# Educom Review

## Learning, Technology and the Atomic Hypothesis
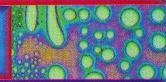
• • • • •

## Hurrah for Supreme Wisdom

## Communing WITH John Perry Barlow

• • • • •

## Dorothy Denning ON Encryption Technology

## COMPUTER-MEDIATED INSTRUCTION: From Theory to Practice

## THE MEDIUM is NOT THE MESSAGE

## EDUCATIONAL MICRO MARKETS

## Why the Internet Will be Regulated

## PUTTING LEARNING ON TRACK

$3.95 • Canada $4.95

09

0 74470 84560 7

Baker • Gehl • Gifford • Graves • Hale • Noam • Rezmierski • Ruth • Twigg
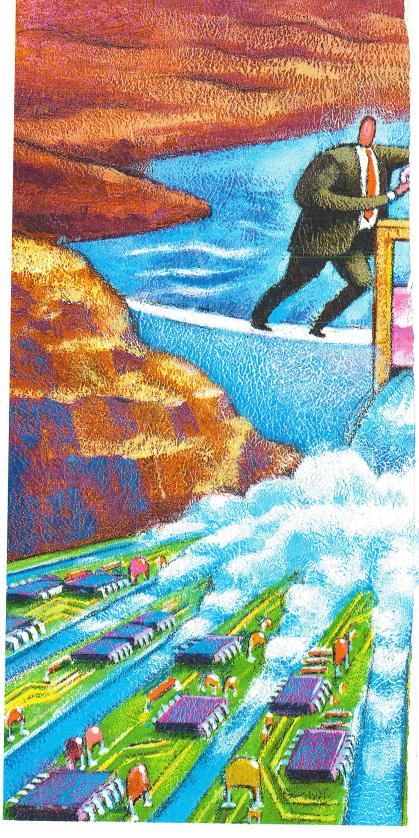
# Why the Internet will be Regulated

*BY* ELI NOAM

A s electronic transactions over the Internet become more common, the question arises whether they will be controlled on the national and international levels. Many Internet enthusiasts dismiss this question as irrelevant: "You cannot regulate the Internet."

Their fallacy is to believe that the Internet is only electronic, which indeed is hard to control. But communications are not just a matter of signals but of people and institutions. Senders, recipients and intermediaries are living, breathing people or institutions with physical domiciles and physical hardware. The arm of the law can reach them. It may be possible to evade such law, but the same is true when it comes to tax regulations. Just because a law cannot fully stop an activity does not prove that such law is ineffective or undesirable.

This argument, most emphatically, does not mean that we should regulate the Internet. But that is a normative question of values, not one of technological determinism. We should choose freedom because we want to, not because we have to. And that choice will not be materially different from those which societies generally apply to the panoply of activities. Why should computer communica-

Eli Noam is professor of finance and economics at Columbia University's Graduate School of Business and director of the Columbia Institute for Tele-Information. enoam@research.gsb.columbia.edu

tions be different? As the Internet moves from nerd-preserve to office park, shopping mall and community center, it is sheer fantasy to expect that its uses and users will be beyond the law. This would seem obvious. Just consider what will happen when the cooperative spirit of the Internet is broken by software programs deliberately set to lie, cheat and harm others. Today, for better or worse, each society will apply its own accumulated wisdom, prejudices, self-interests and misconceptions to the rules governing the Internet. For better or worse, new situations lead to more rules, not less.

In communications, one should take cognizance of a simple but basic principle: every time one makes a new communications flow relatively more convenient, powerful and cheap, one also makes a traditional communications flow relatively less convenient, less powerful and more expensive.

Changes will affect every single one of society's institutions, just as the industrial revolution changed every one of the feudal structures. But for every revolution there is a counter-revolution. And just as the industrial revolution of the 19th century led to the romantic movement as a reaction, so does the information age lead to a neo-romantic longing for the lost golden age. The leading edge, as always, is the protection of children and the support of public safety. The Communications Decency Act was one such response. The Supreme Court overturned this law unanimously in June of 1997 because the U.S. has a very strong free speech protection in its Constitution. Lower courts have overturned similar laws in several states in the U.S. But for other forms of conduct, and transactions where fewer Constitutional protections exist, the restrictions will be more enduring. Fearful of that potential, the White House issued in July 1997 a report by Ira Magaziner which criticized economic regulation of Internet transactions and advocated establishment of an Internet "free trade zone." However, a close reading of the report does not indicate a move by the federal government toward lessened economic regulation of those things it cares about. The report's ringing language is hence largely directed at efforts by other governments—states and other countries—to impose economic regulation on the Internet.

As countries attempt to impose their national rules on Internet usage, they encounter the problems that their rules can be undercut. Information flows rapidly and cheaply and can be routed to less restricted jurisdictions. Kids can run electronic circles around stodgy national rules.

Similar leaks to national content rules abound. Therefore, countries will attempt international regulatory arrangements to support national restrictions.

Thus, rules have the tendency to expand geographically. An example is data privacy. Here, several smaller European jurisdictions initiated protective arrangements, and then discovered that these were being undercut by non-conforming practices elsewhere. This led to expansion of the geographic scope of the rules. The German state of Hesse was the first to introduce data laws in 1970. In 1977, this was expanded to all of Germany; in 1995, to the European Community. And now, the EU has been setting rules to prevent data flows to "non-conforming" countries, in effect seeking adjustments by other countries. As this process continues, it becomes increasingly difficult to ever change the initial rules.

Structurally, such international rules could be established in several ways.

- Supranational organizations with regulatory powers.
- Two-level regulation with preemption.
- Harmonization by treaty, ad-hoc negotiation, administrative coordination, or non-binding recommendations by international bodies.
- Dispute resolution.
- Recognition of foreign laws.
- Law enforcement collaboration.
- Collaborative self-regulation by private firm.
- User coordination—an example is the voluntary self-governance of the Internet.

In any cartel situation, there are incentives to break it and become a nonuniform "haven." Examples include large countries for whom international interaction may be small relative to its cost, such as the United States, which, e.g., can still afford a non-metric system of measurements. At the other extreme, small countries or states also provide examples of non-conformity in regulation: Liechtenstein in banking; Delaware in corporation law; Monaco in taxes.

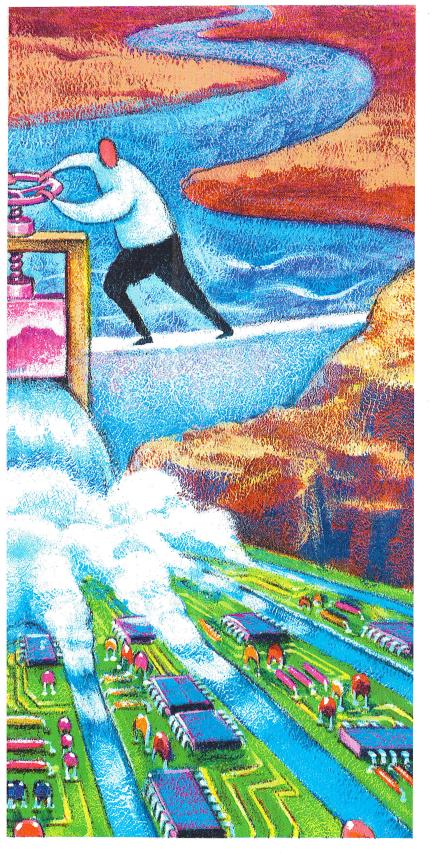Internationally, content-based regulation is near impossible. Content rules depend on values that differ in different societies. Major examples are sexual and political expressions. If an international agreement is a compromise, neither country will be happy. If countries recognize each other's rules, it would require them to be enforcers of others, which is unlikely in many cases. Imagine the United States cracking down, on behalf of the Chinese government, on Chinese dissidents in San Francisco.

Therefore, if international rules are unstable, the primary regulatory action will have to be taken by a country, not by international arrangements. What tools will a country then use? The answer is: the ones that affect these factors that are less mobile than electronic bits—people and physical assets. This means that a country will regulate static and physical elements rather than mobile or intangible ones, such as content, information and transactions. If one cannot grab the bits, grab the user or their non-mobile assets. For example, instead of trying to collect a sales tax (i.e., a tax on a transaction, conducted over the Internet, and hard to reach), governments may, for example, try to tax the transport of the sold merchandise (a "UPS tax").

As this process takes place, why stop at the national level? The control of land assets, for example, has historically been done more effectively on the local level. Thus, Internet regulation may also emerge locally. Also, new types of communities will emerge in which various actors may participate voluntarily. In time, they become self-regulating jurisdictions.

The conclusion is that the information society will be regulated in a fashion more reminiscent of the feudal age than the cyber age: controls will be levied on people and property, not on income or transactions. Inter-governmental agreements will be ineffective. And alternative forms of jurisdiction will emerge that are not tied to territoriality and locality.

Thus, as the cyber age liberates information, it will lead, paradoxically, to stricter controls over individuals and tangible property. More freedom for virtual cyberspace means less freedom in the traditional physical space.　ᴇʀ

and licensed. Organizations can be held liable for content on their computers, available to employees. Routing tables can be controlled. Taxes and tariffs can be levied. Anonymous re-mailers could be outlawed. Access prices can be set. URLs and domain names can be controlled.

This is not to say that such rules, or similar ones, are desirable. But they are unavoidable. China is building an Internet backbone that is connected to the world through only set control points. Arab nations are not allowing their citizens full Internet access and are censoring the WWW. Singapore has laws against "improper" usage of the Net, and controls all ISPs.

In Germany, Bavaria is at the forefront of pornography protection on the Internet. The French, on the other hand, to paraphrase Prof. Henry Higgins in "My Fair Lady," do not seem to care about such things, as long as they are conducted in the French language. Internet servers located in France must be in French. This French preoccupation, just as single-minded as the American one regarding U.S. control over encryption technology, is based on its own fears of terrorism, communism and drugs.

In the past, France had approached computer communications energetically, centrally, but ultimately unsuccessfully. First, it commissioned a beautiful official study, the Nora-Minc report, still the most literate report about the information economy, even 20 years later. With the study identifying the strategic-geopolitical need to fight IBM, which compared to such past global powers such as the Roman Catholic Church and the Communist International (just at the time that two American youngsters, Steve Jobs and Bill Gates, began their successful assaults on IBM), the French government poured money into computer development and micro-management. Such an approach had worked magnificently for French railroads, but it failed for computers. Today, there is almost no French presence in micro-computers, the heart of the information revolution. What industry there is, is largely becoming (outside the defense sector) a subcontractor in return for market access.

Second, the French government created the Minitel system, controlled and financed by the state telecommunications monopoly. It even gave away the terminals for free. All state organizations contributed content. As a result, France became the undisputed world leader in Videotex. The problem was only that Videotex was leapfrogged by the hardware and software that flowed, in a largely unplanned way, from a bunch of upstart American and European institutions, with much sharing, giving away, stealing, chaos. How can one expect a phone company to manage such a process? Today, the Minitel is a technologically backward system. Its usefulness rests on its convenience as a billing system. As soon as the Internet overcomes the billing hurdle of secure micro-payments, Minitel will slide into a secondary status. President Jacques Chirac, who saw his first computer mouse only in December of 1996, dismissed the Internet as "an Anglo-Saxon network." With that kind of a signal to the implementing bureaucracy, the Internet is likely to be regulated in France in various ways.

More rules, because new problems will emerge. And more also, because there will also be an entirely new layer of rules—those set by the various electronically defined communities that are forming.

The techniques for control will vary depending on the target. Transmission backbones can be set and controlled. Interconnection and traffic hand-off points can be regulated. Internet service providers can be held liable, and they could be licensed. Hardware can be required to have a screening chip. Content providers can have their servers traced