7

"Piracy," "Security," and Architectures of Control

The changes produced by the ongoing expansion of copyright and the broadening and deepening of surveillance are not just legal changes. The perceived imperatives of piracy and security are catalyzing major realignments in the structure of the networked information society. In an effort to control flows of unauthorized information, the major copyright industries have pursued a range of strategies designed to distribute copyright enforcement functions across a wide range of actors and to embed those functions within communication networks, protocols, and devices. Meanwhile, in an effort to provide security against a variety of perceived threats, ranging from terrorism to fraud to identity theft, governments and private actors have moved to extend surveillance and authentication capabilities across an equally wide range of actors and instrumentalities. In aggregate, these realignments seek to produce architectures of control: configurations that define in a highly granular fashion ranges of permitted conduct.

Legal scholars have analyzed the emergence of digital architectures of control primarily through the prism supplied by Lawrence Lessig in *Code and Other Laws of Cyberspace*. Lessig sought to draw attention to the ways in which code shapes behavior across a variety of domains; to underscore the point, he asserted that code "is" law. Importantly, however, Lessig did not characterize code as the only or most important regulator of online behavior, but rather described it as one of four regulatory "modalities"—law, code, norms, and the market—that can work singly or in combination. In a diagram that forms the theoretical backbone of *Code*, he depicted the four modalities as Newtonian "forces" acting to shift individual behavior this way or that.[1] Most legal scholars who write about the networked information society have adopted this taxonomy and overall approach, and have focused on elaborating the interactions of the vectors that Lessig specified.

Scholarly responses to emerging architectures of control fall into three general categories. Scholarship in the first category takes seriously Lessig's metaphoric equation of code with law, and attempts to assess emerging digital architectures of control using the standards that would be applied to proposed legal regulation, particularly laws affecting freedom of expression. Scholarship in the second category rejects the metaphoric equation of code with law because of code's origin in private behavior. These scholars analyze code as an exercise of economic liberty; code is not law, they argue, but rather the market in action. Scholarship in the third category argues that code is different enough

from law that we should consider it unique. On this view, regulation by code raises new possibilities, challenges, and dangers.

Each of these approaches has produced important insights, but each also suffers from the same general defect identified in Chapters 3 and 5: constrained by the commitments of liberal political theory, legal scholars frame code's origins and effects in simplistic and unrealistic ways. To the extent that it offers the vectors of law, code, market, and norms as ontologically distinct tools capable of deployment by disinterested, autonomous regulators, the *Code* framework lends itself to precisely this sort of oversimplification. The architectures of control now emerging within information networks are embedded within broader changes in patterns of social ordering in the emerging information society. *Code*'s four regulatory modalities are resources available to be harnessed, sometimes singly but more often in combination, in the service of particular agendas advanced by socially embedded actors.[2] Moreover, those actors deploy additional resources that the *Code* framework does not encompass.

The Emergence of Architectures of Control

We do not live—yet—in an information society thoroughly pervaded by architectures of control. Architectures of control are emerging gradually, in a piecemeal, uncoordinated fashion, at points where the interests of powerful institutional actors align. Nor are architectures of control the result of any grand, sinister master plan; this will not be a conspiracy story. Where such architectures are emerging, they reflect an inclination that is far more deeply rooted and mundane: the desire to use information and information technologies to manage risk and structure risk taking.

Prologue: "Computer Fraud and Abuse"

The story of the emergence of architectures of control begins in the 1980s, with the first efforts to develop laws regulating access to computers and computerized information. For centuries, information about people and about corporate and government operations was maintained on paper and processed by hand. The 1970s and 1980s saw the rise of large computer systems capable of maintaining, sorting, and processing large repositories of information, controlling industrial machinery, and directing the operation of communication networks. This "control revolution" created new challenges for law- and policy makers unaccustomed to thinking about information and information processing as subjects of regulation beyond the limited framework provided by intellectual property laws.[3]

To an extent, existing law supplied templates for allocating rights in the information stored on computer systems. By analogy to existing common-law privacy protections, some types of information about identified individuals might be the subject of a cognizable privacy interest. Many important pieces of privacy legislation, including the federal Privacy Act, date from this period. Alternatively, some (though not all) data or algorithms stored on a computer might be protected as trade secrets.

In many cases, however, whether or not a trade-secrecy claim or a privacy claim might be made, there was a problem that existing laws did not address: the threat of unauthorized access that might compromise the security of the system. By the 1980s, Congress concluded that the time had come for legislation addressing unauthorized access. The Computer Fraud and Abuse Act of 1984 (CFAA) set forth a variety of prohibitions targeting unauthorized access to computer systems designated as "protected." Initially, the CFAA's most stringent protections applied to computers used by the federal government or by financial institutions. Subsequent amendments prohibited unauthorized access to other computers where such access was undertaken knowingly and with intent to defraud or was undertaken intentionally and resulted in the destruction or alteration of information. In 1994, Congress expanded the CFAA's scope substantially, criminalizing a variety of additional actions with respect to non-government computers, including unauthorized access that results only in the use of computer time (above a minimum dollar value) and the knowing transmission of viruses and other programs that cause damage.[4]

The CFAA's core criminal prohibitions—those targeting malicious or knowing damage to computer systems and networks—have enabled the federal prosecution and conviction of individuals who deliberately compromise the technical security of information systems or who use their insider status to violate rules of confidentiality. But the post-1994 CFAA also criminalizes a much broader range of conduct on a much thinner showing of intent. In addition, courts have defined the evidence of harm needed to satisfy the statute's $5,000 minimum in a way that enables nearly any violation to be charged as a felony.[5]

In addition, the CFAA's civil provisions have been invoked in cases involving a variety of Web-based activities that the drafters did not contemplate at all. Typically, defendants in such cases have gained access to information that is publicly available on the Internet in ways that the site proprietor dislikes—by using "deep linking" to extract information rather than proceeding through the "front page," or by using automated tools to crawl a site repeatedly in search of up-to-the-minute pricing information. Often, the site proprietor has posted notices, in English or in computer code, indicating that it prohibits the conduct in question. In such cases, the CFAA is deployed as a species of unfair-competition regulation, defining the limits of appropriate behavior with respect to publicly available data according to the data provider's dictates.

Within less than a decade, however, it became apparent that the CFAA had almost nothing to say about many other situations involving online conduct, and nothing at all to say about the appropriate uses of networked information technologies as tools for regulation of individual behavior. Those situations have engendered different and far more complicated sets of regulatory responses.

Pervasively Distributed Copyright Enforcement

In an effort to prevent online copyright infringement, the major copyright industries have developed and aggressively pursued a portfolio of strategies designed to enforce control of copyrighted content at multiple points in the network. This regulatory regime relies on a range of tools, including technologies that restrict the range of permitted information use, contractual regimes for authorizing "compliant" implementations of those technologies, legal prohibi-

tions against interfering with the resulting technical-contractual regimes, other legal rules broadly distributing responsibility for policing communication networks, and publicly inculcated norms of appropriate user behavior. I classify these strategies into six groups according to the behaviors that each group primarily targets.

The earliest strategies for protection of digital content revolved around "surface level" implementation of automated restrictions on digital content.[6] Surface-level restrictions—variously known as copy-protection technologies, technical protection measures (TPMs), and digital rights management (DRM)—operate at the level of individual media files and restrict the actions that users may take with the files. They are developed and implemented at the application level and in freestanding consumer electronics equipment, via licensing processes coordinated by copyright interests and their designated technology partners. Within these technical-contractual regimes, the relevant technical standards are held as trade secrets. Licensees recruited into the regimes must agree to preserve secrecy, and their implementations of the standards must satisfy associated criteria of robustness.

Surface-level protection strategies have produced some notable failures, but also some notable successes. The most highly publicized and widely criticized efforts to implement surface-level technological restrictions occurred within the recording industry. Users, accustomed to unrestricted recording and copying, resented the experiments. New copy-protection systems for recorded music were hacked almost as rapidly as they appeared, and industry efforts to develop a universal, more robust standard for the technical protection of digital audio files failed. A more successful example of surface-level technological restriction is the encryption system built into DVD players and incorporated in all prerecorded DVDs. Technical rules blocking copying are enforced by other technical rules that prohibit play on any noncompliant media player. The system was developed by a consortium of the major studios and is currently administered and enforced by a private membership association, the DVD Copy Control Association (DVD-CCA), that licenses the technology. This regime's success is not due to its technical efficacy in any absolute sense. The copy-protection algorithm, known as the Content Scramble System (CSS), has been broken, and the decryption algorithm, known as DeCSS, is widely available on the Internet if one knows where to look. Most people don't do this, though, and this appears to be a function of two related factors: the technology's universality and its perceived normalcy. Because the deliberately designed limitations have been in place from the moment that DVD players were first marketed to consumers, the operation of the regime administered by the DVD-CCA is effectively invisible; to most end users, it is "just the way things are."[7]

A second, more durable set of strategies for pervasively distributed copyright enforcement has targeted third-party technology companies whose products and services are perceived to facilitate particularly high levels of infringement. In broad brush, this campaign has two complementary goals. First, it seeks to keep protected content protected. In the United States, the primary vehicle for accomplishing that goal is the Digital Millennium Copyright Act (DMCA), which penalizes circumvention of technological measures that effectively control access to copyrighted works and bans the manufacture and distribution of technologies that might enable copyrighted content to be stripped free

of its protective wrapping.[8] Second, the campaign targeting third-party technology companies seeks to minimize the availability of tools for reproducing, distributing, and manipulating unprotected content. Equipment and services that give users that freedom—including digital video recorders, digital music players, and CD and DVD burners—work at cross-purposes with the effort to shift the market toward protected content. In an effort to assert control over these segments of the technological marketplace, copyright proprietors have invoked a set of doctrines within copyright law that create secondary liability for facilitating copyright infringement. For many years, the doctrinal structure governing secondary copyright liability effectively shielded providers of multipurpose technologies, but the entertainment industries have deployed a carefully designed litigation strategy to erode the certainty that the law formerly provided.[9]

Legal prohibitions do not physically or electronically prevent the spread of unprotected content or circumvention tools, and for that reason some consider them ineffective. For example, the DMCA did not prevent the development and widespread Internet distribution of DeCSS, the unauthorized algorithm that decrypts prerecorded DVDs. For would-be legitimate providers of digital media equipment and services, however, the potential costs of violating the prohibitions are significant. The content industries have filed a steady progression of lawsuits against technology companies for facilitating infringement or interfering with technological protection measures. Such litigation is widely perceived as deterring both innovation by technology developers and investment by venture capitalists. The potential costs of litigation also have affected independent researchers who study the technological systems that the DMCA protects; many such researchers report having changed their research programs to avoid legal conflict.[10]

The third set of strategies for pervasively distributed copyright enforcement seeks to move automated enforcement functions progressively deeper into the logical and physical layers of the user's electronic environment. Such "trusted system" efforts are, and are designed to be, far more impervious to hacker workarounds. They are also far more inhospitable to unauthorized technologies that an independent third party might seek to market. They are, however, far more complicated to implement. Successfully operationalizing trusted-system functionality across the broad range of personal computing and consumer electronic equipment now in use requires the cooperation of major sectors of the software, computer, and communication industries. So far, the track record of these initiatives is mixed.

The most hotly debated aspect of trusted-system strategies for pervasively distributed copyright enforcement has concerned the role of government in coordinating their implementation. For example, after early efforts to secure a private consensus on trusted-system standards derailed, the entertainment industries requested that government enact new laws mandating the development and adoption of content-protection standards. In the United States, an initial effort to secure a broad mandate covering all computing and consumer electronics equipment failed when the technology industries refused to support it. In the wake of that failure, both content and technology industries advanced narrower proposals, including a "broadcast flag" for digital television content, a parallel regime for digital audio broadcasts, and a proposal that would mandate the watermarking of broadcast content to prevent broadcasts recorded using analog

technologies from being digitized. No proposal has yet become law, but new bills are regularly introduced in Congress, and the Federal Communications Commission (FCC) has issued a trusted-system rule that covers the set-top boxes supplied by cable companies.[11] The European Commission also has signaled its desire to encourage the development of trusted-system technologies.[12]

Exclusive focus on the question of technology mandates, however, ignores the extent to which trusted-system initiatives continue to move forward in the private sector. Some focus on implementing controls at the operating-system layer, while others seek to hard-wire trusted-system functionality into every kind of equipment that users might employ to access copyrighted content. Some are offered by a single firm, such as Intel's Trusted Execution Technology, which provides "a highly versatile set of hardware extensions to Intel® processors and chipsets that, with appropriate software, enhance the platform security capabilities."[13] Other efforts to develop and implement trusted-system controls are more collaborative, such as the Trusted Computing Group (TCG), an organization that focuses on personal-computing platforms; the Digital Media Project, which seeks to develop standards for moving protected content across different consumer platforms; and the Copy Protection Technical Working Group, a broad-based industry effort to coordinate the development of standards for digital broadcasting. The most recent generation of trusted-system initiatives incorporate cloud-based storage of digital media content. An example is Sony's Digital Entertainment Content Ecosystem, a set of protocols for delivering stored content to users via authenticated devices and platforms.

The fourth set of strategies for pervasively distributed copyright enforcement targets third-party providers of network services, such as Internet service providers (ISPs) and search engines, that play a vital role in the distribution of online communications, including both protected and unprotected content. ISPs serve as gatekeepers for most online conduct by users, while search engines, social-networking platforms, and other sites that host user-generated content play an analogous gatekeeping role in the processes of online search and retrieval. In 1998, as part of the DMCA, the U.S. copyright industries won passage of legislation establishing a "notice and takedown" procedure under which online service providers may maintain immunity from monetary liability by promptly removing material called to their attention by copyright owners.[14] The content industries have made aggressive use of the notice-and-takedown procedure, using automated detection tools to comb the network for unprotected content and generate large numbers of takedown notices. Both the legal merit and the accuracy of the notices are hotly disputed; one recent study found that more than 30 percent of notices presented questionable claims of infringement and many more were technically flawed.[15] Generally, however, online service providers comply with takedown notices in order to avoid litigation; this shifts the burden to users to show lawful use before the material can be restored.

The DMCA's notice-and-takedown provisions do not apply to service providers based outside the United States, nor do they apply to entities that merely serve as passive conduits for Internet traffic routed from non-U.S. locations. Nonetheless, the statute contains a separate, little-discussed provision authorizing injunctive relief against a service provider to block access to a specific location outside the United States. In at least one case, the entertainment

industries have successfully invoked this provision to encourage "conduit" service providers to close national borders to allegedly infringing traffic. In 2002, the recording industry sued to require providers of Internet backbone service to block access to Listen4Ever, a China-based Web site offering copyrighted music files for download. The Listen4Ever site "disappeared" shortly thereafter, and the industry dismissed the suit.[16]

The DMCA also does not require automatic filtering, but the copyright industries have leaned heavily on Internet intermediaries to adopt protocols designed to screen out infringing content. They have pressured popular content aggregators like YouTube and MySpace to implement automated filtering protocols for "user-generated content," and have pressured ISPs to identify and block traffic over popular peer-to-peer (P2P) networks. The actions of users at a nonprofit educational institution may not be attributed to the institution unless it is on notice of a pattern of infringing conduct, but the copyright industries have stepped up efforts to provide such notice and have provided universities with automated tools for processing takedown notices and disabling student access to P2P networks. In 2008, copyright interests secured passage of legislation conditioning the availability of federal financial aid on an institution's development of "plans to effectively combat the unauthorized distribution of copyrighted material, including through the use of a variety of technology-based deterrents."[17] All these efforts have borne fruit; although neither for-profit entities nor universities have filtered as aggressively as the content industries might wish, some amount of automated filtering is fast becoming the norm.

More recently, the copyright industries have begun pressuring ISPs to adopt so-called three-strikes programs for terminating users' Internet access. In France, entertainment interests won enactment of legislation that authorizes judges to issue termination-of-service orders. Parallel efforts on the European Union level, however, have not succeeded.[18] In the United States, the Recording Industry Association of America (RIAA) has focused principally on seeking private agreements with ISPs. In 2008, it announced a formal program to pursue the consensual implementation of three-strikes policies. The details of that program and any ensuing agreements are still unknown.[19]

The fifth set of strategies for pervasively distributed copyright enforcement consists of efforts directed at changing end-user behavior. Between 2003 and 2008, the RIAA and the Motion Picture Association of America (MPAA) filed thousands of so-called John Doe lawsuits against anonymous file traders. This procedural tactic enabled them to request the issuance of subpoenas to the ISPs whose services were used to access the Internet. The subpoenas requested identification of the subscribers to whom particular Internet Protocol addresses were assigned at the specified times. The RIAA established a settlement service center to process claims against identified users, offering them a choice between a confidential, relatively small monetary settlement and public financial ruin. Most defendants quickly settled, but the RIAA eventually concluded that the campaign's costs, including harm to consumer goodwill, outweighed its benefits. In 2008, it announced that it would suspend its end-user litigation campaign to focus on ISP-level initiatives.[20] Motion picture copyright owners have continued to sue individual users.[21]

The sixth and final set of strategies for pervasively distributed copyright enforcement operates entirely on the rhetorical level and seeks to mold

public awareness of copyright issues. Entertainment industry representatives have deployed a variety of rhetorical tropes designed to position online copyright infringement, and particularly P2P file sharing, as morally objectionable and socially insidious. In a blizzard of press releases and media interviews, and in more formal settings ranging from conference addresses to congressional testimony, they have equated online copyright infringement with theft, piracy, communism, plague, pandemic, and terrorism. In an effort both to boost demand for trusted-system functionality and to shore up support for government-imposed technology mandates, they have also linked P2P file sharing with the spread of pornography and with increased risk of exposure to viruses and spyware.[22] Meanwhile, they have created and distributed (free of charge) curriculum materials for grades K–12 to introduce students to copyright rules.[23]

Pervasively distributed copyright enforcement is a work in progress; its constituent strategies are evolving and hotly contested. It is worth careful study, nonetheless, both in itself and for what it may come to represent. In aggregate, it works systematically to shift the locus of control over intellectual consumption and communication away from individuals and independent technology vendors and toward purveyors of copyrighted entertainment goods. This shift has consequences for information policy that are as large as any dictated by copyright law's system of entitlements and exceptions. More broadly, pervasively distributed copyright enforcement also suggests a template for architectural and legal realignment to serve other imperatives. In fact, such a shift is also underway, catalyzed by perceived threats to national and commercial security.

(In)Security Everywhere

Although the strategies of pervasively distributed copyright enforcement are diverse, they have a common purpose. This section, in contrast, considers regulatory strategies directed toward a heterogeneous group of issues that are perceived as falling under the general heading of "security." These strategies involve a larger group of actors, and some can appear to work at cross-purposes with others. When they are considered as a group, however, common themes emerge. Architectures designed to promote security are driven by a shared logic. According to that logic, security is promoted by pervasively embedding technologies and protocols for identification and authentication; by cross-linking those capabilities with pervasive, large-scale information collection and processing; and by promoting related (though arguably inconsistent) norms of ready disclosure and unceasing vigilance.

The first set of strategies concerns the monitoring of movement in physical space. State sovereigns have always taken an interest in traffic across their borders, but the development of networked information technologies has enabled them to exercise that interest much more systematically. For decades, border officials have cross-referenced international travelers' identification documents against database records of known or suspected criminal activity. Most recently, those records also include biometric information, collected from all travelers to the United States under the auspices of the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program. A similar program is used in Japan, and several other countries are moving toward implementation of biometric screening programs.[24]

Within the last decade, and in the United States more particularly after the terrorist attacks of September 11, 2001, government entities have extended their interest in mobility to encompass movement within public spaces. Annual reports on privacy and human rights prepared by the Electronic Privacy Information Center and Privacy International document the use of video surveillance systems in countries around the world.[25] In major U.S. cities and at government buildings and mass transit hubs, surveillance cameras maintained by federal, state, and local authorities are increasingly an ordinary feature of the landscape. In addition, the U.S. Department of Homeland Security funds the installation of surveillance cameras along national borders and in many rural communities that have requested them.[26]

The extension of video surveillance throughout public spaces intersects with a trend toward the privatization of gathering places. Many spaces that appear public—ranging from courtyards in downtown business districts to suburban shopping malls—are in fact privately owned. To an increasing extent, those spaces are subject to video surveillance by their owners. Although the fact of surveillance is often disclosed, private surveillance networks generally are not subject to due process or disclosure requirements. Private does not equal secret, however. Video records held by private operators are subject to production via the legal process and to compulsion by government investigators. More generally, the combined reach of private and public cameras creates many areas in which visual surveillance becomes difficult to avoid.[27]

A second set of strategies seeks to extend and routinize surveillance of networked digital communications. Governments have long been able to monitor telephone conversations, but the basic architecture of the Internet made e-mail much more difficult to intercept. That has changed. Sophisticated tools now exist for inspecting data packets in transit, for monitoring wireless transmissions, and for locating wireless users. Other legal changes enlist network intermediaries in communications monitoring. The Communications Assistance to Law Enforcement Act of 1994 (CALEA) required telecommunications carriers to implement surveillance capabilities that could be activated "expeditiously" following receipt of a properly authorized request from law enforcement. By FCC ruling, CALEA's requirements were subsequently extended to wireless carriers, broadband pager-service providers, and voice-over-Internet providers.[28] The Foreign Intelligence Surveillance Act (FISA) grants the government surveillance authority beyond that conferred by CALEA, and proceedings under FISA are conducted in secret. As is now well known, in the years following the September 11 attacks, the government conducted additional, extensive warrantless wiretapping without resort to FISA.[29] Last but hardly least, numerous sources suggest that agencies within the federal government, including the National Security Agency and the Central Intelligence Agency, engage in large-scale pattern analysis of telephone, e-mail, and World Wide Web traffic.[30]

Yet the push toward surveillance of networked communications is not entirely government directed. ISPs have shown increased interest in examining their own traffic for a variety of reasons—pressure from content owners seeking to enforce copyrights, desire to monetize and prioritize their own proprietary services, and heightened sensitivity to bandwidth usage. A steady stream of incidents suggests that ISPs are actively experimenting with various network

surveillance techniques.[31] For many years, the telecommunications industry successfully exerted its lobbying and litigation power to block the issuance of "net neutrality" regulation that would prevent Internet access providers from implementing methods of discriminating among different types of network traffic; as of this writing, it is pressing Congress to prevent a partial neutrality mandate issued by the FCC from taking effect.[32]

The third set of strategies relates to the processing of information about individuals and groups. Within the United States, both federal and state governments now routinely use data mining and profiling technologies to identify suspected threats. Heightened public awareness of racial and ethnic profiling has put pressure on law enforcement to explain and justify the ways that it assesses potential threats to safety. For the most part, the official response to complaints about profiling's discriminatory effects has been a push toward "better" profiling with more precise information. Data-mining initiatives gain added momentum as they become linked to strategies in the first two groups; it is logical to think that surveillance of movement across borders, within public spaces, and across communication networks enhances security more effectively when it is supplemented by good information about risks. Some government data-mining efforts, such as those used to identify potential threats to airline safety, have engendered widespread public opposition. Others, such as a series of recent initiatives to enhance networking and data sharing among state law enforcement agencies by establishing so-called fusion centers, have drawn less attention.[33]

Although government data-mining activities are extensive, they are dwarfed in both scale and scope by data-processing activities occurring in the private sector. Because U.S. data-privacy law is relatively permissive, the United States has become the center of a large and growing market for personal information, encompassing all kinds of data about individual attributes, activities, and preferences. Trade in some information, such as financial and health information, is subject to legal restrictions, but most other types of information flow freely among participants ranging from large financial institutions to search engines to divorce attorneys and private detectives. Flows of data are facilitated by corporate data brokers like ChoicePoint, Experian, and Axciom. To help companies (and governments) make the most of the information they purchase, an industry devoted to data mining and "behavioral advertising" has arisen; firms in this industry compete with one another to develop more profitable methods of sorting and classifying individual consumers. In Europe, where data-protection laws are stricter, there is less private-sector trade in personal information, but also more government freedom to collect and store data about citizens.

Government and private-sector record-keeping and data-mining activities are increasingly intertwined. In the United States, a number of federal agencies have awarded multimillion-dollar contracts to corporate data brokers to supply them with personal information about both citizens and foreign nationals.[34] In addition, the government routinely uses subpoenas to acquire particularized information about named individuals from private-sector entities. Personal voice and e-mail communications are subject to statutory protections against routine disclosure, but governments in the United States and Europe

have imposed data-retention mandates on telecommunications providers so that communication information is preserved for later, particularized acquisition.[35]

The fourth set of strategies seeks to distribute protocols for real-time identification and authentication of individuals across a wide range of devices, and to make their use both widespread and routine. This strategy gains added momentum as it becomes linked with strategies in the first three groups; information about real or perceived risks generated through data mining or through the monitoring of movement and communications is most useful when it can be linked to its subjects in real time. Here again, the lion's share of public attention has been devoted to federal initiatives to impose uniform identification and authentication protocols. The track record of such efforts is mixed. In the United States, efforts to move toward a universal identification framework seem, for now, to be failing. Despite repeated extensions of the federal deadline to comply with so-called Real ID requirements (mandated by the Real ID Act of 2005), few states have taken meaningful steps to comply.[36] More narrowly targeted identification requirements have enjoyed greater success. Since 2006, all newly issued U.S. passports include RFID chips that can be scanned by border officials to authenticate the passport and view information about the holder's identity. Worldwide, many countries have universal identification systems, and use government identity numbers for a variety of purposes ranging from tax administration to the provision of welfare benefits.

As before, the focus on government identification initiatives has caused many to overlook the considerable advances of private-sector technologies for authenticating identities and matching them to locations and activities. Global-positioning-system technologies in cars and networked personal devices enable users to locate themselves, but also enable them to be located. Highway toll transponders and transit-system smart cards create records of individual movement. Biometric identifiers are used in many corporate facilities, and have become a popular feature in laptop computers and data-storage devices. PIN codes are ubiquitous and create persistent records of individual transactions. The widespread use of information-based authentication and the resulting heightened risk of identity theft create pressures for even more identification and authentication. With respect to information exchanged across digital networks, the demand for authentication-based security against viruses, spyware, and spam has become a powerful force driving the development of trusted-system functionality. Many innovations in the trusted-system domain are directed principally toward threats from malware and only secondarily toward copyright enforcement. For example, the newest version of the Internet Protocol, IPv6, includes a so-called stateless mode that facilitates persistent identification of Internet users, and was designed to enable secure transactions.[37]

Although strategies for real-time identification and authentication dovetail with the push toward expanded surveillance of border traffic, public spaces, and traffic across communication networks, many private-sector authentication tools have been positioned in the marketplace as serving goals and desires beyond security. In an increasing number of contexts ranging from online shopping sites to intercity highways to airport-security screening lines, "preferred customer" authentication has become a commodity that can be purchased. Data from such authentications feeds back into the data-mining economy, enabling detailed analysis of preferred customers' desires. Technical developments in

trusted-system functionality, such as Microsoft's new program of server-level authentication for popular software applications, are positioned as vehicles for portability in an age of mobile networked devices.[38] By making authentication a condition of access to resources stored on the network, such programs can generate detailed profiles of information use.

The fifth set of strategies is directed at the ordinary people who are the subjects of enhanced security measures. While user-directed strategies in the copyright context simply seek to deter unauthorized file sharing, those in the security context are far more complex, reflecting the fact that every person is simultaneously the target of, a necessary participant in, and a potential consumer of enhanced security measures. Some user-directed strategies are straightforwardly hortatory, directed toward recruiting individual citizens to join the corps of watchers seeking to prevent acts of terrorism. Although efforts to fund a formal program aimed at enlisting the general public as the government's eyes and ears have failed, other, more informal initiatives remain in effect. Metro transit authorities in New York City and Washington, D.C., exhort their riders, "If you see something, say something." An eclectic assortment of state and local law enforcement initiatives has enlisted members of the public in surveillance efforts that range from trolling Internet chat rooms for child predators to monitoring illegal border crossings.[39]

Other user-directed strategies seek to inculcate appropriate beliefs about personal information management. The emerging regimes of pervasively distributed security and authentication depend on the ready availability of large quantities of personal information. It is important, therefore, that individuals continue to provide those regimes with the information that they require. Nurturing the optimal blend of vigilance and compliance requires educating members of the public to understand their own disclosures as essential to the purchase of both security and convenience. Thus, for example, one can protect one's credit rating by laboriously gathering reports from each credit agency and navigating the complex processes the agencies make available to resolve discrepancies, or one can subscribe to a third-party monitoring service simply by giving that service carte blanche access to information about one's credit history. The inevitable and often spectacular failures of systems put in place to ensure commercial security tend to be understood as demonstrating the need for still more disclosure so that more tightly controlled authentication can succeed.

As in the copyright context, the sixth and final set of strategies involves the use of rhetoric to shape public opinion on issues related to terrorism, identity theft, and other security threats. Rhetoric about terrorism also invokes threats to the health of the body politic; if copyright infringement is a pandemic, global terrorism is a "cancer" or "virus" that demands comprehensive, drastic immunotherapy.[40] The color-coded threat-alert system promulgated by the Homeland Security Department, modeled on air-quality alert systems that have become commonplace in most major U.S. cities, works to foster continual background awareness of looming, deadly dangers.[41] Notably, comparable metaphors are largely absent from the official discourse about data protection and identity theft, which proceed chiefly in the language of consumer protection and risk management. Panic about the security of personal information would work at cross-purposes with norms of disclosure that feed the operation of security-related technologies and protocols. Private-sector and nonprofit

data-security advocates, however, sometimes use the "epidemic" metaphor as a way of emphasizing the magnitude of these problems.

Like pervasively distributed copyright enforcement, pervasively distributed security protocols are a work in progress. What is notable, though, is the extent to which different kinds of protocols emerging in different market and government sectors tend to overlap and reinforce one another, creating a broadly distributed web of authentication points for authorizing transactions and communications and deep reservoirs of information about the behaviors of individuals and groups. As the protocols and associated business models and legal regimes continue to evolve, coming into increased alignment with one another, the gaps in that web become progressively smaller.

Technology as/and Regulation: Is *Code* the Answer?

Within legal scholarship, theoretical frameworks for understanding the emergence of architectures of control all begin with Lessig's *Code*, which has organized legal thinking about the regulatory impact of networked information technologies for the past decade. *Code* was and remains a visionary statement—an effort to name a potent force that legal theory had failed to recognize. Drawing together and systematizing a set of insights that had gradually been emerging within the legal literature, Lessig sought to emphasize both the importance of materiality—of the architecture of the built world—and the regulatory complexity that results from taking materiality into account. At the same time, however, the regulatory framework outlined in *Code* remains situated squarely within the conceptual landscape of liberal political theory. In Lessig's diagram of regulatory modalities, the subject of regulation is the liberal subject: a solitary, undifferentiated dot who interacts with regulatory forces that stand out in sharp relief against an empty background.[42] That framing usefully drew legal scholars' attention to the regulatory significance of digital architectures, but it has hindered efforts to describe and theorize the relationship between code and governance.

Within the framework that *Code* established, the two dominant strands within liberal legal theory seem to offer two principal choices for evaluating the regulatory effects of emerging digital architectures. If code is "like" law, then liberal rights theories suggest that its legitimacy should be assessed by interrogating its effects on the various liberties that traditionally have concerned legal scholars and policy makers. Alternatively, if code is more fundamentally the product of private innovation—a creature of the market and of market-driven standards processes—then perhaps its legitimacy should be assessed in the same ways the law typically evaluates other market processes. Within the tradition of liberal legal theory, and particularly within economic theory, that approach requires a default posture of deference to market processes and a suspicious stance toward government intervention.

Under either approach, however, the precise nature of the relationship between code and human freedom has proved elusive, in large part because of the way that liberty is understood within liberal theory. The prevailing conception of liberty as the absence of constraint is not particularly useful for describ-

ing the ways in which different digital architectures affect the experiences of network users. The foundational assumptions underlying arguments from market liberty, meanwhile, do not describe the conditions that actually exist in markets for the technologies that constitute architectures of control.

A few scholars argue that code is not like either law or markets. Their work usefully draws our attention to the ways that code differs from regulatory tools more familiar to legal scholars. At the same time, however, scholars who analyze code as unique give insufficient attention to code's socially embedded nature—to the institutions and actors seeking implementation of architectures of control and to the mechanisms by which those architectures gain market share and popular legitimacy. As a result, they oversimplify the sort of governance that code represents.

Code, Law, and Liberty

If code is like law, then within the framework of liberal rights theory, the most important questions to be asked about it concern its effects on protected liberties. Civil libertarian analyses of code have a variety of starting points; some scholars focus on property rights, while others are more concerned with code's effects on expression and other personal liberties. Lessig himself takes the latter approach, posing repeated questions about how code affects the freedoms traditionally guaranteed by the Bill of Rights. In general, however, the conceptions of liberty and constraint on which these analyses rely are too binary and abstract to be helpful in assessing what architectures of control actually do. Meanwhile, the metaphors used to discuss architectures of control suggest that those architectures structure experienced space in ways that the liberty/constraint binary does not capture.

Liberal theorists who stress the sanctity of property rights argue that architectures of control simply reinforce prerogatives of ownership.[43] On this account, circumventing a copy-protection device is no different from breaking into a locked house, and owners of digital property may legitimately impose terms that involve collection, retention, use, and sale of personal information as conditions of licensed access. Within a property-rights framework, moreover, personal information floating unclaimed in the public domain is there for the taking. Other property scholars argue that these arguments reserve to the property owner a despotic dominion that is absent in the real world. In the real world, property rights are complicated, interdependent creatures, hedged about with exceptions and conventions. To take one small example, we knock on one another's front doors all the time without invoking or even thinking of legal rules about trespass.[44] So too, they argue, with technological self-help; invoking property interests does not inevitably lead to the conclusion that a property owner can do anything it pleases to protect those interests. But theorists who advance a more moderate conception of digital property rights struggle to locate within the boundaries of property theory principles that can explain exactly when such behavior becomes objectionable.

Scholars who focus on expressive liberty argue that emerging architectures of control stifle individual freedom of expression. This is so, they claim, because architectures of control artificially restrict uses of digital content and foreclose the possibility of anonymous self-expression.[45] Freedom of expression also has become the conceptual fulcrum of a litigation campaign challeng-

ing the DMCA's prohibition on devices for circumventing technical protection measures applied to copyrighted works. Neither scholars nor litigators, though, can easily explain what types of architectural constraint would be legitimate within a freedom-of-expression framework. The argument from property rights cuts the other way, moreover. In the real world, private property rights frequently trump speech rights, and copyright owners assert that this rule should apply in disputes about digital property as well.

As this brief summary suggests, both property and speech arguments about digital architectures share some peculiar characteristics, beginning with the confident assumption that one or the other discourse can be made to generate definitive rules for resolving disputes about how much control is too much. Neither property theory nor speech theory definitively resolves questions about the permissible extent of architectural control. More fundamentally, both property-based and speech-based arguments about architectural effects on liberty take as their baseline a conception of liberty that is foundational to liberal political theory, but that maps poorly to the reality of the networked information environment: the conception of liberty as consisting in the absence of constraint, exercised by the autonomous self that remains after social shaping is stripped away. To say that code constrains that sort of liberty is not, in the end, to say very much at all. Physical architectures and human-designed artifacts constrain that sort of liberty, too. Autonomy-based conceptions of liberty therefore cannot help us determine what makes particular architectural configurations desirable or undesirable.

Some scholars, whom I will call the "code libertarians," attempt to avoid the problem of liberty and constraint altogether. They agree that the decentralized, loosely coordinated strategies that I have described evidence intent to restrict freedom of expression, but argue that individual liberty will prove impervious to architectural control. The crux of this argument is the gap between regulatory ambition and technical feasibility. Surely, argue these scholars, it is going a bit far to say that these developments strip people of whatever agency they possess. If we are to take individual freedom seriously, we also must take seriously the individual capacity to resist control that seems unjust. Working from that premise, the code libertarians reason that if new architectural obstacles to resistance and appropriation appear, people will find ways around them. If the new order is this bad, people will refuse to accept it, and if it is foisted upon them, they will sabotage it.[46]

In the literal sense, the code-libertarian argument about the effect of digital architectures on individual liberty is quite right. Technically sophisticated observers agree that a certain amount of uncontrolled copying of unprotected content will always evade the content industries' reach. That argument traces its roots to an important paper advancing what has become known as the "darknet hypothesis," which posits that "any widely distributed object will be available to some fraction of users in a form that permits copying."[47] While it may be a mistake to assume that copy protection on all works will be broken, the darknet hypothesis suggests at minimum that some copy protection will be.[48] For similar reasons, technically sophisticated commentators also tend to believe that efforts to impose perfect surveillance are doomed to failure. Well versed in techniques for withholding personal information, they argue that such techniques are available to anyone who wants them and will become widely

used if people come to perceive demands for personal information as oppressive or risky. And the same assumptions that underlie the darknet hypothesis suggest that at least some security protocols will be broken.

Rather than avoiding the problem of liberty and constraint, however, the code-libertarian argument merely relocates that problem within a familiar set of implicit claims about what liberty is. Superficially, the claim that liberty inheres in the capacity for hacking and other forms of self-help sits within a long tradition of civil disobedience to unjust laws (and it has been framed that way, albeit unsuccessfully, in litigation over the scope of the DMCA's anticircumvention provisions). Yet it is potentially far more absolute, premised on a right to defy not only unjust architectures, but any code-based restrictions at all.

Ultimately, focusing on the incompatibility of technical constraints with absolute conceptions of liberty obscures more important questions about what is at stake in the legal and technical realignments that I have described. It does not follow that because architectures of control cannot eliminate residual liberty, they will have no effect on the everyday lives of network users. Exploring those effects, however, requires tools that legal theorists are unaccustomed to using. If we pay attention to some other terms that tend to crop up in debates about digital architectures, they suggest avenues of inquiry that have little to do with abstract liberty or freedom of expression.

First, consider the speed with which the darknet hypothesis has captured the imaginations of academics and policy makers. We saw in Chapter 5 that the debate about how far privacy rights extend in the networked information society is structured in important and largely unacknowledged ways by visual and spatial metaphors. The debate about the darknet hypothesis reveals a similar process at work in the domain of network architecture. Public discourse about the threats of digital piracy, terrorism, and cybercrime positions uncontrolled spaces and networks as sources of chaos and danger. In the darknet hypothesis, that danger is expressed metaphorically as the negation of visibility. Reasserting control over these spaces entails making visible what occurs within them—enabling those in authority to "see" activities formerly shrouded in darkness. Although no single metaphor comparable in power to the darknet hypothesis has emerged in public debate about security and surveillance, members of the data-processing industries sometimes describe their activities in terms of a need to minimize "black space" around individuals and groups.

Meanwhile, despite the negative connotations with which they are burdened, metaphors like "darknet" and "black space" suggest something important about the relationship between the architecture of information networks and the structural conditions of human flourishing. Like the concepts of "breathing room" and "breathing space" that we encountered in Chapters 3 and 5, the metaphors suggest that ordinary people experience freedom spatially, as affording a type of shelter that is important to their own well-being. The possibility of obtaining shelter through hacking and tinkering does not undercut, but instead reinforces, this point, which concerns the baseline held out to the ordinary network user as the alternative to lawlessness. Users who have the technical capability to do so may retreat to darknets or take refuge in black spaces not because they are up to no good but rather because architectures of control allow no other refuge. A society divided between controlled nets and darknets, however, is not the same as one in which a broader variety of authorized spaces are

subject to less rigid control. Likewise, a society in which the struggle to retain black space around one's everyday activities is cause for suspicion is different from one in which it is not.

Finally, consider participants' own descriptions of the conduct at issue in legal disputes about architectures of control. In the copyright context, many defendants characterize their conduct neither as trespass nor as speech, but rather as "tinkering"—taking something apart to see how it works or to make it work better.[49] In other contexts, tinkering may enable network users to alter their presentation of identity in some way, enabling them to use information resources without generating data trails. Advocates for expressive freedom have tried to reframe tinkering as itself expressive, or at least innovative (and therefore deserving greater deference by intellectual property laws). But that reframing is both awkward and unhelpful; when all speech is conduct and all conduct speech, the attribute of expressiveness ceases to be useful in informing thinking about the structure of information rights. Taken at face value, the term "tinkering" is a reference to the material environment, not the information environment. It describes the exercise of tactical, situated creativity with respect to the artifacts encountered in everyday life.

The terms "darknet," "black space," and "tinkering" all suggest powerfully that legal explorations of the ways that architectures of control affect human freedom should be proceeding down very different paths. In particular, they suggest that legal scholars should pay more careful attention to literatures that explore how artifacts and architectures shape the experiences of their users and how material culture and social ordering are intertwined.

Code and Markets

Perhaps, though, legal theorists who take seriously Lessig's equation of code and law have simply been pursuing the wrong analogy. Since code is produced, for the most part, via market-driven processes, then maybe regulation by code is most appropriately understood as a variant of regulation by the market. Some legal scholars argue that in a decentralized market economy, whatever modes of social ordering emerge from the market will be modes that are chosen by market participants, including both information vendors and information consumers.[50] Arguably, it is a mistake to regard orderings imposed in this fashion as anything other than voluntary, and if they are voluntary, it is a waste of time to worry about whether they are coercive of individual users in a more abstract, theoretical sense. The problem with this argument, which I will call the "market libertarian" argument, is that markets for the technologies that make up architectures of control persistently violate its most fundamental assumptions about how market processes work. The dynamics of marketplace acceptance and rejection are much more complicated than the market-libertarian model would have us believe. They are intimately bound up with the actions of government acting as both regulator and customer, as well as with decisions made by large technology companies pursuing a variety of self-interested goals. The choices available in the resulting markets are not inconsistent with, and may enable, the imposition of highly restrictive regimes that many market participants experience as onerous.

The market-libertarian argument about code-based regulation is often expressed in the language of economic efficiency, but ultimately it relies on

liberal political theory's foundational presumption of separation between state and market. Within the structure of liberal thought, the presumption of state-market separation operates in ways that are simultaneously normative and descriptive. Risks to liberty and social welfare are thought to arise principally from state interference with or entanglement in market processes. This means that code-based regulation is problematic when government attempts to impose technology mandates or when market actors capture regulatory processes and bend those processes to their own ends. This normative theory of state-market separation requires a descriptive model within which state-market separation is the norm and state-market entanglement the aberration. That is, however, a very poor model of the way that networked information technologies actually develop. State and private interests are deeply and inevitably intertwined, and architectures of control are emerging at the points of convergence. The complexity and path-dependence of that process makes it extremely difficult for markets to police.

In the context of copyright, both information providers and governments have powerful (though slightly different) motives for the pervasive extension of control. Information providers seek, first and foremost, to enforce what they perceive as their entitlements. Governments are in general sympathetic to the asserted need to protect private property, both for idealistic reasons related to notions of the social contract and the rule of law and for less idealistic reasons related to legislative and regulatory capture and the promotion of trade-related agendas. Thus, one might logically expect to see extensive state backing of private intellectual-property enforcement efforts undertaken by powerful domestic industries, and in fact this has been the case. Governments also seek to protect online commerce, including all the varieties of "legitimate" commerce in or enabled by the ready availability of personal information.

More fundamentally, however, state sovereigns confronting perceived security imperatives are not indifferent to the possibility of inserting control and surveillance functions into communication networks, nor to the existence of large databases of information about individual transactions and preferences. In the realm of online communication, architectural controls designed for one purpose can easily be adapted to others. Embedded controls that identify and locate information users, purchasers of goods and services, and transit and communication customers also lend themselves well to the reproduction of territorial sovereignty. Comprehensive databases linked to surveillance and authentication tools can empower sovereigns to combat a wide range of other evils—terrorism, or pornography, or hate speech, or dissent.

Devolution of surveillance capability into private hands enables greater control than government could achieve directly. Generally speaking, in democratic societies, government surveillance initiatives incur far more searching public scrutiny and meet with far more resistance than analogous private efforts deployed to enforce private bargains. Many profiling projects undertaken by the government have quickly become mired in controversy. Except among a small group of technological and legal cognoscenti, private-sector trusted-system initiatives and authentication technologies for increasing security in e-commerce have generated comparatively few ripples of alarm. Here the ideology of the marketplace itself reinforces the ongoing realignment of digital architectures. Just as privatization legitimates self-enforcing control and surveillance, so pri-

vatized control and surveillance reinforce the perception that the ordering imposed is freely chosen by arms-length contracting parties. To the extent that such capabilities remain primarily a matter of industry initiative, information providers enjoy much greater freedom to define the scope of their entitlements and the reach of their business models. The emerging network of private enforcement and surveillance capabilities serves both private and state interests far better than more extensive official involvement might. It is unsurprising, then, that proposed bills to enhance copyright enforcement, guarantee security in e-commerce, and confer expanded surveillance powers on law enforcement have exhibited persistent overlaps.[51]

Cyberlaw scholarship lacks a compelling theoretical model of this process. Michael Birnhack and Niva Elkin-Koren come closest, characterizing the evolving relationship between public and private sectors as an "invisible handshake."[52] Yet even that account slips now and then into the practiced rhetoric of market freedom and state coercion. Critical to the emerging dynamic is that each participant in the development of digital architectures of control sees in the other's goals a window of opportunity. Private actors may be worried about the customer-relations ramifications of conducting surveillance for the state or about the imposition of costly and inflexible technological mandates; at the same time, however, they have repeatedly proved themselves willing to risk some goodwill and sacrifice some technical autonomy in return for greater freedom to pursue other goals.

The market-libertarian model of economic governance fares no better when we consider intramarket dynamics. The model posits that (assuming a competitive marketplace) if consumers do not want systems that restrict the use of digital media files or that impose onerous authentication requirements in the name of "security," they will reject them. But the actual operation of technology markets is very different from what that description suggests, in two critical ways. First, the ultimate users of information goods are by no means the most important consumers of the technologies that make up emerging architectures of control. Second, the idealized model of consumer choice that is a cornerstone of the market-libertarian argument does not account for technological and institutional path-dependence.

The primary markets for copyright-protection systems are not end-user markets but rather the markets of intermediary licensors for those technologies. In the copyright context, those markets include both content distributors and manufacturers of devices for rendering the content. Pervasively distributed copyright enforcement seeks to eliminate unsanctioned technologies and business models by recruiting technology companies into the contractual networks that implement technological restrictions. The twin threats of indirect infringement liability and DMCA liability provide strong incentives to join these networks. Increasingly, therefore, the rational strategy is to license content and build devices subject to restrictions, regardless of whether the intermediary might otherwise prefer a different strategy. Large incumbents in the consumer electronics and personal computing markets have greater resources, and they have successfully resisted some copyright-industry initiatives to impose broadly defined mandates that would disrupt existing markets and distribution systems. They have been much less inclined to resist the introduction of restrictions in newer technologies, such as DVD players, digital music and video game play-

ers, and software-based multimedia devices, for which consumer expectations are less fully formed. And they have participated in efforts to develop trusted-system functionality for digital media files and digital broadcast content.

Similarly, the primary customers for security technologies include device manufacturers and a broad array of e-commerce companies, ranging from online marketplaces to banks and brokerage firms. The government is not simply a potential source of security mandates, but also an important customer for security systems in its own right. In response to public- and private-sector demands for security and authentication, large technology companies have participated willingly in efforts to develop secure protocols for system access, data storage, and commercial transactions. Some developers of trusted systems, including most notably market leaders Microsoft and Intel, appear to believe that trusted-system capabilities mesh well with other security-related design goals, such as enhanced network, server, and file security. For Microsoft in particular, deployment of this functionality also seems bound up with a number of business-related objectives, including preservation of its market position vis-à-vis open-source platforms.

Large communication providers confront a complex calculus of legal and business considerations. Many of these companies initially resisted content-industry demands for identification of individual subscribers accused of engaging in P2P file sharing.[53] But the large telephone and cable companies that provide most residential Internet access also have other agendas of their own. Cable companies have participated in the ongoing effort to develop a regulatory framework establishing trusted-system protection for cable television content. In addition, many communications companies seek to use their newly installed high-speed fiber-optic networks to establish quality-of-service pricing and to deliver their own proprietary content to subscribers. Therefore, they are not generally averse to technologies for flagging and sorting network traffic.

The choices and practices of content intermediaries, e-commerce companies, communication providers, and technology developers do not prevent end users from resisting functionality that they find undesirable or offensive, or from demanding functionality that they would value more highly, but they make both strategies more difficult to implement and therefore less likely to be pursued. The more deeply embedded such functionality becomes, the harder it becomes to avoid by purchasing noncompliant or alternative equipment and services. This effect will intensify if, as Jonathan Zittrain predicts, users are taught to fear files and applications that the platform vendor cannot or will not authenticate.[54]

The interplay of supply and demand in the market for the technologies that make up architectures of control is further complicated by the dynamics of technical standardization. Like all networked information technologies, the technologies that constitute architectures of control are designed based on standards for formatting, exchanging, and processing information. Standards processes typically occur long before implementations surface in the consumer marketplace. Many standards processes are closed, and the subject matter is technically complex. To become involved in setting standards, users must be determined enough and informed enough to overcome a series of significant hurdles. Some consumer advocacy groups have begun to do exactly this; what remains to be seen is whether these efforts will generate enough critical mass to

affect the content of the standards that are selected. Unaffiliated and academic researchers have been more inclined to cast a critical eye on standards and standards processes associated with emerging architectures of control. Perhaps even more than their colleagues at for-profit companies, however, these individuals are highly motivated to solve the difficult theoretical problems that are involved in making architectures of control work.

More generally, standardization creates technical and institutional path-dependencies that are difficult for any market participant to dislodge. Standards can be changed, but change moves slowly, and design decisions tend to have consequences for many generations of products. The licensing arrangements associated with architectures of control add to the overall inertia, creating institutional lock-ins that structure commercial relationships among content providers, technology providers, and other intermediaries. The dynamic of path-dependence is enhanced by some decidedly nontechnical factors. To the extent that draconian enforcement initiatives and heavy-handed public education efforts fuel popular resistance to architectures of control, increased popular resistance in turn fuels and legitimates the rhetoric of crisis and the extension of technologies to control it. The ratcheting-up of a crisis mentality increases the downside risks of liability for independent entrepreneurs and government oversight for standards developers. In short, even as the new control-based initiatives fail to convince end users, they strengthen their hold on the intermediaries whose products, services, and standards define the end-user marketplace.

For all of these reasons, the market-libertarian explanation for the emergence of architectures of control is far too simple. Idealized models of market choice cannot provide a useful template for evaluating the dynamic of constrained, path-dependent choice that predominates in markets for networked or network-capable information technologies. To understand why technology markets are offering particular choices rather than other conceivable choices, we must look elsewhere.

Code as Itself

A few legal scholars have sought to develop new analytical frameworks for analyzing digital architectures, frameworks that reject easy analogies to law or markets and instead ask different kinds of questions. Some argue that code represents a unique mode of governance that is wholly new. Others assert that emerging digital architectures make possible a form of regulation conceived long ago but never before realized: perfect panoptic surveillance. These theories represent important steps toward developing an understanding of how the regulation imposed by code differs from that imposed by law alone. In their confident embrace of digital exceptionalism, however, they also reflect the conceptual poverty of the models of social ordering that predominate within the mainstream cyberlaw literature.

James Grimmelmann argues that regulation by code is both uniquely plastic and uniquely inflexible. He asserts that regulation by code is different and more troubling than regulation by physical architecture because of the immediate and fine-grained control that code permits and because software regulation lacks transparency. Raising some of the same concerns, Polk Wagner argues that law should step in to regulate forms of online behavior so that code will retreat. Both scholars are right to worry that the ability to design highly

granular forms of control will tempt policy makers and entrepreneurs to mischief. Within both analyses, however, law and code are the only two regulatory variables in play. The institutional and cultural factors that might lead us toward certain (worrisome) implementations of code rather than toward other possible implementations are incompletely explored.[55]

Jonathan Zittrain tackles the latter question, arguing that the move toward digital lockdown is motivated principally by fear of the unknown. He asserts that networked information technologies should be prized to the extent that they foster generativity, which he defines in terms of a technology's capacity to serve as a platform for unpredictable future innovation.[56] Zittrain's principal worry is that maintaining current levels of generativity may be incompatible with the kinds of security that people want. But because he devotes little analysis to the other factors that cause the policy landscape to tilt in one direction or the other, it is hard to understand either how we got here or how to change current trajectories of technological and commercial development.

In contrast to Grimmelmann, Wagner, and Zittrain, each of whom seeks to develop an account of code's difference out of whole cloth, Sonia Katyal finds conceptual precedent for code-based regulation in Foucault's discussion of the Panopticon. Foucault characterized the Panopticon as the perfect prison, designed to ensure both complete access to those to be surveilled and complete invisibility for the watchers.[57] As we saw in Chapter 5, privacy scholars have long invoked panoptic imagery to criticize the use of networked digital technologies for surveillance and profiling purposes. In so doing, however, they read Foucault's description of the Panopticon as a lesson in the power of visual surveillance. Katyal develops her analysis of "piracy surveillance" along similar lines, arguing that the combination of P2P architectures with laws enabling access to personal information about network users is troubling because it operates to make users' activities visible.[58]

All of these thinkers are onto something important about what code does differently and why it matters, but liberalism's anxieties are also prominently on display in the answers that they offer. Code's capabilities for control do not arise in a vacuum, nor does its generativity. And visibility is only one of the considerations that code puts into play.

Let us begin by returning to the Panopticon. Foucault proffered the Panopticon not as a blueprint for a particular disciplinary institution, but rather as an organizing metaphor for a group of disciplinary strategies embedded in the operation of ordinary social institutions and coordinated by the everyday routines and interactions of a variety of public actors. He analyzed the emergence of hospitals, schools, armies, and prisons as institutions that enact social discipline by targeting marginal, abnormal, or imperfect members of society for treatment, education, socialization, or punishment. In particular, he argued that these ostensibly marginal institutions also discipline those not subject to their control, albeit indirectly. Schools, hospitals, armies, and prisons normalize by partition; by defining, segregating, and disciplining those deemed abnormal or transitional, they simultaneously define and enforce the parameters of normalcy for everyone else.[59]

So conceptualized, panoptic discipline requires neither constant visual observation nor centralization of authority; instead, it depends importantly on

several other factors. First, it entails an arrangement of social space that enables but simultaneously obviates the need for continual surveillance. Second, this arrangement proceeds from and is reinforced by the ordinary operation of social institutions. Third, it is accompanied by discourses—ways of organizing and framing perceived truths—that establish parameters of normal behavior. Finally, the institutionally embedded arrangements of spaces and discourses in turn foster the widespread internalization of disciplinary norms. In contrast to the four-part taxonomy outlined in *Code*, the components of panoptic discipline meld into one another in ways that are fluid and relatively seamless. And as James Boyle explains, law that meshes with the mechanisms of panoptic discipline is far more powerful than law that simply seeks to command obedience.[60]

This is not to argue that a properly conceived panoptic model is all we need in order to understand regulation by code. That model is also incomplete in important respects. Foucault emphasized the authoritarian nature of eighteenth- and nineteenth-century social institutions, but the technology-based strategies described above are for the most part deployed and coordinated by a decentralized network of private actors. The discursive discipline embedded in the operation of contemporary market institutions also operates differently; it is not dictated by authoritarian institutions, but rather is generated within a variety of market and nonmarket settings via complex feedback processes. A good model of regulation by code must account for the ways that normalization proceeds under the conditions of constrained, path-dependent choice described above.

In addition, the core commitments of liberal theory tend to disable legal scholars who study code as code from acknowledging two central aspects of the regulatory dynamic. First, as we have seen again and again throughout this book, legal theorists tend to overlook or deemphasize the material and spatial dimensions of social processes. As Zittrain's and Grimmelmann's analyses implicitly recognize, code's normalizing effects do not flow solely from what it prohibits. They flow far more powerfully from what code permits, and how. The STS perspective in particular would insist on moving beyond a crude materialist determinism to an analysis of the mundane, material ways in which code organizes social and economic activity. Of particular interest are the unexamined ways in which code's affordances—the actions it permits and the ways it presents information—shape users' expectations and habits. Regarding architectures of control, critical questions concern the availability of breathing space and the extent of institutional tolerance for tinkering as material (not expressive) practice. For similar reasons, a cultural geographer would want to consider the ways in which code propagates new pathways and boundaries throughout the spaces in which people live, producing configurations that embody new arrangements of institutional power.

Second and relatedly, liberal commitments encourage legal scholars to overlook the ways in which prevailing conceptions of the "normal" are themselves constructed. Code is both a means and an effect of discursive normalization. The design of digital architectures reflects beliefs about rational social ordering that are not themselves givens. It also reflects beliefs about unacceptable risks and the most reliable ways of minimizing them. Legal theorists of technology have difficulty probing these issues both because they have difficulty acknowledging discourse as a substantive determinant of policy in its own right

and because they have difficulty recognizing rationality as a culturally-constructed norm. Thus, in responding to pervasively distributed copyright enforcement, legal scholars and public-domain advocates have tended to focus on the "theft," "piracy," and "communism" strands, all of which hinge on presuppositions about the extent to which copyright is really "property," and to ignore or ridicule the other, more hyperbolic comparisons. Privacy scholars have preferred to debate whether post-9/11 security measures actually improve security rather than to delve too deeply into the ways in which public discourse invests that term with particular, contingent meanings.

Scholars who recognize code as a modality of governance not reducible either to law or to markets are on the right track. But understanding the regulatory effects of emerging architectures of control requires a model of governance that incorporates factors that legal theorists of code have systematically overlooked. Such a model must accommodate the complex institutional dynamics of contemporary technology markets. It should acknowledge and allow examination of the ways that artifacts and architectures configure their users. Finally, it should permit interrogation of the ways that artifacts and architectures reflect and reproduce social discourses about risk and risk minimization.

Challenges for a Theory of Code and Law

While architectures of control have excited enormous interest among legal scholars, the social and institutional contexts within which they are embedded have not excited nearly enough. The ability to interrogate the assumptions underlying such architectures and, if necessary, to control their excesses depends critically on the capacity to see them as socially driven solutions to socially constructed problems. The four-part *Code* framework has been instrumental in setting legal scholarship on that path, but it cannot take us where we need to go. An account of regulation as emerging from the Newtonian interaction of code, law, market, and norms is far too simple regarding both instrumentalities and effects. The architectures of control now coalescing around issues of copyright and security signal systemic realignments in the ordering of vast sectors of activity both inside and outside markets, in response to asserted needs that are both economic and societal. Understanding the technical, social, and institutional changes now underway requires a theoretical tool kit that encompasses the regulatory functions of institutions, artifacts, and discourses.

Notes

[1] Lessig, *Code and Other Laws of Cyberspace*, 88.

[2] This terminology, which originates in the political science literature, helpfully reminds us that regulatory modalities are means by which self-interested actors pursue institutional change. See, for example, Raab & de Hart, "Tools for Technology Regulation." See generally Giddens, *The Constitution of Society*.

[3] On the organizational changes enabled by the advent of information processing technologies, see Beniger, *The Control Revolution*.

[4] Computer Fraud and Abuse Act of 1984, Pub. L. No. 98–473, 98 Stat. 2190 (codified as amended at 18 U.S.C. §1030). For the 1986 amendments extending the statute's coverage to nongovernment computers, see Pub. L. No. 99–474, 100 Stat. 1213. For the 1994 amendments, see Pub. L. No. 103–322, 108 Stat. 2097.

[5] For good summaries of these changes and their effects on prosecutorial behavior, see Ohm, "The Myth of the Superuser," 1349-51; Skibell, "Cybercrimes and Misdemeanors," 927-33.

[6] The "surface level" terminology is my own. See Cohen, "Pervasively Distributed Copyright Enforcement," 4-7.

[7] For good descriptions of the music industry's failure to implement a coordinated strategy for surface-level protection and of the motion picture industry's relatively successful implementation, see Gillespie, *Wired Shut*, 137-91.

[8] Pub. L. No. 105–304, 112 Stat. 2863-77 (codified at 17 U.S.C. §§1201-1204).

[9] For a fuller description, see Cohen, "Pervasively Distributed Copyright Enforcement," 9-11.

[10] See Electronic Frontier Foundation, "Unintended Consequences: Twelve Years under the DMCA" (2010), http://www.eff.org/files/eff-unintended-consequences-12-years.pdf, 2-6.

[11] Failed legislative efforts include the Consumer Broadband and Digital Television Promotion Act of 2002, Proposed Bill No. S. 2048, 107th Congress, 2nd Session; the Digital Transition Content Security Act of 2005, Proposed Bill No. H.R. 4569, 109th Congress, 2nd Session; and the Audio Broadcast Flag Licensing Act of 2006, Proposed Bill No. H.R. 4861, 109th Congress, 2nd Session. In 2003, the entertainment industries successfully prevailed on the Federal Communications Commission to issue a broadcast-content protection rule, but the rule was invalidated on jurisdictional grounds. See American Library Association v. Federal Communications Commission, 406 F.3d 689 (D.C. Cir. 2005). For the FCC's cable plug-and-play rule, see Federal Communications Commission, "Commercial Availability of Navigation Devices and Compatibility between Cable Systems and Consumer Electronics Equipment," 68 Fed. Reg. 66,728 (Nov. 28, 2003).

[12] See High Level Group on Digital Rights Management, Final Report (2004), http://ec.europa.eu/information_society/eeurope/2005/all_about/digital_rights_man/doc/040709_hlg_drm_2nd_meeting_final_report.pdf.

[13] Intel, "Technology Overview: Intel Trusted Execution Technology," http://www.intel.com/technology/security/downloads/TrustedExec_Overview.pdf.

[14] Pub. L. No. 105–304, 112 Stat. 2877-86 (codified at 17 U.S.C. §512).

[15] Quilter & Urban, "Efficient Process or 'Chilling Effects'?"

[16] The statutory provision authorizing injunctive relief against backbone providers is 17 U.S.C. §512(j)(1)(b)(ii). For a discussion of the Listen4Ever case, see Daniel W. Kopko, "Looking for a Crack to Break the Internet's Back: The Listen4ever Case and Backbone Provider Liability Under the Copyright Act and the DMCA," *Computer Law Review and Technology Journal* 8 (2003): 83.

[17] Higher Education Opportunity Act, Pub. L. No. 110–315, 122 Stat. 3078 (codified at 20 U.S.C. §1094(a)(29)). For the background notice-of-repeat-infringement rule, see 17 U.S.C. §512(e).

[18] See Rick Mitchell, "French Constitutional Panel OKs Piracy Law, Cutting Internet Access After 'Three-Strikes,'" *BNA Patent, Trademark & Copyright Journal*, Oct. 30, 2009, 804.

[19] See Sarah McBride & Ethan Smith, "Music Industry to Abandon Mass Suits," *Wall Street Journal*, Dec. 19, 2008.

[20] See ibid.

[21] See Eriq Gardner, "EXCLUSIVE: 'Expendables' Producer Next to Sue Thousands of Online Pirates," *Hollywood Reporter*, Jan. 4, 2011, http://www.hollywoodreporter.com/blogs/thr-esq/expendables-producer-sue-thousands-online-68257.

[22] For a good summary of the rhetoric deployed by representatives of the motion picture industry, see Gillespie, *Wired Shut*, 118-25.

[23] See Gillespie, "Characterizing Copyright in the Classroom."

[24] See U.S. Department of Homeland Security, "US-VISIT Biometric Identification Services," http://www.dhs.gov/files/programs/gc_1208531081211.shtm; Peter Alford, "Japan Immigration to Scan Foreign Faces," *Australian*, Oct. 25, 2007, 11; Wilmer Heck & Annemarie Kas, "Fingerprints in Passports Can't Be Used by the Police--Yet," *NRC Handelsblad*, Sept. 18, 2009, 1.

[25] The most recent report, *Privacy and Human Rights 2006*, can be found online at http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559458.

[26] See U.S. Department of Homeland Security, "DHS Announces $12 Million for Operation Stonegarden to Support Local Border Security Efforts," Dec. 15, 2006, http://www.dhs.gov/xnews/releases/pr_1166216119621.shtm; U.S. Department of Homeland Security, "Secretary Napolitano Announces $60 Million in Operation Stonegarden Grants for Border States," June 4, 2009, http://www.dhs.gov/ynews/releases/pr_1244070019405.shtm.

[27] On the privatization of public space, see generally Kohn, *Brave New Neighborhoods*, and Low & Smith, *The Politics of Public Space*.

[28] See Communications Assistance for Law Enforcement Act, Pub. L. No. 103–414, 108 Stat. 4279 (codified at 47 U.S.C. §§1001–10); U.S. Federal Communications Commission, "Communications Assistance for Law Enforcement and Broadband Access and Services," 20 *F.C.C. Record* 14989 (2005), *affirmed*, American Council on Education v. F.C.C., 451 F.3d 226 (D.C. Cir. 2006).

[29] See Foreign Intelligence Surveillance Act, Pub. L. No. 95–511, 92 Stat. 1783 (codified at 50 U.S.C. §1801); Schwartz, "Warrantless Wiretapping, FISA Reform, and The Lessons of Public Liberty," 411-17.

[30] See Eric Lichtblau & James Risen, "Spy Agency Mined Vast Data Trove, Officials Report," *New York Times*, Dec. 24, 2005; Leslie Cauley, "NSA Has Massive Database of Americans' Phone Calls," *USA Today*, May 11, 2006; Alexander Dryer, "How the NSA Does 'Social Network Analysis,'" *Slate*, May 15, 2006, http://www.slate.com/id/2141801; Siobhan Gorman, "NSA's Domestic Spying Grows as Agency Sweeps Up Data," *Wall Street Journal*, Mar. 10, 2008.

[31] See Ohm, "The Rise and Fall of Invasive ISP Surveillance," 1432-37.

[32] See Comcast Corp. v. Federal Communications Commission, 600 F.3d 642 (D.C. Cir. 2010); Paul Barbaglio, "House Commerce Adopts Resolution to Overturn FCC's Net Neutrality Rules," *BNA Electronic Commerce & Law Report*, Mar. 16, 2011, 420; John Letzing, "As Debate Intensifies, Net Neutrality Rivals Invest in D.C. Influence," *Wall Street Journal*, Apr. 7, 2010, http://online.wsj.com/article/BT-CO-20100407-

706109.html; Kevin Bogardus & Kim Hart, "Companies Lobby Newest FCC Members on Net Neutrality Rule," *Hill*, Nov. 11, 2009, 16.

33 For a summary of official policy on fusion centers and links to reports and guidelines, see U.S. Department of Justice, "Fusion Centers and Intelligence Sharing," http://www.it.ojp.gov/default.aspx?area=nationalInitiatives&page=1181. A wider variety of information can be found at Electronic Privacy Information Center, "Information Fusion Centers and Privacy," available at http://epic.org/privacy/fusion/.

34 Hoofnagle, "Big Brother's Little Helpers," 598-618.

35 See Electronic Communications Privacy Act, Pub. L. 99–508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §2703(f)); Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, 2006 O.J. (L 105) 54.

36 Spencer S. Hsu, "States Get More Time to Comply with Real ID," *Washington Post*, Dec. 19, 2009.

37 DeNardis, *Protocol Politics*, 79.

38 See Ashlee Vance, "Microsoft Office 2010 Starts Ascension to the Cloud," Bits Blog, *New York Times*, July 13, 2009, http://bits.blogs.nytimes.com/2009/07/13/ microsoft-office-2010-starts-ascension-to-the-cloud/.

39 See, for example, Nik Bonopartis, "Net Vigilantes Go Where Police Can't: Groups Help Identify Pedophiles," *Poughkeepsie Journal*, Oct. 4, 2004. Texas Border Watch, http://www.texasborderwatch.com/. For a good general discussion of the dynamic by which ordinary people are recruited as participants in surveillance activities, see Andrejevic, *iSpy*, 175-82. To be fair, vigilance by ordinary citizens has achieved some spectacular successes. See, for example, Corey Kilgannon & Michael S. Schmidt, "Street Vendors' Keen Eyes Alerted Police to Threat," *New York Times*, May 3, 2010 (attempted bombing of Times Square in New York City); Anahad O'Connor & Eric Schmitt, "Terror Attempt Seen as Man Tries to Ignite Device on Jet," *New York Times*, Dec. 26, 2009 (attempted bombing of Detroit-bound airliner on Christmas Day).

40 For examples, see "Address by the Right Honorable Tony Blair, Prime Minister of the United Kingdom of Great Britain and Northern Ireland," *Congressional Record* 149: H7060 ("The virus is terrorism. . . "); "Authorizing Use of United States Armed Forces against Those Responsible for Recent Attacks against the United States," *Congressional Record* 147: H5638 (statement of Rep. Hoyer) ("[W]e must cut out and destroy this cancer which plagues civilized society"); "National Security in the Wake of Events of September 11," Congressional Record 147: H6121 (statement of Rep. McInnis) ("My analogy . . . is a battle . . . against a cancer").

41 See U.S. Department of Homeland Security, "About the Homeland Security Advisory System," http://www.dhs.gov/files/programs/Copy_of_press_release_0046.shtm#2

42 Lessig, *Code and Other Laws of Cyberspace*, 88.

43 See, for example, Dam, "Self-Help in the Digital Jungle," 394-97, 407-09; Smith, "Self-Help and the Nature of Property," 101-06.

44 Bracha, "Standing Copyright Law on Its Head?," 1806.

45 See, for example, Balkin, "Digital Speech and Democratic Culture"; Benkler, "Free as the Air to Common Use."

46 See, for example, von Lohmann, "Measuring the Digital Millennium Copyright Act against the Darknet," 640-43.

[47] Biddle et al., "The Darknet and the Future of Copyright Protection."

[48] For a well-supported argument that not all copy protection will be broken, see Ohm, "The Myth of the Superuser," 1359-62.

[49] See http://www.freedom-to-tinker.com/.

[50] See, for example, Dam, "Self-Help in the Digital Jungle," 407-12; Picker, "From Edison to the Broadcast Flag," 293-96.

[51] See, for example, Cybersecurity Enhancement Act of 2010, Bill Number H.R. 4061.EH, §105(a), 111th Congress, 1st Session (version enacted in House).

[52] See Birnhack & Elkin-Koren, "The Invisible Handshake."

[53] See In re Charter Communications, Inc. Subpoena Enforcement Matter, 393 F.3d 771 (8th Cir. 2005); Recording Industry of America v. Verizon Internet Services, Inc., 351 F.3d 1229 (D.C. Cir. 2003), *cert. denied*, 543 U.S. 924 (2004).

[54] Zittrain, *The Future of the Internet*, 57-59.

[55] See Grimmelmann, "Regulation by Software;" Wagner, "On Software Regulation."

[56] Zittrain, *The Future of the Internet*, 70-73.

[57] Foucault, *Discipline and Punish*, 200-09.

[58] Katyal, "The New Surveillance," 309-20; Katyal, "Privacy vs. Piracy," 244-51.

[59] Foucault, *Discipline and Punish*, 135-69, 210-28.

[60] Boyle, "Foucault in Cyberspace."