Code and Other Laws of Cyberspace. *By Lawrence Lessig.* New York: Basic Books, 1999. 297 pp. ISBN 046503912X.

From time to time a book is published that makes clear the changing metaphors of an age. *Code and Other Laws of Cyberspace* is one of those books. In it, Lawrence Lessig, a law professor at Harvard University, magnificently voices the need for changes in the imagining of the Internet and cyberspace, from a naturally and inherently uncontrollable, self-organizing, decentralized, and free space—"the Net interprets censorship as damage and routes around it"[1]— to a place with no Nature or Essence where user intervention is always necessary: "the Net does not take care of itself" (p. 211). With this point as a cornerstone, Lessig takes the reader through an exposition of the different kinds of what he calls "regulators," that is, the shaping forces of cyberspace. The author goes to great length to explain their characteristics, dynamics, interactions, and possible outcomes. Lessig's goal is to increase the awareness that we are all directly responsible for the creation and maintenance of a cyberspace which promotes the core values—freedom of action and of speech, anonymity, and privacy, among others—that we cherish in real life.

"If there is any place where nature has no rule, it is in cyberspace. If there is any place that is constructed, cyberspace it is" (p. 24). This is how Lessig defines cyberspace, and why he argues that the prevalent fallacy of the innate abilities of the cyberspace is wrong and perilous. It is incorrect on two different levels: It convinces us that we can sit back and relax because the Net will take care of itself, and it increases an already widespread belief in our lack of personal responsibility. "In cyberspace," Lessig argues, "we are nature" (p. 233) and our decisions are reflected in the values protected by that space. Under this light, not choosing itself becomes an active choice.

In cyberspace, just as in real space, behaviour is regulated by four different "regulators": the law, that is, what kind of behaviours and practices are legally sanctioned; social norms, that is, what is considered (un)acceptable by a community; the market, namely, the monetary costs associated with certain activities; and architecture (which in cyberspace is substituted by code), that is, the "built environment of social life" (p. 86). It is the interaction between these four "regulators" that make cyberspace what it *is*.

The effectiveness of these regulators depends on the context to which they are applied. For example, if one is trying to regulate the driving speed in a residential area one can: (a) create a speed limit (law), (b) make cars so expensive that only a few can drive them (market), (c) antagonize all those who speed in the area (social norms), or (d) place speed bumps in the most needed areas (architecture or code). In this particular case, the most effective way of behaviour control is architecture because it achieves the best results at the lowest cost. Still, it would also be possible to use all sorts of combinations between regulators, for example, establish high fines for all of those who exceed the speed limit and create a neighbourhood watch to ensure this limit (law, market, and social norms).

Lessig's argument is that in cyberspace, similar to the above example, the built environment, or code, is the most efficient behaviour regulator. This is because of the inherent artificiality of cyberspace, its lack of nature. Since cyberspace has no nature it has to be constantly (re)defined by those who create it, and this (re)definition is made by means of its code. In cyberspace "code is law" (p. 6). Code—constituted both by software and hardware—defines the possibilities and constraints of the cyberspace.

This being so, throughout the book Lessig warns of the dangers of the commercialization of code: the privatization of law and the increased ability of government to control behaviour. The first emanates from the fact that "architecture is a kind of law: it determines what people can do and cannot do. When commercial interests determine the architecture, they create a kind of privatized law" (p. 59). He cites as an example Mark Stefik's (Xerox PARC) trusted systems. Trusted systems refer to "computers that can be relied on to do

certain things. For example, suppose that a creator or publisher forbids all copying of a particular digital work. A trusted system in this context would reliably and infallibly carry out that stipulation" (Stefik, 1996, p. 226). This sort of network system allows owners of copyrighted material to distort the conventional copyright rules by "selling" a product which can not be lent to anyone else, or copied for personal use, or perhaps even not read more than once.

The second has to do with the fact that commercial entities are easier to control, which implies that "as code writing becomes commercial—as it becomes the product of a smaller number of larger companies—the government's ability to regulate it increases" (p. 52). To this extent, and even though the architecture of the Web today has been one of freedom, Lessig argues that the current move goes towards an architecture of control. And, although perfect control may never be possible, it is also not necessary. Here, the "principle of bovinity" applies, that is, "tiny controls, consistently enforced, are enough to direct very large animals" (p. 57).

Lessig presents some ways to fight this grim future: open source-code and legislative action. The open-source code movement warrants that code can be examined by all. This functions as a kind of constitutional check by ensuring that all citizens can "read" and affect the "built" environment that surrounds them. The legislative action consists of a re-adaptation of the (U.S.) Constitution to cyberspace, in order to guarantee that values that we experience today will still be held in cyberspace.

Code and Other Laws of Cyberspace is not another shiny book trying to promote the hype that surrounds most technological discourse. On the contrary, it is a dark and gloomy book where one can expect to be faced with penetrating reflections on the current state of affairs. As Lessig puts it, "I've spoken as if there could be hope. But Hope was just a television commercial" (p. 233).

Lessig's point is clear and constantly re-stated throughout the book: the current and future shape of the Net depends on and reflects our actions and inactions. In order for the Net to continue to be an instrument of freedom, we must act to protect it. This action involves informed government intervention rather than a libertarian faith in the market. The, at times, excessively legal tone of Lessig's writing is the book's only shortcoming; however, its powerful and cleverly laid out argumentation overcomes any stylistic faults. The author writes with a clarity and insight that make this book good reading and an excellent source of intellectual stimulation.

Code and Other Laws of Cyberspace possesses the signs of an instant classic and is unmistakably a seminal work for anyone interested in the social shaping and impact of the Net. It will be required reading for years to come.

Note

1. This well-known Internet quote, with its many variants, is attributed to John Gilmore (Electronic Frontier Foundation). For further information, see URL: http://cyber.law.harvard.edu/people/reagle/inet-quotations-19990709.html.

References

Lessig, Lawrence. (1999). *Code and other laws of cyberspace*. New York: Basic Books.

Stefik, Mark. (1996). Letting loose the light: Igniting commerce in electronic publication. In Mark Stefik (Ed.), *Internet dreams: Archetypes, myths, and metaphors* (pp. 219-253). Cambridge, MA: MIT Press.

Ana Viseu
University of Toronto