Harvard Journal of Law & Technology
Volume 11, Number 2 Winter 1998

THE GOVERNANCE OF CYBERSPACE: POLITICS, TECHNOLOGY AND GLOBAL RESTRUCTURING[1]

Edited by Brian D. Loader.[2]
New York, N.Y.: Routledge. 1997.
<http://www.routledge.com>
Pp. 256. $18.95 (soft). ISBN 0-415-14724-7.

The Governance of Cyberspace arose from a small conference focusing on the political and social implications of the Internet (p. xii). Held at the University of Teesside, England, in April 1995, the conference's participants ranged from social scientists to science fiction writers (pp. ix-xii). The twelve contributors (thirteen, if we include the editor, Brian Loader, who wrote the introduction) come from diverse backgrounds, yet share one thing in common: a penchant for European-style political and social science. This style of political science tends to be more theoretical and less empirical than the political science with which most Americans are familiar. Accordingly, rather than providing definitive answers to policy questions, the chapters of this book by and large merely raise questions for the reader to consider.

Rather than covering all thirteen chapters, this Book Note focuses on specific chapters which exemplify the larger issues raised in each part of the book. Potential readers of the book should then be able to discern the topics of most interest to themselves.

The political and social implications raised by *The Governance of Cyberspace* center on three questions. First, what exactly is "cyberspace"? Second, what does cyberspace mean for governance? Third, what does cyberspace mean for us as citizens? These three questions are dealt with, respectively, in Parts I, II, and III of the book.

PART I: THEORISING CYBERSPACE

Part I begins the process of examining cyberspace and its implications. Chapter 2, "Cyberspace Sociality: Controversies Over

---

1. Editor's Note: The spelling and punctuation of titles, headings, and quotations reflect the British origin of this work. Throughout this Book Note, they will be shown in their original form.

2. Brian D. Loader is Co-Director, Community Informatics Research and Applications Unit, University of Teesside, Middlesbrough, U.K.

Computer-Mediated Relationships," written by David Lyon,[3] is representative. It asks, "What is cyberspace?" in sociological terms.

Under one analysis, cyberspace challenges sociologists to explain new types of human relationships (p. 24). Computer-mediated communications ("CMCs") allow relationships to be carried on when participants are some distance from each other (p. 26). To explain such relations between people, sociologists must refine their vocabulary by, for instance, speaking of "tertiary relationships," relationships between individuals who encounter one another mostly through the aid of computers or other machines (p. 26).

Under another analysis, CMCs, rather than calling for a refined sociological vocabulary, call for a completely new sociology, one which questions the assumptions on which contemporary sociology is based (p. 24). Following this line of reasoning, "the stable self, construed as central to social relationships in most modern sociology, is now in question" (p. 28). This destabilization of the self occurs because of the opportunities offered by cyberspace for people to hide their true identities: authors of electronic material or participants in online interactions can disguise their identities and so pose as different people in different contexts (p. 28). Thus, it is perhaps no longer appropriate to even speak of a person having "an" identity; instead, we should speak of an individual as having plural, perhaps contradictory, identities (pp. 30, 34).

How compelling is this shift toward theorizing multiple identities? People have a natural need to understand,[4] and understanding often comes from synthesizing seemingly incoherent facts into a seamless whole. For example, consider a person who at times evinces the utmost piety and reverence toward God. At other times, he drinks and curses, or does other things which go against the teaching of his particular faith. A sociologist advocating the plural identities theory would say, "He is different at different times. There is no such thing as the stable self." A typical person, however, would say, "He is a hypocrite." The sociologist sees two aspects of a person and says that they cannot be reduced to one thing, since they are incompatible. The lay observer sees the same two aspects and does reduce them to one thing: a hypocrite. Are the theorists of the new sociology doing anything more than telling us to focus on a person's inconsistencies?

Yes. Their point is not simply that such a new sociological theory exists. Rather, their point is that the Internet, with its

---

3. David Lyon is Professor of Sociology, Queen's University, Kingston, Canada.

4. *See, e.g.*, ARISTOTLE, METAPHYSICS *980a ("All men by nature desire to know.").

opportunities for anonymity and heretofore-impossible relationships, gives us a strong reason to need such a new sociological theory. Cyberspace offers many opportunities to portray oneself in different guises: through anonymous chat rooms, e-mail, etc. While similar opportunities existed before the rise of cyberspace (e.g., by writing books under a pseudonym), cyberspace allows for more, and simpler, opportunities. If cyberspace becomes as pervasive as some of its proponents expect, then it may become necessary to rethink our theories of human interaction, since the ground rules will have so thoroughly changed.

Will cyberspace actually become important enough to lead to such a shift in sociological thought? Lyon thinks so. He tells us that "cyberspace challenges time-honoured notions of social reality" (p. 33). As things now stand, this is going too far. But we must forgive the author, a sociologist steeped in the lore of cyberspace, for this excess. Similarly, such excess must be forgiven of much of the book; its authors, while coming from various fields, are almost all technophiles in some sense of the word. Thus, they occasionally lose sight of the true reach of computers in our society. Rather than a world in which computer usage is widespread but occasional, the authors tend to see a society deeply immersed in computer-mediated communications, leading to major societal implications. For instance, the third chapter's[5] sociological examination of cyberpunk fiction suggests that downtowns are becoming privatized, that middle class neighborhoods are being walled off, and that poor neighborhoods are being marginalized — all because of the rise of cyberspace (pp. 41-43).

Still, Roger Burrows, the author of the third chapter, admits that "[t]his sketch of virtual culture and the new technologies of urban social polarisation is, of course, overdrawn. But ideal types, by their very nature, always are" (p. 44). As long as we recognize the latter statement, and remember that *The Governance of Cyberspace* is merely trying to discuss "ideal types" in order to further the debate about the implications of cyberspace, overstatements are excusable.

PART II: NATION-STATES, BOUNDARIES AND REGENERATION

With this caveat in mind, let us continue. Most of us still have the majority of our social encounters in person. This does not mean that cyberspace has not had or will not have a large effect on our lives, as

---

5. Roger Burrows, *Virtual Culture, Urban Social Polarisation and Social Science Fiction* (pp. 38-45). Burrows is Assistant Director, Centre for Housing Policy, University of York, U.K.

Part II shows us. Chapter 8 is representative. Entitled "The Challenge of Cyberspatial Forms of Human Interaction to Territorial Governance and Policing,"[6] this chapter asks, "How is the governance of cyberspace related to the governance of a territory?"(emphasis omitted) (p. 126). Rather than discussing the impact of cyberspace on the state's role as a *provider* for its citizens, it deals with a less discussed, but more crucial, issue: the implications of cyberspace on the state's role as *protector* of its citizens. That is, it deals with the "classical" state concerns of "[t]erritorial governance and policing," rather than "welfare" concerns (p. 126). This emphasis makes sense: if there is no classical state, there can be no welfare state. Only when there is civil order can there be anything even remotely resembling redistribution of wealth. Without a tax collector and agents to investigate and penalize non-payment, the collection of taxes necessary to fund welfare programs would be difficult, if not impossible.

Chapter 8 proposes that new technology may make the state's exercise of its classical functions more difficult (and, by implication, also impair the exercise of its welfare functions) (p. 134). New technologies facilitate the globalization of crime organizations, leave systems vulnerable to remote criminal attack, and impede state control of anti-social information (pp. 129-30). We have no way to separate these negatives of cyberspace from the positives; we can cope with them, but, unless we eliminate cyberspace, we cannot eliminate these problems (pp. 129-30; 134).

A key question raised by these issues is whether or not we should rely on nation-states to protect us from our technology (p. 134). In one sense, it would seem that we must, since we are talking about the classical functions of the state. In another sense, however, it is possible that cyberspace will mean that the classical functions of the state devolve to private individuals or to non-governmental entities. Governments "are obviously not, or not yet, adapted to this novel situation" (p. 134) of being unable to perform their classical functions in cyberspace. Accordingly, the possibility at least exists that private actors, rather than the state, can best handle these problems.

Indeed, as Part III reveals, private initiative is taking the place of government action on several fronts. In the field of copyright, technology has increased the ability to access, manipulate, and thus pirate data. Because of the inherent difficulties involved in finding and proving copyright violations, companies have come up with alternative

---

6. Klaus Lenk, *The Challenge of Cyberspatial Forms of Human Interaction to Territorial Governance and Policing* (pp. 126-35). Lenk is Professor of Public Administration, University of Oldenburg, Germany.

methods of protecting their data. Methods such as encryption of documents and required "keys" to operate CD-ROMs attempt to step in where copyright law does not or cannot (pp. 194-207).[7] In at least one field then, private initiatives are in fact dealing with problems heretofore dealt with by governments. This does not mean that governments will fail to figure out methods of dealing with these issues in the future; but it does suggest that in some ways cyberspace can expand the sphere of private action, while shrinking the sphere of government action.

PART III: POLICING CYBERSPACE: PRIVACY AND SURVEILLANCE

Chapter 11, entitled "The Future of Cryptography,"[8] continues the discussion of the relationship between cyberspace, governments, and their citizens. It does so in the context of cryptography. Cryptography protects documents stored or transmitted on computers from unauthorized access. This protection can be a two-edged sword; while it allows average citizens to protect documents and communications from a would-be thief or a prying government official, it can also shut out government officials from reading transmissions between criminals planning illegal activities (p. 177). In this way, encryption could promote what Chapter 11 terms "crypto anarchy," a condition in which governments, locked out of information due to unbreakable encryption, are unable to read intercepted communications between criminals (p. 178). As long as governments cannot decode an encrypted document, intercepting that document would reveal nothing. Even when a document could be decoded, it would take much more time and effort to do so than simply to listen in on someone's phone call. The resulting delay in investigation could result in the commission of additional crimes, extra expense to catch the criminal, or insufficient evidence to support a conviction.

On the other hand, savvy criminals currently avoid discussing plans on the phone, or in any location that could possibly be bugged. To the extent that they do so, encryption seems to offer no new difficulty. The point, however, seems to be that encryption technologies would allow not just savvy, but also mediocre, criminals to hide their activities from the government. Granted, these criminals would need to have

---

7. Puay Tang, *Multimedia Information Products and Services: A Need for 'Cybercops'?* (pp. 190-208). Tang is a Research Fellow at the Centre for Information and Communication Technologies, University of Sussex, U.K.

8. Dorothy E. Denning, *The Future of Cryptography* (pp. 175-89). Denning is Professor of Computer Science, Georgetown University, Washington, D.C.

access to computers and know how to use them. But as computers become ever more advanced, they become increasingly easy to use. The prospect of a large number of criminals using computers to plan their crimes, while somewhat farfetched currently, is on the horizon. If this occurs, law enforcement, and law and order in general, could be seriously hindered.

Fortunately, such problems need not arise, even in a highly computer-literate society. Technologies such as key escrow permit encryption, but also allow authorized outside parties access to the documents (p. 180). Under the key escrow system, a "key" to encrypted data would be provided to a fiduciary, who would provide the key only to an agency or an individual authorized to have such access (p. 180) (e.g., by a court order upon probable cause). The Chapter suggests that we voluntarily adopt such a system to prevent cryptography from becoming a real problem for law enforcement (p. 180). But such a system raises a host of questions. Would the fiduciary be a private individual or a government agency? If the former, how do we know the fiduciary could not be bought off? If the latter, how do we know that the relevant government agency will respect our privacy, or that its database containing our private keys will not be penetrable by hackers? Do we want the government so involved in our private affairs? Is the cryptography problem that large, or will it be? And how do we know if, or when, it does become large enough to get the government involved?

SUMMARY

Part III of *The Governance of Cyberspace* deals with issues of private action and reaction implicated by the Internet, while Part II addresses issues of government action and reaction. But, of course, governments and their citizens are at some level inseparable, since there cannot be a government without citizens or (arguably) citizens without government. Since each group's membership overlaps, and, in Lockean theory, a government is nothing more than the collective will of the majority of its citizens,[9] the actions of one group not only affect the actions of the other, but in some sense *are* the actions of the other.

In this way, Parts II and III of the book can be seen to be delicately entwined with each other. But this is not all. Part I deals with the question, "What is cyberspace?" As we have seen, it asks this

---

9. JOHN LOCKE, SECOND TREATISE OF GOVERNMENT § 99 (Richard H. Cox ed., H. Davidson 1982) (1690) ("And thus that, which begins and actually constitutes any political society, is nothing but the consent of any number of freemen capable of a majority to unite and incorporate into such a society." (emphasis omitted)).

question in a social rather than a technical sense. Rather than asking about the nodes and connections which make the Internet work, it asks, "What is cyberspace?" in human terms, in terms of its effects on people. In a sense, the question posed in Part I is also the question posed in Parts II and III. For, throughout the book, the focus is on the effects of the Internet on society: in other words, on the question, "What is cyberspace, as far as society is concerned?" Thus, the three parts of the book, while ostensibly asking different questions, coalesce into this common inquiry. With the current boom in Internet use, and with no end to this boom in sight, this inquiry into what cyberspace means for us is an important question for our time.

The arguments in this volume are not airtight. But into all logic an assumption must fall. In other words, as Aristotle pointed out, logic cannot rest on logic alone, but ultimately must be based on an ungrounded proposition.[10] To the extent that we accept the assumptions inherent in *The Governance of Cyberspace: Politics, Technology and Global Restructuring*, it is an informative read. Moreover, to the extent that we reject these assumptions, *The Governance of Cyberspace* forces us to examine the strength of our competing assumptions. This thoughtful and timely volume thereby accomplishes its goals of examining the effects of the Internet on society, and of encouraging a reader to do the same.

Kenneth W. Long, Jr.

---

10. ARISTOTLE, *supra* note 4, at *1006a ("[I]t is lack of training not to recognize of which things demonstration ought to be sought, and of which not. For in general it is impossible that there should be demonstration of everything, since it [the demonstration] would go on to infinity . . .").