text on accountability for data-processing practices, the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), requires that individuals be given the right to inspect and correct data maintained about them, and requires disclosure of the purpose for which data processing is being conducted. See ibid., ¶¶9, 13, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

[41] Universal City Studios, Inc., v. Reimerdes, 111 F. Supp. 2d 294, 331-32 (S.D.N.Y. 2000), *affirmed*, Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001).

[42] See note 40 to Chapter 7, above.

[43] See Buzan, Waever, and de Wilde, *Security*, 21-42; Der Derian, "The Value of Security."

[44] Foucault, *Discipline and Punish*, 195-98.

[45] For a perceptive analysis, see Nissenbaum, "Where Computer Security Meets National Security."

[46] See, for example, Ellen Nakashima & Alec Klein, "U.S. Agency Tries to Fix No-Fly List Mistakes," *Washington Post*, Jan. 20, 2007; John Schwartz, "She Says She's No Music Pirate. No Snoop Fan, Either." *New York Times*, Sept. 25, 2003; John Schwartz, "High-Tech Voting System Is Banned in California," *New York Times*, May 1, 2004; Clint Ecker, "Massive Spyware-Based Identity Theft Ring Uncovered," *Ars Technica*, Aug. 6, 2005, http://arstechnica.com/old/content/2005/08/5175.ars.

[47] For a comprehensive discussion of the politics of network standards, see DeNardis, *Protocol Politics*.

[48] See 17 U.S.C. §1201(f), (g), (j). For an analysis of the ways that the DMCA works to prevent "disruptive innovation," see Seltzer, "The Imperfect Is the Enemy of the Good."

[49] See Castells, *The Power of Identity*; Castells, *The Rise of the Network Society*; Deleuze, *Negotiations*; Baudrillard, *Simulacra and Simulation*; see also Galloway & Thacker, *The Exploit*.

[50] Madison, "Complexity and Copyright in Contradiction"; see also Kang & Cuff, "Pervasive Computing," 122-28. On the tension between order and vibrancy in urban planning, see generally, Jacobs, *The Death and Life of Great American Cities*; Lang, *Creating Architectural Theory*.

[51] See Andrejevic, *iSpy*; Haggerty & Ericson, "The Surveillant Assemblage."

[52] Coombe, *The Cultural Life of Intellectual Properties*; McGrath, *Loving Big Brother*.