Cyberrules: Problems and Prospects for On-Line Commerce

Debora Spar

Program on Information Resources Policy

Harvard University

Center for Information Policy Research

Cambridge, Massachusetts

A publication of the Program on Information Resources Policy.

Cyberrules: Problems and Prospects for On-Line Commerce

Debora Spar
May 1996, P-96-6

Project Director
Anthony G. Oettinger

The Program on Information Resources Policy is jointly sponsored by Harvard University and the Center for Information Policy Research.

Chairman
Anthony G. Oettinger

Managing Director
John C. B. LeGates

Debora Spar is an associate professor at the Harvard Business School and an expert in business-government relations, international cooperation, and foreign direct investment. She is the author of *The Cooperative Edge: The Internal Politics of International Cartels* (1994) and coauthor, with Raymond Vernon, of *Iron Triangles and Revolving Doors: Cases in U.S. Foreign Policymaking* (1991) and *Beyond Globalism: Remaking American Foreign Economic Policy* (1989).

ISBN 1-879716-38-0

Printing 5 4 3 2 1

September 1996

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University **Center for Information Policy Research**

Affiliates

Apple Computer, Inc.
AT&T Corp.
Bell Canada
BellSouth Corp.
The Boeing Company
Carvajal S.A., (Colombia)
Center for Excellence in Education
Centro Studi San Salvador, Telecom Italia (Italy)
CIRCIT (Australia)
The College Board
Commission of the European Communities
Computer & Communications Industry Assoc.
CSC Index (U.K.)
CyberMedia Group
DACOM (Korea)
Deloitte & Touche Consulting Group
ETRI (Korea)
European Parliament
FaxNet Corp.
First Data Corp.
France Telecom
Fujitsu Research Institute (Japan)
Grupo Clarin (Argentina)
GTE Corp.
Hitachi Research Institute (Japan)
IBM Corp.
Knight-Ridder Information, Inc.
Korea Mobile Telecom
Lee Enterprises, Inc.
Lexis-Nexis
Lincoln Laboratory, MIT
John and Mary R. Markle Foundation
Microsoft Corp.
MicroUnity Systems Engineering, Inc.
MITRE Corp.
National Telephone Cooperative Assoc.
NEC Corp. (Japan)
The New York Times Co.
Nippon Telegraph & Telephone Corp. (Japan)
NYNEX
OSCOM Communications, Inc.
Pacific Bell
Pacific Bell Directory
Pacific Telesis Group
The Post Office (U.K.)
Research Institute of Telecommunications and Economics (Japan)
Revista Nacional de Telematica (Brazil)
Samara Associates
Scaife Family Charitable Trusts
Scientific-Atlanta, Inc.
Siemens Corp.
Sprint Communications Co. L.P.
State of California Public Utilities Commission
Strategy Assistance Services
TRW, Inc.
United States Government:

- Department of Commerce
  - National Telecommunications and Information Administration
- Department of Defense
  - National Defense University
- Department of Health and Human Services
  - National Library of Medicine
- Department of the Treasury
  - Office of the Comptroller of the Currency
- Federal Communications Commission
- National Security Agency

United States Postal Service
Viacom Broadcasting
VideoSoft Solutions, Inc.
Weyerhaeuser

Acknowledgements

The author gratefully acknowledges the following people who reviewed and commented critically on this and previous versions of this paper. Without their consideration, input, and encouragement, the paper could not have been completed: Jonathan D. Aronson, Anne Wells Branscomb, Miltos Caromeris, J. J. Alexander Dyck, Brian Kahin, Jessica Korn, George C. Lodge, Thomas K. McCraw, Nancy Nichols, Richard H. K. Vietor, and David Yoffie.

These reviewers and the Program's affiliates, however, are not responsible for or necessarily in agreement with the views expressed here, nor should they be blamed for any errors of fact or interpretation.

The author extends special thanks to Jeffrey Bussgang, who conducted much of the original research used here and was co-author of a previous version of this paper published in *Harvard Business Review* (June 1996), and to Elizabeth Stein and Laura Bures, for research assistance.

Executive Summary

In societies, as in games, rules matter. They set the boundaries of permissible behavior, clarify the terms of interaction, and lay the groundwork for recognizing victors and punishing losers. When rules break down, interaction of any sort becomes a much riskier and uncertain venture.

Recently, though, an arena of business with few established rules has attracted a tremendous amount of commercial interest and enthusiasm. Since the late 1980s, the Internet has been growing at a staggering pace, doubling in size each year, and expanding its user base (in 1995) at a rate of roughly 10 to 20 percent a month. With managers scrambling to push their businesses on-line, the Net has become the focus of vast media and commercial attention. Yet what is often overlooked in this excitement is the critical importance of rules. Before the Internet can truly attract and support the wide-scale commercial enterprises its adherents foresee, it must provide businesses with the basic rules of commerce. These should include, eventually, a common conception of property rights, a systems for setting and securing the means of electronic exchange, and a mechanism for enforcing both property rights and secure exchanges. Most of these rules are still fluid and evolving.

This report explores the prospects for "cyberrules" and the processes by which such rules are likely to emerge. It starts with one simple assumption—that rules matter—and one corollary—that they matter particularly for commercial transactions. The goal is not to describe the rules of cyberspace that should evolve or who should mastermind their creation but, rather, to examine cyberspace from a rules-based perspective, exploring how law and order and standards are evolving along the cutting edge of the electronic frontier.

Contents

One

Rules Matter

In societies, as in games, rules matter. They set the boundaries of permissible behavior, clarify the terms of interaction, and lay the groundwork for recognizing victors and punishing losers. In both competitive games and civil societies, rules are intended to prevent interaction from degenerating into chaos. They provide some sense of security and predictability, informing participants of what is permissible and what is not. Even in their breach, rules are critical, because they define a violation and arrange for its punishment. When rules break down, interaction of any sort becomes a much riskier and uncertain venture. Witness the child who sulks off the playground because someone "broke the rules" or, infinitely more tragic, the chaos of Somalia, Rwanda, and the former Yugoslavia.

In business transactions as well, rules matter. Indeed, as in games more narrowly or societies more broadly defined, rules ease and facilitate commercial interaction. Despite the occasional sense of operating in uncharted or unordered territories, business for the most part operates in an environment where rules prevail. These rules can be formal, such as contract law, laws of incorporation, and antitrust. Or they can be informal, incorporating norms of commerce such as upholding a deal or paying bills within thirty days. In either case, and most frequently in tandem, these rules describe the environment in which business occurs. By clarifying what is and is not permissible, they facilitate exchange between the transacting people or firms and enable the parties to exchange goods and services with a shared concept of what this exchange entails and a shared confidence that the terms of the exchange will be met. Without this confidence, commercial transactions are liable to decline. Like children frustrated by an anarchic game or motorists reluctant to drive on a road without rules, firms may be wary of transacting unless they have some reasonable information about the basic rules of their exchange: who owns the goods or services being exchanged (property rights); how the exchange will be compensated (means of exchange); and how the terms of the deal will be structured and ensured (security and enforcement).

So basic and pervasive are these rules that they often go unnoticed by the businesses that rely upon them. Indeed, until a contract is broken or property stolen, most business executives pay little explicit attention to the underlying rules of their game. That is the beauty of rules: they aim to make the structure of the game so transparent and secure that the players can dedicate the bulk of their energies to mastery and technique. But if the rules are changing or inchoate or unknown, the game is liable to falter. This is true for sports and societies. It is true also, in many cases, for commerce.

Recently, though, an area of business with few established rules has attracted a tremendous amount of commercial interest and enthusiasm. Since the late 1980s, the Internet has been growing at a staggering pace, doubling in size each year and expanding its user base in 1995 at a rate of roughly 10 to 20 percent a month. With managers scrambling to push their businesses on-line, the Net has become the focus of vast media and commercial attention. Headlines describe its explosion as but the start of an Information Revolution (capitals optional, but generally preferred) that promises to change the conduct of commerce dramatically.

Clearly, change is underway. But what is often overlooked in the excitement about this change is the importance of rules. Before the Internet can truly attract and support the wide-scale commercial enterprises its adherents foresee, it must first provide businesses with the basic rules of commerce. These should include, eventually, a common conception of property rights, a system for setting and securing the means of electronic exchange, and a mechanism for enforcing both property rights and secure exchanges.

In the mid-1990s, most of these rules are still fluid and evolving. The legal status of electronic property rights remains ambiguous, as do the legal and practical issues surrounding on-line exchange. Enforcement authority is limited on the Internet, and few agencies exist with either the power or the predisposition to punish violators of the norms of on-line conduct.

This state of affairs, I suggest, cannot survive forever. Though portions of the Internet may remain rugged and unruled, other portions—most of them—will eventually develop their own rules and norms. The rules may vary markedly from area to area and may be governed by a host of potential authorities— governments, businesses, independent sysops, or possibly even no one at all. But there will, over time, be rules. And there will, in particular, be rules that adhere to and support commercial transactions—rules that will allow on-line ventures to run their businesses with some stability, security, and certainty.

This paper explores the prospects for "cyberrules" and the processes by which such rules are likely to emerge. I start with one simple assumption—that rules matter—and one corollary—that they matter particularly for commercial transactions. My normative claims are exceedingly limited. I by no means suggest that governments or their bureaucrats ought necessarily to rush into cyberspace. Nor, on the other hand, do I share many analysts' view that cyberspace should necessarily remain open, unregulated, and free for all. Indeed, I say very little about what form of cyberspace is most desirable or what role governments ought to play in shaping its evolution. Rather, my concern is restricted to describing what I see as an inevitable aspect of on-line development: There will be rules in cyberspace, and the shape and makers of these rules will in time affect how we go on-line and what we do there.

My definition of "rules" is deliberately kept open and inclusive. Rules, in my view, encompass far more than the explicit rules and regulations of any particular state. They include international agreements, commonly accepted practices, cultural norms, and businesses' standard operating procedures. They include, in short, the "rules of the game"—standards that define what is permissible and acceptable and that, in one form or another, can effectively be enforced and maintained on-line.

My goal is not to describe how such rules should evolve or who should mastermind their creation, but, rather, to examine cyberspace from a rules-based perspective, exploring how law and order and security and standards are evolving along the cutting edge of the electronic frontier.

Two

From Science to Sales:
The Commercial Evolution of the Internet

> *Someday the Internet may become an information superhighway, but right now it is more like a 19th-century railroad that passes through the badlands of the Old West. As waves of new settlers flock to cyberspace in search of free information or commercial opportunity, they make easy marks for sharpers who play a keyboard as deftly as Billy the Kid ever drew a six-gun. Old hands on the electronic frontier lament both the rising crime rate and the waning of long-established norms of open collaboration.*
>
> — Paul Wallich[1]

The Internet got its start in the late 1960s as a communications infrastructure called ARPANET, run by the Department of Defense and its Advanced Research Project Agency (ARPA). Consisting of a series of links joining together discrete computer networks, the ARPANET was an experiment in "internetworking," designed to give university research scientists an opportunity to create a solid "network of networks" to facilitate the exchange of scientific and military information and save the costs of replicating computer capabilities at multiple sites. Taking advantage of recent developments in computer technology, and trying also to make the system impervious to nuclear attacks or natural disasters, the developers of the ARPANET structured the system in a highly decentralized manner.

Over time, this decentralized network of networks became known as the Internet. Following the model of the national telephone system (and even employing many of its connections), the Internet's pathways remained out of sight and mind to its users. No one needed to know how messages moved from one site to another, only that they got there securely. Unlike the telephone system, however, the architecture of the Internet allowed any single user to broadcast a message simultaneously to any site on the network. This possibility reflected the Internet's scientific purpose: to enable an elite corps of researchers to share critical information. Given this purpose, the Internet's founders saw no need to restrict access to the system or to embed within it any means for controlling the flow of information. On the contrary, in the late 1960s and early 1970s, before the advent of the personal computer, it was reasonable to conclude that anyone with the technical means to access the Internet would be from the very scientific or engineering community that the system was designed to serve.

[1] "Wire Pirates," *Scientific American* **270**, 3 (March 1994), 90.

For roughly twenty years, this community quietly flourished on-line. Expanding rapidly from just four host computers in 1969 to nearly two thousand by 1985, the Internet became a common mode of communication among university researchers, government scientists, and a handful of outside computer engineers. Funding for the creation and maintenance of the system's infrastructure came from the National Science Foundation (NSF), which during the course of the 1980s took responsibility from the Department of Defense. As computer use expanded and then exploded in the 1970s and 1980s, so too did the Internet grow. Academics from outside the hard sciences began to communicate via e-mail, as did the increasing legions of software writers and computer company employees.

As discussions grew to incorporate new entrants, electronic bulletin boards were formed, and for the first time, people began to "meet" in cyberspace. Still, the culture of the Internet remained akin to that of a small, like-minded community. Users were overwhelmingly computer-literate, highly educated, and scientifically minded. Many were hackers, and commerce had no place in their slowly expanding community. Indeed, NSF policy explicitly discouraged any use of the Internet for nonscholarly purposes.[2]

By the late 1980s, this policy had effectively disappeared. Aware of the growing commercial interest in the Net, as well as its own budgetary limits, the NSF began slowly to privatize it. Initially, private firms just provided infrastructural services to the Net's established user base. Then in 1989, commercial service providers emerged, offering Internet access to a wide new range of private and commercial customers. In 1990, the Internet was officially opened to commercial ventures. As a result, the Net was transformed. In the early 1980s the Internet community consisted only of about 25 linked scientific and academic networks. By 1995, when the last piece of the NSF backbone was retired in favor of higher speed, privately owned backbones, the Net had grown to include over 44,000 networks extending to 160 countries and including 26,000 registered commercial entities.[3] Extending far beyond academe and the Defense Department, users numbered somewhere between 40 and 50 million in 1995, and were increasing by an estimated 10 to 20 percent a month.

More than just a quantum increase in numbers, the entrance of the "newbies" meant a fundamental change in the culture of the Internet and the community it had spawned. Arriving on-line primarily through servers such as Prodigy or America Online, these new users

[2] The NSF's acceptable-use policy statement read in part: "NSFNET Backbone Services are provided to support open-research and education in and among U.S. research and instructional institutions, plus research arms of for-profit firms when engaged in open scholarly communication and research. *Use for other purposes is not acceptable.*" Cited in Michael Sullivan Trainor, *Detour: The Truth About the Information Superhighway* (San Mateo, Calif.: IDG Books, 1995), 175. (Emphasis added.)

[3] Philip Einer-DeWitt, "Welcome to Cyberspace: What Is It? Where Is It? And How Do We Get There?" *Time* **145**, 12 (Spring 1995), Special Issue, "Welcome to Cyberspace," 4; Sullivan-Trainor, 175.

understandably had little interest in the research questions that had bound previous users together. The newbies were also largely unfamiliar with much of the Internet's specific protocol or with the systems that sat at its foundation. Cyberspace for the newbies was simply an adventure—an opportunity to meet people, gain information and, ironically perhaps, recreate a sense of small-town intimacy and immediacy. But many newcomers also came to cyberspace for profit—to explore the potential of a vast new realm and stake a claim in the technology that promised to revolutionize the nature of transactions. As a result, the Internet's relatively new business district—the *.com* domain—quickly swelled to become the largest sector of the Net, and the transformation of commerce seemed well underway.

Three

Uses and Users

Amidst all this enthusiasm, it might easily be supposed that nearly all commercial enterprises had moved their entire businesses on-line, from Time Warner to IBM to the local flower shops. But as of mid-1996, commercial uses of the Internet remain relatively narrow and well defined. Essentially, the Internet remains just a conduit for sending and receiving bits of information. As such, it can serve business either as a means of delivering information about other tangible goods or as a means of directly transmitting information-based, intangible goods.

In the first case, use of the Internet has no effect on the good being sold or the means of its delivery: a raincoat purchased from L.L. Bean's home page is still a raincoat and will still arrive by truck or plane—that is, by an inherently mechanical means. Because of the nature of what they sell, tangible goods firms cannot transmit their products electronically. Instead, going on-line entails using the electronic medium of the Net to interact with existing customers and entice new ones. The difference lies less with the product or its production than with the way in which it is sold and marketed: the services that surround the commercial process.

Accordingly, most companies that produce tangible goods have seized upon the Internet largely as a means of providing customer support and low-cost advertising. The pioneers in this area are computer manufacturers, whose commerce on the Net emerged quite naturally from their communication on the Net.[4] Silicon Graphics, for instance, the multibillion dollar leader in workstations, uses e-mail to share problem-solving techniques with its customers and distributors, saving the company an estimated $5 million a year in reduced service calls.[5]

Other on-line pioneers included retailers such as the Internet Shopping Network and Timberland. In many ways, their conversion to electronic commerce is more telling than that of the computer manufacturers: seeing computers sold and serviced on the Net, after all, is hardly a shock, given that the people who buy workstations are among the oldest travelers on the Internet. Cubic zirconium and hiking boots, however, are a different matter, because they are hardly the "techie" products initially expected in cyberspace. And yet, increasingly, there they are, along with the full range of products from such retailers as Crate & Barrel, Sharper

[4] In 1994, for example, three of the leading U.S. computer manufacturers—Sun Microsystems, Silicon Graphics, and Digital—estimated that between 70 and 90 percent of their customers already had access to e-mail over the Internet. See Lisa Thorell, "Doing Business on the Internet. Case Studies: DEC, Silicon Graphics, and Sun," *Internet World* 5, 5 (July-August 1994), 53.

[5] Ibid.

Image, Neiman Marcus, Sara Lee, and a host of other mail-order firms lining up in cybermalls.

But however large they grow, the malls will always be constrained by their physical incompatibility with electronic commerce, because the products they sell—the raincoats, jewelry, and boots—are entirely tangible. The Internet may affect the ways in which these goods are sold, or serviced, or marketed, but it does little to alter the underlying nature of the business.

By contrast, electronic commerce in *intangible* goods raises the prospect of a fundamental shift in the nature of exchange. Unlike tangible goods, intangible products such as software and financial services themselves consist largely of information. So long as commerce was based primarily on tangible exchanges, providers of intangible products were compelled to convert their bits to atoms, packaging inherently intangible products into tangible forms. Thus, financial service providers built banks and provided tellers, while software creators put information on plastic disks and wrapped them in brightly colored boxes. Now, however, the Internet, as an electronic conduit for information, offers these providers the opportunity to discard tangible packaging and return to their basic intangible product. This change is radical, and it presents business with tempting new opportunities.

Consider the sale of software. Like computer manufacturers, the firms in the $80 billion software industry are ideally situated for doing business on-line. Their employees and customers both tend to be technically sophisticated and to own the physical conduits—the terminals—that connect them to the Net. Unlike computer firms, though, software producers can actually distribute and service their product electronically. Using the Internet, they can allow customers to download directly the software and manuals they desire. They can also provide customers with databases of support information and answer electronically their most common questions. Through these means, providers can significantly lower their costs of distribution and technical support.[6] Over time, on-line sales have the potential to restructure the software industry altogether, because the electronic medium allows software creators to reintegrate the distribution function previously ceded to other firms. Or as Laurent Pacalin, Director of Worldwide Electronic Distribution for Oracle Corporation, a leader in database software, observed, on-line distribution allows the software company to "leapfrog the box-pushers and deal directly with the customers."[7] And so the "box-pushers," like many

[6] Product distribution costs alone (disk duplication, diskettes, manuals, and shipping costs) typically account for 20 percent of a software firm's costs. For more on the possibilities of on-line distribution, see George Lawton, "Software Distribution Through the Internet," *Software Magazine* 3 (March 1995), 29.

[7] Notes from personal interview by Jeffrey Bussgang, Jan. 31, 1995, p. 19.

intermediaries, may be left behind, their packaging rendered obsolete by direct electronic exchange.

Similar changes are likely to befall publishing companies, whose products of information and text lend themselves quite naturally to electronic commerce. As with software, on-line "distribution" promises to reduce publishers' costs by significantly eliminating paper, printing, binding, warehousing, and circulation. It also offers publishing firms novel ways of mixing and manipulating the product they offer. With the rapid development of digitally based multimedia technology, "published" information need not consist only of text and still photos. Instead, on-line publishing can allow "readers" to mix together sound, video, and text-based information. Magazines can invite any "reader" with a terminal to interact directly with authors, or to receive only certain types of stories. Already, on-line magazines such as *HotWired* have emerged to take advantage of this evolving electronic format, armed with the philosophy that just as "television wasn't radio with pictures, the Net isn't magazines with buttons.... Instead, this is a new medium demanding new thinking, new content."[8]

As in the software industry, much of the new thinking demanded by on-line publishing focuses on new ways of packaging the published content. The old way was relatively simple. Publishers put the content—book, magazine, or newspaper—between two tangible covers and left it to the reader to move sequentially through the enclosed information. For those who did not want to read all of the text, tables of contents or indexes served as a road map and allowed for nonsequential choosing or skimming. But that was the extent of the options. With electronic publishing no such constraints exist. Instead, the very structure of the medium encourages users to move from topic to topic, article to article, with little concern for linear order. This structure also encourages the growth of new intermediaries to wade through the barrage of on-line information and retrieve and customize it for specific groups or individual users. Consequently, even as electronic publishing threatens to destroy some segments of the existing industry, it promises to create others. The repackaging of the product will undoubtedly bring about a massive restructuring of the industry.

A similar restructuring is probable also in the financial services industry. If electronic commerce progresses as its adherents expect, it will have a profound impact on banks and brokerage services. Again, the source of change lies in the intangibility of the product being sold, and the impetus for change is sharply reduced cost. If banks and other financial service providers ultimately sell information, and if they can sell this information electronically, they will have less need for the tangible trappings that have surrounded their business in the past. Or as Shikhar Ghosh, Chairman of Open Market, notes, "Banking is a pure information

[8] Quoted from *HotWired*'s "welcome" message to subscribers (April 1995).

business...so why invest in furniture, buildings, vice presidents?"[9] Indeed, why not move to a model of business based on transactions, rather than relationships? Under the current system, people bank with a bank. They choose an institution and route their transactions through it. If, however, banks truly move their business to the Internet, the nature of this relationship may be subject to change. Because the processing costs for moving money electronically are negligible, on-line banking implies that customers will be able to open and close accounts effortlessly. Banks may then find themselves competing on new ground, developing different means for wooing and maintaining their traditional customers.

What this means for the banking industry, and for the myriad businesses linked to the current banking and financial systems, is unclear. At a minimum, though, it means that commercial interaction may be pushed further away from a personal or relations-based mode of exchange and closer to a purely transaction-based mode. This, after all, is one of the more compelling commercial prospects of the Internet: to make individual transactions accessible, immediate, and inexpensive.

Put into a historical perspective, this transformation is even more profound than many current analysts have noted. Historically, the evolution of commerce has depended on and coincided with the evolution of institutions to secure the means and rules of exchange. Because transacting—giving away one good in exchange for another—is inherently risky and costly, institutions and relationships have emerged over time to mediate these risks and costs and allow for exchange to proceed. The history of these relationships and institutions surrounds the history of commercial evolution. It begins with primitive exchanges (three pigs for a cow) that rest almost everywhere on personal familiarity and are limited to the scope of a trader's immediate circle of contacts. Driving the need for familiarity is the risk inherent in the transaction: if the cow dies the following morning, the unfortunate purchaser wants some recourse to the seller, and the best means for assuring that is to know precisely who the identity and location of the seller. Security comes also from the knowledge that the traders will transact again, thereby reducing the likelihood that either will succumb to the temptation to cheat the other.[10] For interaction to progress beyond the limited bounds of familiarity, the traders (and their society) must develop institutions that allow them to replace personal ties with more formal and impersonal ones. As societies develop such formal ties, commerce expands beyond the community and economic growth ensues. The nature of the ties—such as private property, contract law, a common currency, and a means of enforcement—is to reduce the cost of transactions and ensure security in the absence of a long-term personal relationship. As transactions become more complicated (overseas purchasing, foreign

[9] "Open Market," Harvard Business School Case N9-195-205.

[10] This can be represented more formally as the familiar observation that cooperation is more easily achieved when interaction is iterated over time.

investment, corporate mergers, futures trading, junk bonds) so, too, must the rules evolve, reducing the risks and costs that remain inherent in exchange.

What the Internet does, particularly for intangible products, is to push this commercial evolution into its next, electronic phase. Moving ever further away from the personal relationships of primitive commerce, it promises to reduce business to its most basic component: the transaction. Theoretically at least, the technological prowess and open architecture of the Net should allow millions of users to transact with one another anonymously, immediately, internationally, and inexpensively. This is the radical commercial promise of the Internet.

Yet, what those who make this promise often neglect to consider is that even this radically new form of commerce will demand and require a supporting set of rules. Like successful commerce in any other space or time, it will need rules of property, rules of payment, and rules of security. It will need some entity to ensure the sanctity of possession and the security of exchange. It will need some means to punish those who cheat, or steal, or trespass. At the moment, most of the rules and rulers remain in their infancy.

Four

The Rules of Exchange

"It's business on a lawless frontier."

— Michael Wolff, Internet author[11]

Once upon a time, the Internet had rules. In its earliest days, the Net was very much a community of like-minded individuals who developed clear codes of conduct and working norms of behavior. Their rules were rarely written or even explicit, but they did not have to be, because they were widely observed by all those traveling on the Net. Just as early automobile drivers developed the rules of the road, so the early Internet users developed their own norms of behavior. They created symbols to express emotions such as joy [:-)] and sorrow [:-(]. They created rules, such as Don't-change-the-subject and Read-the-FAQ-file, and they even created a language of sorts, with expressions such as "FAQ," "flame," and "spam."[12]

Despite its reputation as the untamed realm of hackers, the early Net was actually an organized, orderly community. The strength of its rules was powerfully demonstrated in 1994, when a now infamous pair of Arizona lawyers posted an advertisement for their services on hundreds of electronic bulletin boards, bombarding many uninterested users with multiple copies. Seeing the advertisement as a violation of the Net's then existing norm against private commerce and "junk-mail," thousands of users "flamed" the lawyers' office with a torrent of hate mail and cyber-threats. With this spontaneous response they demonstrated not only the power of on-line norms but also the ability of the Internet community to monitor and enforce these norms, punishing violations with on-line's closest approximation of force.

Since the lawyers' venture, however, the norms have themselves come under attack, besieged by an onslaught of newcomers. These newcomers are by no means bad for the Net; indeed, they (even the derided newbies) are the ones with both the mass and the power to alter how the Net is used and what it can do. But because they come from beyond the scientific and engineering communities, and particularly because they want to use the Internet

[11] Jared Sandberg, "Computer Experts See Hackers Gaining an Upper Hand in Fight Over Security," *Wall Street Journal*, Jan. 24, 1995, B-4.

[12] A "FAQ" (frequently asked question) file contains answers to questions that many people ask when first joining a discussion. FAQs exist to prevent on-line discussions from bogging down by repeated introduction of the same topics. "Flame," both a verb and a noun, refers to the extremely harsh criticism (generally too harsh for real life) to which Internetters often subject one another. "Spam," also a verb and a noun, refers to unsolicited e-mail inappropriately floods flooding mailboxes.

as a means of conducting business as well as correspondence, their participation breaks the existing rules and demands new ones. In particular, mass participation on the Internet requires at least three sets of rules: rules of property rights, rules of currency, and rules of enforcement.

Five

Property Rights

All economic systems are based on a shared understanding of property rights. Developed usually over decades or even centuries of evolution, these rights clarify the basis of ownership and exchange. They provide a consistent way of defining who owns what and how these possessions can be transferred from one owner to another. In the basic example above (p. 12), for instance, property rights establish that Person A owns the cow and is willing to exchange it for the three pigs. Without well-accepted rules of property, the exchange either would not occur or would be exceedingly costly. Someone else could always just take the cow by force or stealth. Property rights reduce the costs of exchange by clarifying ownership and providing some means for punishing those who violate it. They define not only possession but also theft.

In modern market economies, property rights also provide the incentives that drive innovation and growth. If property is communal or property rights ill defined, no one in the community has an incentive to produce anything more than can be consumed. What creates the incentive, and thus what drives technological and economic progress, is a system that clearly defines private property and enables the owner of this property to appropriate it for individual benefit.[13] Without the ability to appropriate rents from private property, few people in any community would be willing to invest in specialization, or technological advance, or even a particularly hard day's work. To generate these types of investments, communities and economies must therefore create and preserve rules of private property.[14] And as economies evolve, they must ensure that their property rights evolve as well.[15]

[13] Marxists, of course, would insist that the communal state represents the natural and desirable condition of economic organization. With a handful of exceptions, though, it is exceedingly difficult in the 1990s to find evidence of the long-term viability of an economic system based on communal rights.

[14] The argument of this section draws extensively on the work and writings of Douglass C. North. See, in particular, North, *Structure and Change in Economic History* (N.Y.: W.W. Norton & Company, 1981); and North and Robert P. Thomas, *The Rise of the Western World: A New Economic History*, (Cambridge, Eng.: Cambridge University Press, 1973).

[15] In this context, it is interesting to note that at every major junction in the evolution of capitalism, the transformation of commerce has coincided with and been facilitated by a change in the structure of property rights and the incentives they create. Hunters and gatherers became farmers once they developed the means to protect "their" lands; feudal lords turned to commerce once they were allowed to own and bequeath property; and oceanic exploration flourished once the kings of Europe offered bounties for discovery and cleared the seas of pirates. Where property rights fail to develop, economic growth stagnates, as is the case in the less-developed world. Insufficient property rights can also explain the demise of Soviet-style commerce, where property rights were clear (all in the hands of "the people") but did not establish the incentives necessary to fuel economic growth. What allowed the system to grow, by contrast, was a rigid structure of state-controlled disincentives (coercion). Once the coercive apparatus declined, so too did any substantial economic activity.

This connection between property rights and commerce applies with full force to the Internet. For even if electronic commerce fundamentally transforms the nature of business, it does not eliminate business's basic need for an infrastructure that clarifies ownership and allows owners to reap the economic rewards of their possessions. At the moment, however, there is only a limited system of on-line property rights. The Net instead approximates a free-for-all in which information is often regarded as a public good and common practice is "what's yours is mine."[16] This norm of sharing was eminently reasonable in the early days of the Net, when its purpose lay in facilitating communication among researchers. As a norm for commercial activity, sharing is less reasonable. It simply will not work, because few entrepreneurs have a long-term interest in sharing their product. They may want to advertise the product on the Net, they may even want to sell it directly on the Net, but they also want to make money from it—to appropriate the rents of ownership and recoup the costs of investment and innovation. So long as all information on the Net is treated as common property, this cannot be done.

What makes the issue of on-line ownership so troublesome is that ownership almost always refers to information, to bits rather than atoms. And despite a spate of recent developments, owning bits is still difficult, because most legal systems are based primarily on tangible rather than intangible property. The most generally applicable laws, those of copyright and intellectual property, are relatively underdeveloped and often contentious. They also vary dramatically across countries.

To understand the extent of the problem, consider the three industries described earlier: software, publishing and financial services. In each the product being sold is essentially information: text and ideas. On the Internet, these goods can be disseminated and reproduced at extremely low costs, which presumably gives the author of the text or the originator of the ideas new ways of distributing the work. It also potentially denies them the proceeds from this work. For once information is transmitted into the vast and anonymous realm of cyberspace, it can be endlessly copied and altered—inexpensively and without detection. That is why the Internet is such an exciting development for people who want to access information. That is also why it demands caution by firms in the business of selling information. No firm that creates property wants to leave this property untended and unprotected in an accessible public space. Yet this is precisely the dilemma that information-based firms face as they consider the move toward electronic commerce.

Understandably, then, firms that deal in the business of information are approaching the Net with caution. The Recording Industry Association and the Walt Disney Company both initially held back, worried that their products might be not only misappropriated but also

[16] Anne Wells Branscomb, *Who Owns Information? From Privacy to Public Access* (N.Y.: Basic Books, 1994), 6.

actually changed or misrepresented on-line.[17] Similarly, the Smithsonian Institution has limited electronic reproduction of its artistic works, reasoning that "at least for now...cyberspace is a chaotic wild west frontier full of highway bandits and subject to only the roughest kind of vigilante justice."[18]

At the root of the problem for all these companies is the inapplicability of existing copyright law to electronic commerce. Even in the United States, where copyright laws are arguably the most advanced, "original works of authorship" are defined as "fixed in a *tangible* medium of expression...from which they can be perceived, reproduced or otherwise communicated."[19] Even though the central statute governing copyright law was explicitly amended in 1980 to cover software programs, its extension to electronic transmission remains vague.

According to Bruce Lehman, commissioner of the U.S. Patent and Trademark Office, "Existing copyright law doesn't make it clear that it is a violation of the copyright owner's rights to distribute a protected work over the Internet."[20] Or as Nicholas Negroponte puts it, "all copyright law is essentially a Gutenberg artifact, bound to paper and constructed in ignorance of the digital age."[21] So long as this digital gap exists, anyone who makes intellectual content available on the Internet will be risking that their content—their intellectual property—will be broadly distributed without their consent and with little, if any, economic return. For anyone or any firm that makes a living from intellectual property, these risks are simply too large. Even those who do not intend to profit from their intellectual property may want to retain control; actors, for instance, might not want their faces or voices clipped from one movie and inserted into another, nor might authors want their words rearranged to serve others' themes or purposes. But under the existing norms of electronic commerce, firms have no secure means to prevent these practices, so the Internet remains a "lawless frontier," where intellectual property is potentially up for grabs and ownership lies often in possession.

There is, of course, a fairly obvious way to solve the problem of property rights. If this problem is the absence of law, then a solution may rest—historically has often rested—with the creation of law by a central government. In cyberspace, that law would come, most probably, from an extension of existing copyright law. Because copyright already deals with

[17] See Otis Port, "Halting Highway Robbery on the Internet," *Businessweek* (Oct. 17, 1994), 212; and Max Frankel, "Cyberights," *The New York Times Magazine*, Feb. 12, 1995, 26.

[18] Ralph Blumenthal, "Thieves in the Idea Marketplace," *The New York Times*, Feb. 11, 1995, 1-13.

[19] Copyright Act of 1976, as cited in Dorothy E. Denning and Herbert S. Lin, *Rights and Responsibilities of Participants in Networked Communities* (Washington, D.C.: National Research Council, National Academy Press, 1994), 87. (Emphasis added.)

[20] Quoted in "Writing Copyright Law for an Information Age," *The New York Times*, July 7, 1994, D-4.

[21] Nicholas Negroponte, "A Bill of Writers," *Wired* (May 1995), 224.

intangible products such as ideas, and because it provides for the commercialization of intellectual property, its extension into cyberspace would seem to make a great deal of sense. By guaranteeing owners of intellectual property that their information and ideas would remain "theirs" on-line, copyright law should allow information-based firms to move more confidently on to the Internet. Accordingly, lawmakers in Washington have recently been tinkering with the statutes of copyright law. In September 1995, a working group convened under the auspices of the White House Infrastructure Task Force recommended changes in the language of the 1976 copyright law to include transmission explicitly as a form of distribution. The working group also endorsed a "fair use" provision that would limit any noncommercial use of intellectual property that damages the legal owner of the property.

If enacted as law, the working group's provisions will do a lot to protect the property of firms that transact in cyberspace. But they still won't do nearly enough. First, copyright law is already among the most intricate and esoteric areas of law. Courts vary widely in their interpretation of existing statutes, and even in their understanding of the laws' intent. The extension of these laws into a whole new realm of commerce is almost certain to create great clouds of ambiguity and uncertainty, leaving courts and litigants to fumble toward new definitions of private property and property rights. Second, because the laws are national, they will have only a limited influence on the international transactions that proliferate on the Internet. Even if the laws stop a Cincinnati-based firm from covertly downloading a U.S.-based competitor's software or textbook or database, they may not stop the same firm, or any other, from routing the download through a computer in Bangkok or the Netherlands. Third, even if the laws were applied at the global level (and there is talk of doing so under the auspices of the new World Trade Organization), the laws still do not provide the means for a commercial provider to determine whether its information has been altered or copied in cyberspace. The laws also provide no technical solution to the problems involved in tracing on-line violations. Even if a firm suspects that its product has been stolen, how can it find the thief, especially if all transactions can be routed through multiple sites and untraceable user-ID's?

There is also another problem concerning any legal or governmental solution: the Net does not want it. Ideologically, the Net is still composed of those who see information as the ultimate public good, something that fundamentally transcends the realm of private property. Quoting Thomas Jefferson, for instance, *Wired* magazine recently commented that "ideas should freely spread from one to another over the globe, for the moral and mutual instruction of man, and improvement of his condition.... Inventions...cannot, in nature, be a subject of property."[22] Though often less eloquently expressed, the notion of public information permeates the Internet. So does the more radical belief that governmental intervention

[22] Quoted in "The Economy of Ideas," *Wired* (March 1994), 88

anywhere on-line represents an unacceptable invasion of privacy, even of freedom. As commercial interests enter the Internet community, such sentiments may easily be diluted, especially given that commercial providers stand to benefit from the extension of law into cyberspace. A strong disinclination toward regulation seems likely to remain on-line for some time, as indicated by a leading industry consultant's claim that "the federal government has the unique power to do things really badly really fast."[23]

Who, then, will write the rules for protecting intellectual property in an electronic age? One possibility is that no one will, and that the rules will remain in their present vague and inchoate form. If so, then electronic commerce is liable to stagnate. It may not, like CB radio, almost overnight go from technological hot-shot to toy, but neither will it become a significant forum for commercial activity. Instead, the Net will remain much as it is right now—a beehive of activity and experimentation, a channel for mass communication and correspondence, but a channel in which information is exchanged only for free, rather than for profit. This would not necessarily be a bad fate for the Net, but it would be quite different from the scenario that most Internet adherents currently foresee.

A second possibility is that these same adherents will themselves create the rules of electronic commerce. Facing a void of legal rules and definitions, they will adopt practices and develop technological means that work to preserve their property on-line and ensure some means of recouping their investments. These practices and technologies will not, of course, have the status of law, but over time they may become the standards of electronic commerce, much as the customs and practices developed by medieval merchants eventually became commercial law in Europe.

This is not to imply that firms can, by themselves, create laws of intellectual property. They cannot, because they have neither the legal mandate nor the physical means of enforcement. At some point, governments are likely to be essential to the process, especially insofar as they retain the ability to punish those who would break the rules. But in the search to protect their own property interests on-line, firms and entrepreneurs may begin to create the procedures that become the basis of law. Every time, for instance, a firm pays for software on-line, or reimburses electronic authors for copies of their work, the firm is establishing a precedent of electronic ownership. Similarly, every time firms limit their distribution to a well-defined list of customers, they reinforce the right of property and create some technical means for securing such a right. Even the most sophisticated technical system, of course, cannot operate in a legal void, and ultimately distribution channels can only be secured in an environment where unauthorized access is clearly defined and punishable as a

[23] Peter Huber, quoted in Paul Andrews, "Cyber-Thinkers Ask Government to Stay Off the Digital Highway," *Seattle Times*, 23 Aug. 1995, A3 [NEXIS].

violation of law. As this law evolves, however, corporations, rather than state agencies, may shoulder the bulk of the development.

Six

Means of Exchange

If firms become the creators of on-line property rights, they will be acting not out of direct interest in the rules of electronic commerce but rather from a defensive, almost instinctual interest in preserving property. Their concern is will probably lie, not with the system of property rights per se, but with the specific cases of their own property and their own means of financial preservation. By contrast, a second area of on-line rules—the rules and means of exchange—is explicitly about the rules themselves and is already compelling firms to venture directly into the rulemaking business.

As described above, property rights are the foundation of any market-based system. They are the fundamental institution, the rules of the road upon which any economic exchange depends. The means of exchange are more prosaic and tangible. Rather than defining the rules in any significant way, they provide the means by which they operate.

In most economic systems, the means of exchange is money: currency of one form or another is widely accepted as payment for transactions. Though the form of currency has evolved over time—from shells to gold to coin, cash, and checks—the rules and processes surrounding it have remained largely the same. Typically, currency is issued by a central government that retains a monopoly over its creation and backs it with fractional reserves of gold, precious metals, or other countries' currencies. Even when the currency is not directly backed by a tangible asset, the government's management of its supply creates a value based on confidence (that the government will always accept it as a store of value) and scarcity (that there is never quite enough to go around).

In contrast to the rules of property, which must change to meet the demands of electronic commerce, these existing rules of money could probably function quite well as a means of conducting electronic exchange. Even in cyberspace, consumers can order goods priced in dollars (or yen or marks), charge them to a credit card, and let banks intermediate the financial transaction. Nothing intrinsic to electronic commerce forces the existing means of exchange to adapt. There are no technical obstacles to routing and recording even nontraditional transactions through this well-established route, no new demand for financial oversight or regulation.

Instead, the source of change lies with the vast financial opportunities that electronic commerce appears to present. Specifically, it lies with the instantaneous and nonphysical nature of electronic transactions. If electronic purchases become commonplace, they will probably include such minute transactions, dubbed "micropurchases," as buying an article from the *Atlantic Monthly* or browsing through three minutes of the *New York Times*. The cost of processing such services through the traditional route would overwhelm the price of the service itself; for small on-line entrepreneurs, cost could even doom the business from the start. But if payment could occur electronically and instantly, then the cost of transacting would plummet, allowing commercial activity to flourish on-line. As an added benefit, electronic exchange potentially could function like cash, allowing both buyer and seller to maintain anonymity. With a wallet full of "e-cash", buyers could browse quickly and anonymously in cyberspace. Without needing to rely on credit cards, bank tellers, and checkbooks, they could save both time and money. This is many observers' seductive vision of Internet commerce—fast, cheap, and completely anonymous.

Technologically, the creation of electronic money rests with the issuance of an anonymous electronic note. An institution sells electronic money to its customers, coding the e-cash onto a wallet-size card or transmitting it directly to another on-line merchant. It debits the amount of the e-money, plus a small transaction fee, from the customer's old-fashioned account. Three aspects of this process are critical: (1) that electronic transfers remain anonymous; (2) that they remain secure; and (3) that transaction fees remain minimal. In the past, similar requirements were met by agencies of a central government. Governments printed the currency, allowed it to circulate anonymously, punished those who stole or copied it, and covered their expenses through taxes. On the Internet, however, no central authority establishes the means of exchange. National governments have shown little interest, because e-cash raises troubling questions for them and their law enforcement agencies. How, for instance, will e-cash expand the possibilities of tax evasion and money laundering? And how will governments track the assets of individuals or the trading balances of states? If e-cash proliferates, it is liable to allow many aspects of economic activity to escape the scrutiny of government agencies. With these issues looming, government agencies have little incentive to play any role in the creation of e-cash.

For private firms, however, the incentives are great. First, there is the simple cost-cutting potential of electronic payment. Many firms, and particularly banks, have a considerable interest in cutting the costs of intermediate transactions and moving directly to electronic payment systems. Several institutions, such as Citibank and Wells Fargo, already employ proprietary software systems that allow customers to do their banking on-line. As banks and other financial systems increasingly compete in new and fluid ways, such payment systems could well become critical to their success.

The real prize, though, will probably come from pushing electronic payment out of proprietary networks and into the broader reaches of cyberspace. Eventually, the value of e-cash, like the value of any currency, will be determined by the market's demand for it. To increase demand, the currency must be widely accepted. In the past, governments ensured acceptance simply by proclaiming their currency "legal tender." In the future, the game may become significantly more competitive. Firms that establish the most accessible and secure means of exchange will capture the market of all those seeking to conduct electronic transactions beyond internal borders. Success in this game will breed further success, because the acceptability of a currency increases its attractiveness to other users.

Accordingly, the race to develop the means of electronic exchange has already become one of the most spirited competitions in cyberspace. Much of this race is about technology, and winning will entail the refinement of encryption algorithms and secure "electronic wallets." But because technology alone cannot support a full-fledged system of electronic exchange, the race is also about rules. If payment systems are ever to proliferate along the Internet, they will probably require a trusted entity to oversee and regulate their use. The issue—much broader than the widely publicized threat of credit card theft—is the confidence with which any major financial institution can hope to approach the Internet. Many such institutions already engage in electronic commerce, moving vast sums of money through their own internal networks or via external proprietary networks such as SWIFT (the Society for Worldwide Interbank Financial Telecommunication). But performing these transactions in a closed and controlled network is very different from allowing them to occur across the conspicuously public spaces of the Internet. If such firms are to move onto the broader reaches of the Net, they will need some means of recourse. They will need, at a minimum, to know that some identifiable and credible entity is backing the value of their money and preventing widespread fraud and abuse. Historically, these tasks have fallen to governments. On the Internet, private firms might well find themselves performing equivalent functions, creating and maintaining the rules of electronic exchange. In the process, they are likely to stumble on a third critical area of rules: rules of security and enforcement.

Seven

Security and Enforcement

Rules of security and enforcement are, to a large extent, the crux of the matter for Internet commerce, and perhaps even for the broader reach of Internet communication. Yet rules are only as good as the capacity to enforce them. Without enforcement, rules are meaningless—words or notions without either compliance or commitment.

In cyberspace, rules of enforcement will be particularly important for the maintenance of property rights and the establishment of the means of exchange. For property rights to function on-line, the rights must not only be clear but also secured and enforced: knowing that the information (software, book, financial data) is legally yours does no good if others can easily access it and use it without fear of punishment. Similarly, the entire concept of electronic payment rests with the ability to make these payments secure: to guarantee that no one can steal or counterfeit electronic cash and that any possible perpetrators will be traced, apprehended, and punished.

Ensuring the security of property and transactions is an age-old problem, one that has generally been solved by the coercive powers of an outside authority. Often coercion issues from the state: modern governments, for instance, consistently retain the power to punish and imprison those who steal others' property or counterfeit currency. In other instances, coercion comes from private forces. The Sicilian Mafia and the Cali cocaine cartel, for example, both employ extensive private security forces to ensure that the intricate rules of their games are upheld. In still other cases, property rights are upheld by embedded community norms, such as those of an Israeli kibbutz. In all of these cases, some entity ultimately determines whether the rules have been broken and how the perpetrator should be punished. Despite their obvious differences, the modern state, the Mafia, and the kibbutz all share certain key characteristics: they are governed by an accepted set of rules and norms, and they have the means and the authority to enforce the rules of their realms.

The Internet, as said earlier, has no central authority. As information travels along the complex network of networks, it passes through many different computers and sorters, with separate packets potentially crossing various international borders. This far-flung and unpredictable architecture, which is precisely what makes the Internet such a powerful and impervious medium, also turns enforcement of any sort into a particularly thorny problem. The open structure of the system means, inherently, that there is no central point of control—there is, to put it colloquially, "no *there* there."

This architectural resistance to authority poses no problem for many of the Internet's uses and users. Indeed, for many functions—anonymous chatting, cross-border advertising, "underground" information—it is a tremendous, really unprecedented boost. For commercial users, though, the lack of control is more problematic, particularly with regard to issues of property rights and the means of exchange. Before firms transfer large chunks of their valuable information on-line, and before they employ novel systems for electronic payment, they will need some guarantee that their property and their payment will be safe in cyberspace. But the decentralized structure of the Internet makes such guarantees difficult to offer or enforce. No policing agency controls the multiple point of access, and no government has defined precisely what constitutes theft or how an anonymous "thief" could be traced, identified, or apprehended on-line. Even if governments were to define precisely the rules of cyberspace, and even if they somehow managed to establish the means of catching cybercriminals, on-line enforcement would still be plagued by the overwhelming issue of national borders. In cyberspace, information can cross borders instantly and imperceptibly, but laws, and their enforcement, remain creatures of the tangible realm, attached to the territory from whence they are issued. As a result, the prospects for on-line enforcement remain uncertain.

Eight

Conclusions

As stated at the outset, this paper is about rules. Beginning with the assumption that rules matter, I have tried to describe the extent to which the absence of rules may hinder the development of commerce on the Internet and the kinds of rules that need to emerge before commerce can reach its full on-line potential.

The topics of "rules" and "Internet" may strike some, initially, as unrelated. Because the Internet developed as an open and free-wheeling community, it has grown to pride itself on its very lack of rules and absence of authority. But, as I have suggested, there actually were rules, very strong and well-developed rules, in the early days of the Internet. And there will have to be new rules developed and enforced as the Net evolves to incorporate a new and very different base of users.

So long as rules are seen in their broadest sense, including norms and practices as well as formal laws, most observers would probably agree (even begrudgingly) that rules of some sort are necessary in cyberspace, and that enforcement mechanisms of some sort must also accompany them. Where disagreement lies is over the content of the rules and, especially, the nature and identity of the enforcer.

This last section offers a brief description of a range of possibilities for ruling the Net. My aim is not to not to suggest which one is most likely, or even most desirable. Rather, I want only to explore what the range of options looks like, what advantages and disadvantages each contains, and how a movement toward any one of them would affect the subsequent evolution of the Internet.

The first possibility is that Internet users will continue to eschew any type of formal rules or government-sanctioned authority in cyberspace. This appears to be the outcome predicted and desired by groups such as the Electronic Frontier Foundation, which argue that "governments of the Industrial World...are not welcome among us...[and] have no sovereignty where we gather."[24] If this view prevails, and if centralized authorities are effectively banished from cyberspace, the Internet of the future may resemble in some ways the Internet of the recent past. It will be primarily a medium for the free flow of information, a channel for open and anonymous communication, and a realm in which a handful of informal rules emerge slowly, piecemeal, and without any real penalty for their violation. Insofar as

[24] John Perry Barlow, "A Declaration of the Independence of Cyberspace," quoted in Catherine Yang, "Law Creeps onto the Lawless Net," *Businessweek* (May 6, 1996), 58

information is generally regarded as a public good, the Internet will not be a realm particularly well-suited to commerce—which to those espousing this view may not be a bad outcome.

A second and very different possibility is that the cross-national structure of the Internet will eventually demand an international system of regulation and enforcement. This view is popular with many international civil servants already working to develop a suitable framework for ruling the Internet. In the spring of 1996, for instance, the Geneva-based World Intellectual Property Organization (WIPO) completed a draft treaty for a series of amendments to the Berne convention that aims to expand international copyright convention to include electronic transmissions. As with most international agreements, the WIPO treaty suggests a delicate balance between international and national governments. An international body would act to develop and arbitrate a set of global rules, while actual enforcement of the rules would remain in the hands of national governments. As expressed by its supporters, this approach to cyberspace has many advantages. It makes the rules explicit, applies them across the breadth of the Internet, and taps an appropriate enforcer. As with most international agreements, however, effectiveness depends on the commitment of its members. If users around the world disregard the treaty's provisions, or if governments fail to enforce them, WIPO, or any other international organization, can do little in its defense.

Accordingly, many national governments have recently moved to strengthen their own controls over cyberspace. In 1996, the U.S. government passed the contested Communications Decency Act; Germany upheld its decision to prosecute the U.S.-based company CompuServe for the transmission of pornographic materials; and China made clear its desire to establish a closed and patrolled national service called Intranet. Although none of these measures deals directly with the commercial uses discussed here, they nevertheless describe a model that could be applied to property rights and means of exchange. The model is an obvious one, even a fairly common one. As technology creates new means of interaction, governments step in to rule and regulate these areas of interaction, using their traditional powers of coercion to ensure that the rules are upheld. Even in the age of cyberspace, this model is compelling. It is clear, it is transparent, and it fits well with the expectations and sensibilities of most citizens—especially those who might bristle at the thought of either cyber-anarchy or international regulation.

Yet, as stressed throughout this discussion, the traditional model of government-as-enforcer does not readily translate to cyberspace. Detecting violations, tracing violators, and dealing with crimes that can cross borders all are problems that defy easy solutions. In addition, the most far-reaching attempts to rule and police cyberspace have been greeted, at least in the United States, with nearly complete derision. The Communications Decency Act has been criticized not only as unconstitutional but also as unenforceable. The Clipper chip—a proposal (1993) of the National Security Agency (NSA) that would have enabled the government to eavesdrop on all electronic transmissions—was denounced by those who saw it as an unconstitutional invasion of privacy. Thus, although national governments remain, potentially at least, the obvious source for the creation and enforcement of on-line rules, any steps toward increasing government's power in this sphere are bound to be fraught with both political and technological barriers.

Which brings me to the fourth and final possibility for on-line enforcement. This is the possibility that firms, rather than governments, will begin to establish the rules of cyberspace. Recall that firms have perhaps the most to gain from going on-line. Yet before they make this leap en masse, firms will need to have in place the basic rules of the game: rules of property, security of exchange and means of enforcement. If neither national nor international governments are well positioned to make and enforce these rules, then business entities might begin to fill the vacuum.

Already, evidence suggests that such a movement is underway. Rather than lobbying governments to create and support the rules of Internet commerce, firms such as Microsoft, America On-line, and Open Market are effectively writing the rules themselves. Specifically, they are using both technology and organizational structure to support enforceable systems of property rights and secure exchange.

To a large extent, these firms are relying on technology to provide the security that commerce demands and governments cannot yet provide. Two approaches in particular are generating considerable interest: encryption and firewalls. With advanced encryption systems, firms can protect both property and exchange. They can guarantee that information and payment are genuine and that they are received only by a certain user, or group of users. With firewalls, firms can physically enclose their corner of the Internet, restricting access to their commercial interactions and, as necessary, to their intellectual property.

These technologies become potentially even more powerful when coupled with a business model that creates, in effect, an enforcer. Already, early forms of enforcement exist in on-line service providers such as America Online and CompuServe. Even though these providers thus far have limited themselves only to minimal services (access and navigation), they could easily move to the much higher value-added services associated with rules and rulemaking. They could, for instance, provide access only to certain groups, or cluster their users into communities linked by similar interests or needs. Armed with the appropriate tracking and billing technologies, service providers could potentially perform the crucial functions of intermediation and enforcement. They could track their users, bill them, and pay their content providers. They could also guarantee both users and providers that violations of the rules would be punished, probably by expulsion from the service provider's community.

In effect, these firms could create and enforce the rules of commerce in their own orderly and well-defined corners of cyberspace.

In many ways, this last possibility is the most attractive to proponents of Internet commerce. If firms can establish and support commercial communities, then they can have the orderly and rule-bound commerce that many desire without the governmental involvement that many fear. Yet, as with the other possibilities for ruling the Net, this one has its obstacles and drawbacks. It allows for the firms that write the rules to become exceedingly powerful and to control vast amounts of data. It also pushes these firms into the potentially uncomfortable position of enforcer. Most seriously, the scenario described by private rulemaking—one of walls and guards and tracked purposes—is the precise opposite of the open market and universal access that have characterized the Internet to date. It is also apparently at odds with the free-flowing democracy that mass electronic communication is often thought to foster. Insofar as private firms develop and enforce the rules of Internet commerce, they may simultaneously constrain, or at least restrict, the options for open and noncommercial interaction.

For the purposes of this paper, I will not be so foolhardy as to suggest which of these four possibilities represents the most viable path for the evolution of on-line rules.[25] My point instead is to suggest that rules will matter greatly in cyberspace. Each of the paths I have described carries its own set of costs and benefits, winners and losers. Each would shape the subsequent evolution of the Internet in a different way and establish different balances of power among society's competing groups. They will define what the game is about and who gets to play it. Real power will reside with the marshals of the new frontier—not those with the fanciest wizardry or the hottest sire, but those who rule the Net.

[25] I have been foolhardy elsewhere, however. See Spar and Jeffrey J. Bussgang, "Ruling the Net," *Harvard Business Review* (May-June 1996); see also Spar and Bussgang, "Ruling Commerce in the Networld," *Journal of Computer-Mediated Communication* 2, 1, a special issue on "Emerging Law on the Electronic Frontier," edited by Anne Wells Branscomb, Harvard University Program on Information Resources Policy (June 1996) [on-line].

Acronyms

ARPA	Department of Defense Advanced Research Project Agency (its communications infrastructure was called ARPANET)
FAQ	Frequently asked questions
NSA	National Security Agency
NSF	National Science Foundation
SWIFT	Society for Worldwide Interbank Financial Telecommunication (Belgium)
WIPO	World Intellectual Property Organization (Geneva)

PPSPAR

ISBN 1-879716-38-0