March, 2000

Book Review: Lawrence Lessig, Code and Other Laws of Cyberspace

Henry H Perritt, *Chicago-Kent College of Law*

Lawrence Lessig, Code and Other Laws of Cyberspace

HENRY H. PERRITT JR.*

Larry Lessig's *Code and Other Laws of Cyberspace*[1] joins Ithiel de Sola Pool's *Technologies of Freedom*[2] as changing the way people think about the relationship between information technology and law. *Technologies of Freedom*, written in the early 1980s, got lawyers and policy makers thinking about the implications of a collapse of the traditional boundaries that defined legal regulation of newspapers, telephone communications, and broadcast.

Code and Other Laws of Cyberspace punctures some important myths that have retarded constructive, creative thinking about the Internet's relationship to law. The first myth is that the Internet represents a sufficiently distinct culture that it should be thought of as its own sovereign with no relevant ties to traditional legal systems. The second myth is that technical solutions to misconduct on the Internet always are better than legal solutions.

Lessig begins with four stories that illustrate the special challenges that the Internet and related technologies present to traditional legal institutions. From these stories, he synthesizes four themes that drive the organization of the rest of the book: (1) regulability, which is a function of network architecture; (2) regulation by code, likely to increase in importance as governmental pressure for regulation stimulates private actors to express rules in computer programs; (3) competing sovereigns, not only competition among nation states, but also between nation states and private communities and governments in cyberspace; and (4) latent ambiguities in constitutions and other basic law, which present the risk that constitutional protections will become even thinner as cyberspace becomes a more important marketplace and political arena.

Lessig points out that regulability depends upon architectures of control, particularly identity and authentication. As commerce becomes more important on the Internet, pressures to change the architecture to reduce the

* *Dean and Professor of Law, Chicago-Kent College of Law, Illinois Institute of Technology*

1. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).
2. ITHIEL DE SOLA POOL, TECHNOLOGIES OF FREEDOM (1983).

opportunities for anonymous interaction and to increase technical methods for authentication will increase, making the Internet more regulable. Cookies and encryption are two obvious changes in the architecture already visible. To illustrate this phenomenon, Lessig asks us to imagine the following scenario:

> [E]veryone holds a digital ID, and not necessarily a governmentally issued ID; any ID will do. As you pass onto a site, the site checks your ID. If you do not hold the proper ID for that type of site—if you are under eighteen and it is an adult site, or if you are from Minnesota and it is a gambling site—the site does not let you pass. But if you hold the proper ID, the site does let you pass. This process occurs invisibly, or machine to machine. All the user knows is that she has gotten in, or if she has not, then why.[3]

States—both states within the United States and nation states—have mutual incentives to reinforce this kind of regulation.

Lessig then applies these ideas to specific legal categories. Applying the new architectures of control to intellectual property upsets the traditional balance struck by the public law of copyright by eliminating fair use and the practical possibility of some infringement at the margins. This tilts the balance toward the interest of copyright owners at the expense of society's interest in vigorous advancement of knowledge, necessarily premised on value-added contributions of those who have gone before. As to privacy, Lessig reviews the now-familiar threats that the Internet and mouse tracking present to personal privacy. Here, the new architectures of control can lead in opposing directions. They can make it easier to collect and to combine private information, but they also can make it easier for individuals to know the privacy practices of those with whom they deal through the Internet and to withhold their information from entities whose privacy protections they do not like.

In both instances, Lessig argues that collective action through political institutions is appropriate—in the case of copyright, to control the commercial forces favoring the new architectures of control; and in the case of privacy, to force movement toward architectures of control in the face of opposition by commercial interests.

The third area of application is free speech, where Lessig upsets the conventional wisdom that private technical controls on harmful speech are always better than governmental controls.

> Zoning, then, builds into itself a system for its own limitation. A site cannot block someone from the site without that individual knowing it. Filtering is different. If you cannot see the content, you cannot know what is being blocked. In principle at least, con-

3. LESSIG, *supra* note 1, at 55.

> tent could be filtered by a PICS filter somewhere upstream and you would not necessarily know this was happening.[4]

Lessig has two problems with this kind of architecture. First, it diminishes the exposure of citizens to speech they have not specified in advance as welcome, thus undermining the robust exchange of ideas that is a conceptual foundation of the First Amendment. Second, and potentially more serious, is the lack of transparency of technological controls over speech. Unlike traditional legal control, which can be debated openly and vigorously, technical controls slip in by the back door and are implemented by private entities and not governments, thus placing the controls outside constitutional protections.

He challenges the idea that cyberspace is a separate sovereign, distinct from traditional sovereigns. The key problem with this conception, Lessig argues, is that with traditional sovereigns, you leave the territory of one when you enter the territory of another. That is not so with the Internet. An Internet citizen is simultaneously present in a sovereignty of cyberspace at the same time he is present in the territory of a traditional sovereign.

Lessig suggests several responses. First, he suggests a careful move toward the German tradition that subjects private structures of power to some degree of control by fundamental constitutional values, rather than enforcing a stark dichotomy between public and private actors, subjecting only the former to constitutional controls.

Second, he cautions against abstention by legislators to private interests, urging that fundamental choices should be made through the regular representative political process. He is not extreme in his recommendation.

> I don't think that everything is necessarily public, or that the Constitution should regulate every aspect of private life. I don't think it is a constitutional issue when I turn off Rush Limbaugh. But to say that there should be a difference is not to say that the difference should be as dramatic or absolute as present constitutional thinking makes it.[5]

Professor Lessig's arguments are sophisticated, but he develops them carefully, in everyday language, painstakingly explaining aspects of technology and legal doctrine that may not already be known by readers. He also writes with unusual candor, identifying the critical logical elements of his argument and inviting readers to disagree with them.

Action by legislatures is not the only solution Professor Lessig proposes. The danger of regulation by code is its lack of transparency. People subjected to the regulation do not know they are being regulated. Moreover, because the computer programs including the regulating code are pro-

4. *Id.* at 179.
5. *Id.* at 221.

prietary, the proprietor has exclusive authority to regulate, free of legal or constitutional scrutiny. "Open code" eliminates both of these dangers. Open code, exemplified by the protocols developed by the Internet Engineering Task Force (IETF), the World Wide Web Consortium, and the Linux Operating System, is code that is available for anyone to inspect, and is free of copyright, trade secret, or patent restrictions, allowing anyone to modify it. When regulatory features are proposed or actually written for open code, an open debate over the desirability of the regulation is possible. Moreover, the pluralism inherent in the development of open code ensures broader accountability, at least to those participating in writing the code, if not to all producers and consumers. Professor Lessig and the Berkman Center at Harvard University are active proponents of open code approaches.

In essence, Lessig reminds us that the Internet, as revolutionary as it is, has not made politics disappear. It has not erased competing interests, or the power imbalances that allow dominant interests to trample the interests of weaker ones. The technologies of freedom and of commerce embodied in the Internet do not erase 3,000 years of human learning about political institutions and legal systems. The challenge before us—one which Lessig helps us understand through this important new book—is how to connect the political institutions of democracy to the Internet without losing the benefits of either.