explains in the Preface; the scholars are discussing problems that "law and regulation *can never resolve*" (xi; my emphasis). This is probably true, yet, as many of the essays themselves argue, law and regulation *must* attempt to resolve them. The same can be said of the authors. If those who think about and research the issues cannot or will not make any attempt to resolve these dilemmas, what can we expect of the lawmakers and politicians—not to mention the citizens—who read the works of such experts for advice?—*M. Wendy Hennequin, Department of English, Box U-1025, University of Connecticut, Storrs, CT 06269 <M.Wendy.Hennequin@uconn.edu>*

Code and Other Laws of Cyberspace

Lawrence Lessig. New York: Basic Books, 1999. 297 pp. $30.00.

Legal scholars have argued long and hard concerning the role of law in society. The law is also developing in the new cyber society, and scholars, policy-makers and other stakeholders have been wrestling with the problem of law in cyberspace. Is cyberspace "regulable" (a lawyer's term if there ever was one, p. 27) and if so what is or should be the nature of that regulation? The operation of law—the regulation of behavior—in cyberspace, as in society, in general is a result of a mix of forces: market, law, norms, and architecture (p. 89). Lessig discusses these four "modalities" throughout his book and in a brief appendix (an odd choice for its placement.) This articulation is a welcome reminder that the law is not the only factor in any policy analysis. This construct anchors a thoughtful, readable yet documented conversation of the problems and potentials of law (code) and code (architecture) in cyberspace. Most intriguing is the focus upon cyber architecture as code and its potential influence in the four-part matrix. And although this articulation is not unique, it is presented in a fresh ("code") perspective. The book is a good introduction to this dilemma in a variety of legal contexts (privacy, copyright, speech, etc.), but those who are familiar (other legal scholars) with the debate of whose interests will govern cyber policy—owners versus users—might find his exposition somewhat thin in places. For example, the chapter entitled "Intellectual Property" is really about copyright, and then only scratches the surface of the plethora of issues raised by the government's now infamous White Paper. Such topics are routinely debated in the legal literature. But Lessig's book again is best described as a conversation, one meant for readers at many levels of expertise, and therein lies the book's value. (*The National Law Journal* in an article on the country's top 100 lawyers called it "seminal.")

The message is simple: left to itself commercial and private interests will come to dominate cyberspace, and this domination will be achieved not by law but by code, the architecture of cyberspace. The battle for control of cyberspace is the battle over code. The first two parts of the book ("Regulability" and

"Code and other regulators") explore these themes in detail. The fact that Lessig constructs his legal exposition with a word ("code") that can mean precisely what it threatens to destroy underscores the "ambiguities"(p. 22) that cyberspace presents to us. A legal code can provide structure; it can regulate. Digital code also provides a mechanism for structure, thus for control. It might be said that this ambiguity arises from these two competing forces of control, though Lessig might not quite express it that way. This ambiguity arises, according to Lessig, from the differing networks that make up the web of virtual space, and this goes back to his theme: "The networks thus differ in the extent to which they make behavior within each network regulable. This difference is simply a matter of code — a difference in the software. Regulability is not determined by the essential nature of these networks. It is determined instead by their architecture" (p. 27).

But code appears indiscriminant. This is due to certain imperfections of information. Since "there is no simple way either to know who someone is [the first imperfection of "credential"] or to classify data [the second imperfection of "labels"], there is no simple way to make access to data depend on who the user is and on the data he or she wants access to" (p. 28). "Real-space life thus carries with it this mix of authenticating and authenticated credentials. Social life is a constant negotiation between these different credentials" (p. 31). Cyberspace is different. In cyberspace these natural social devices are not present (though proponents of the technology might argue with this assumption). Code is not designed for social validity; rather it is "concerned with network efficiency" (p. 33). However, "the differences in the architectures of identity in real space and cyberspace have profound consequences for the regulability of behavior in cyberspace…. The absence of self-authenticating facts in cyberspace reduces its regulability" (p.33). The nature of cyberspace opens the door for the ascendancy of code. The struggle for control of the cyber architecture, of the code, is the struggle for the control of cyberspace itself. "Left to itself, cyberspace will become a perfect tool of control" (p. 6). The question is who sets the parameters of control? The challenge of cyberspace, like any legal structuring, then is the proper balance of public and private.

Lessig believes that although the architecture of the Internet makes regulation of behavior by government more challenging, it does not mean that it is impossible "for the government to regulate the architecture of the Net." Thus Lessig believes that since code controls cyberspace, and code is architecture the best way to regulate is to control code (with code, legal code that is). This should be the role of government, to tinker with the architecture, which in turn will make regulation easier, i.e., not be hampered by the code/architecture juggernaut. This type of indirect regulation, the regulation of architecture (in Chapter 5 Lessig gives various examples, e.g., DAT (Digital Audio Technology) or the V-Chip) can be effective when intermediaries are targeted, as opposed

to individuals. "Intermediaries are fewer, their interests are usually commercial, and they are ordinarily pliant targets of regulation" (p. 50.) Lessig explains that regulation could force the use of digital identifiers for individual users whereby various jurisdictions and the providers within those jurisdictions (the intermediaries) would comply (honor) the home rules associated with the digital ID. In other words, a person in a state that restricts gambling (Minnesota) could not gamble simply by visiting an on-line site from a Nevada source because the Nevada server would not recognize the ID (this assumes regulation forces Nevada to respect (honor) another state's legal code). How does it honor the wishes of the Minnesota legislature? It enforces that "honor" with digital code. Lessig argues that regulation would occur as a result of the forwarding of the mutual interests of the various parties. "[T]he same architecture that enables Minnesota to achieve its regulatory end can also help other states achieve their regulatory ends, And this can initiate a kind of quid pro quo between jurisdictions" (p.55). This type of regulatory targeting would raise "serious constitutional issues" (p. 51).

A section of the book includes several chapters of case studies more or less built around various legal issues in cyberspace: Translation, Intellectual Property, Privacy, Free Speech, Interlude, and Sovereignty. Since my expertise is intellectual property, a focus on the content of those two chapters is the most appropriate. Lessig characterizes the options for protecting property in cyberspace into two categories: traditional protection of law (having the state define space, indicating where or how one can or can not enter) and a fence (self-regulation). In real space, a mix of law and fence exist. This occurs because at times one provides more efficient protection than the other does. Which is better in cyberspace? It depends perhaps on the tradeoff: "the right [copyright] is protected to the extent that laws (and norms) support it, and it is threatened to the extent that technology makes it easy to copy" (p. 124). Lessig criticizes the White Paper on intellectual property because it confuses real and virtual space, treating them both alike. According to Lessig "something fundamental has changed: the role that code plays in the protection of intellectual property has changed. Code can, and increasingly will, displace law as the primary defense of intellectual property in cyberspace. Private fences, not public law" (p. 126). As a result the wrong questions are being asked: not whether the law can aid in protection but whether the protection offered by the law is too great; this occurs, using Lessig's metaphor, because the "fences" have become too high and solid. For example, code can help copyright owners meter (a type of fence) use of copyrighted material, charging according to how much we read; this of course jeopardizes the first sale right and the concept of fair use among others. The "copyright is already being displaced, if not by code then by the private law of contract" (p. 135). Lessig would argue that at least contract is a form of law. This means that important choices face us: do we let code develop and

allow intellectual property to "become completely propertized" (p. 140) or do we work to preserve some sort of "intellectual commons" (p. 141)? The arguments are well made if a bit cursory when compared to say the work of David A. Rice and others in the legal literature who argue against the ascension of private wagering, whether by contract or by "fence."

A final section of the book entitled "Responses," including a review of the role of judiciary in articulating a democratic response, is perhaps disappointing for its brevity. The major point seems to be that things are different now (in terms of architecture) than when Jefferson and the framers envisioned our democracy, and that it should command the courts and other stakeholders to err on the side of the "intellectual commons," not code, thus preserving democracy.

Whether one agrees or disagrees with Lessig, his thoughtful, articulate and well documented commentary on the role of law, government, and regulation in cyber society is an excellent primer on the background and nature of the legal infrastructure and the problems society faces in constructing the structure of cyberspace.—*Tomas A. Lipinski, Center for Information Policy Research, University of Wisconsin — Milwaukee, P.O. Box 413, Milwaukee, Wisconsin 53201. <tlipinsk@csd.uwm.edu>*

Libricide: The Regime-Sponsored Destruction of Books and Libraries in the Twentieth Century

Rebecca Knuth. Westport, CT: Praeger, 2003. 277 pp. $39.95.

Censorship is a hot topic practically and intellectually: The control, bowdlerization, or elimination of articles, books, films, websites, ideas, and cultural artifacts continues to haunt us. Virtually everyone has some ideological position to protect and he or she does not mind extirpating the opposition. Taken to its logical conclusion, censorship leads to libricide, the complete destruction of books, usually in massive bonfires; sometimes the buildings housing the collections are burned as well. In a carefully burnished and documented study, Rebecca Knuth discusses the historical evolution of library collections, which she supplements with a meticulous theoretical foundation for the destruction of books in the twentieth century. Among the ideologies discussed are nationalism, imperialism, racism, and communism. There follow five chapters detailing the horrors of ideological genocide and its concocmitant necessity: the confiscation of materials and especailly the destruction of all competing ideas through book burnings. Each example details man's barbaric nature, but most egregious is the Nazi attempt to annihilate all peoples and ideas that countered their psychotic ideology. Knuth grounds her discussion of libricide in the concomitant attempt to murder the sick, maimed, different, and especially European Jews. The care, scholarly preparation, and planning with which the Germans set out to accomplish the extirpation, destruction, and removal of books

About the Contributors

Joseph E. Behar is a professor of Sociology at Dowling College, and the book review editor of JIE.

Stephen Carney is a librarian who lives and works in Edmonton, Alberta, Canada. His research interests include intellectual freedom and social responsibility, alternative library discourses, and democratic participation at all levels of social and political life.

Russell Eisenman has published more than 200 journal articles. His seven books include *The New Families* (Basic Books, 1972), *From Crime to Creativity: Psychological and Social Factors in Deviance* (Kendall/Hunt, 1991), and *Contemporary Social Issues: Drugs, Crime, Creativity and Education* (BookMasters, 1994). His research areas include creativity, birth order, crime, drugs, and sex.

David Henige is at the University of Wisconsin–Madison.

M. Wendy Hennequin is at the University of Connecticut.

Professor Feng-Yang Kuo holds a Ph.D. degree in Information Systems from the University of Arizona. He was a faculty member of Information Systems at the University of Colorado at Denver from 1985 to 1997 and is currently a professor of Information Management at Sun-Yat-Sen University, Taiwan. Professor Kuo's research interests include information ethics, cognition and learning in organizations, and human-computer interactions. He has published articles in *Communications of the ACM*, *MIS Quarterly*, *J. of Business Ethics, Information and Management*, *J. of Systems and Software*, and *Decision Support Systems*.

Tomas Lipinski is assistant professor and co-director of the Center for Information Policy Research at the School of Library and Information Science, University of Wisconsin–Milwaukee. He holds a JD from Marquette University and an LLM from the John Marshal School of Law. He received his Ph.D. from the School of Library and Information Science, University of Illinois, Champaign-Urbana.

Tim Rumbough is a professor of Communication Studies at Bloomsburg University of Pennsylvania in Bloomsburg, PA. He holds a Ph.D. (1993) in Communication from Florida State University. He has published several articles about dontroversial uses of the Internet and computer-mediated communication.

Martha M. Smith is currently auxiliary associate professor and director of the Online MS in Information and Library Services at Drexel University in Philadelphia. Lately she has been a featured speaker at ALA, PLA, and several state library association conferences on Practical Ethics in Turbulent Times. She can be contacted at <*marti.smith@cis.drexel.edu*>.

Mark Yannie has been an academic librarian, information media class instructor, and a reviewer for *Choice*; his articles have appeared in *Tech Trends*, *Catholic Library world*, and *The Christian Librarian*. He is currently a librarian with the Hennepin County Public libraries of suburban Minneapolis, Minnesota.