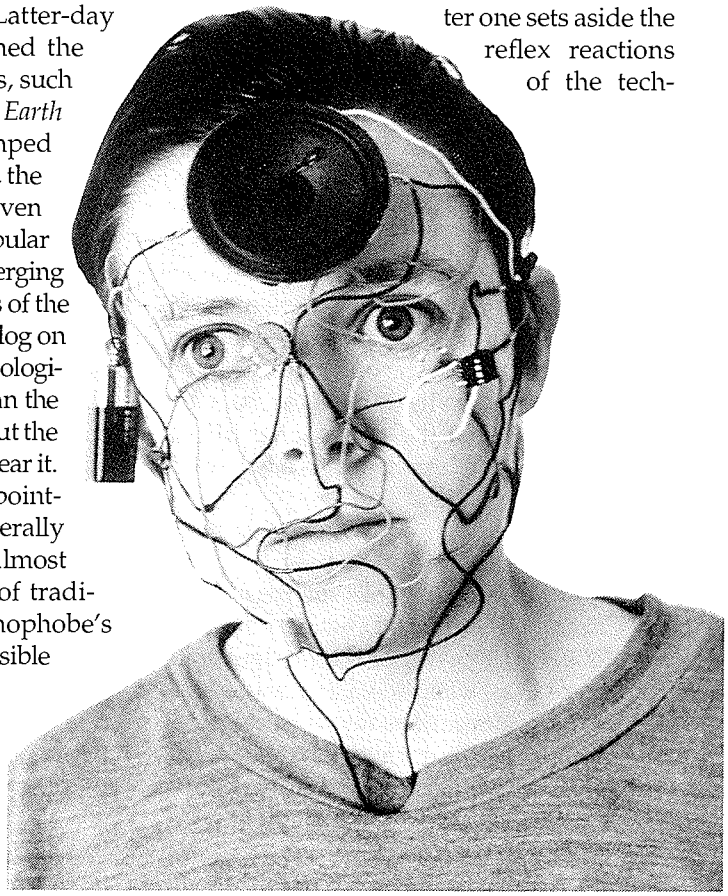
THE CULTURAL CONSEQUENCES OF THE INFORMATION SUPERHIGHWAY

BY TOM MADDOX

The coming of the information superhighway, or, more modestly, the National Information Infrastructure (NII), has reanimated America's running debate about the vices and virtues of technology. It has also reshuffled the ideological deck in interesting ways. Latter-day counterculturalists who have joined the ranks of the technological optimists, such as Howard Rheingold of the *Whole Earth Review*, find themselves encamped alongside the likes of George Gilder, the onetime apostle of Reaganomics. Even as Theodore Roszak, one of the popular prophets of the 1960s, assails the emerging "cult of information," staid members of the academic establishment scramble to log on to the Internet. In truth, these new ideological divides are little more helpful than the old, for it is as right to be hopeful about the future unfolding before us as it is to fear it.

As technophobes are fond of pointing out, technology's effects are generally unpredictable, often negative, and almost always produced at the expense of traditional ways of life. From the technophobe's point of view, therefore, a moral, sensible response to the NII is to reject it in principle and fight against it with whatever means are at hand—to sabotage it intellectually and combat the policies that would bring it into being.

Persuasive as some of its concerns may be, such a neo-Luddite view of the NII seems beyond the pale of serious consideration. As a people we are wont to explore the paths along which our desire leads us, and it seems virtually foreordained that our desire will lead us to build and use the NII. Even after one sets aside the reflex reactions of the tech-



nophobe, however, there is much reason to feel uncertainty and anxiety over the NII. The history of electronic media, especially television, is a powerful reminder that new information technologies can easily be turned to malign ends. Through advertising and other means, they have been used not only to exploit our hearts' desires but to manufacture new ones. Along with the specter of greater government control over citizens' lives that becomes possible with the new information technologies, this "commodification of desire" must be considered one of the darker prospects of the NII. Add to it the inescapable unease one feels in contemplating a wired world, an almost subliminal fear of the accession of what historian Manuel de Landa, in *War in the Age of Intelligent Machines* (1991), calls the "machinic phylum"—the set of things that operate according to the machine's laws of rationality and order. To put these fears more succinctly, with the NII, it seems likely that the machines will grow stronger, as will marketers and governments.

It is possible that another, less defined group, at once the weakest and least organized and also the most numerous, subtle, and relentless, can wrest control of the NII. That is the group of each of us, insofar as we represent ourselves and not the need to consume, on the one hand, or to behave obediently, on the other—each of us as we represent what the philosopher Michel Foucault called "a certain decisive will not to be governed."

Certainly, in many situations this group has virtually no voice and no power. Against it, Foucault insisted in books such as *Madness and Civilization* (1961) and *Discipline and Punish* (1975), is the power of the modern state. And there is as well the vast array of businesses and organizations that exist primarily to sell us images of our wants and needs, to ply us with our own fantasies. Their most effective and characteristic medium is commercial television, where the advertising surrounds and overwhelms a content that, as MTV videos and elaborate "infomercials" illustrate, increasingly becomes indistinguishable from it.

The same groups can be seen working, along with others, to create the NII. Government spokespersons and telecommunications industry flacks ply the media promising manifold blessings, at least to citizens of the United States. "All Americans have a stake in the construction of an advanced National Information Infrastructure," according to a U.S. government "Agenda for Action." "Development of the NII can help unleash an information revolution that will change forever the way people live, work, and interact with each other." In *Business Week*, an MCI Telecommunications ad fantastically asserts: "The space-time continuum is being challenged. The notion of communication is changed forever. All the information in the universe will soon be accessible to everyone at every moment." All because of a dream known as the information superhighway and a vision known as network MCI. The pitchman's hyperbole and the government's bland assurances alike should tell us that we are being hustled, worked—like a crowd standing in front of the ring-toss stand at a traveling carnival.

Note the two passages' common theme of changing things forever: "communication," according to MCI; "the way people live, work, and interact," according to the government. Oddly, just here, where the hyperbole appears to be at its worst, both advertising agency and government are telling the simplest of truths: Should the NII come to pass, it will change things forever. Like the magician's showy gesture or the pitchman's barked promise, these declaiming voices serve to distract our attention from something else: in this case, the subtler, more disturbing truth that no one—neither the White House nor MCI nor anyone

***Tom Maddox** is writing coordinator at Evergreen State College. He is the author of* Halo *(1991), a science fiction novel, and a columnist for* Locus *magazine.*

else—can predict the nature of the changes that will be brought about by the NII.

Consider some of the characteristic technologies of the last 100 years: the telephone, the automobile, the radio, the television, and the computer. At the time of their inception and for many years afterward, no one understood the implications of their invention and use. Sociologist Colin Cherry, writing about the history of telephone systems, says, "The new invention can first be seen by society only in terms of the liberties of action it currently possesses. We say society is 'not ready,' meaning that it is bound by its present customs and habits to think only in terms of its existing institutions. Realizations of new liberties, and creation of new institutions means social change, new thought, and new feelings. The invention alters the society, and eventually is used in ways that were at first quite unthinkable." That the automobile would become such a common killer of adolescents, for example, or the telephone a powerful instrument for the gratification of a distinctive brand of aural sexual pleasures that did not exist as such before its invention—who could have predicted these and a myriad other such things?

"Mechanical properties do not predestine the development and employment of an innovation," social historian Claude Fischer notes in his study of the social consequences of the telephone, *America Calling* (1992). "Instead, struggles and negotiations among interested parties shape that history. Inventors, investors, competitors, organized customers, agencies of government, the media, and others conflict over how an innovation will develop. The outcome is a particular definition and a structure for the new technology, perhaps even a 'reinvention' of the device."

One could write the history of the broadcast media in the United States in very similar terms. When radio stations began broadcasting in the 1920s, they sprang up almost at random and did pretty much what they wanted. "Radio" was still up for grabs; the nature of the medium was undefined. Advertisements, for example, were extremely controversial in the early days, many people (including Secretary of Commerce Herbert Hoover) holding that the airwaves should be employed for the public good, not for commercial purposes. In 1927, motivated in part by the need to keep stations on separate wavelengths, Congress created the Federal Radio Commission (FRC), directing it to regulate the radio waves according to "public interest, convenience, and necessity." This remains the standard for the regulation of broadcast media today by the FRC's successor, the Federal Communications Commission, the justification for de facto censorship of radio and television and other regulation of program content.

There were dissenters, of course. Radio preacher Aimee Semple McPherson, who in fact trampled all over other stations' wavelengths, telegraphed Washington:

> PLEASE ORDER YOUR MINIONS OF SATAN TO LEAVE MY STATION ALONE STOP YOU CANNOT EXPECT THE ALMIGHTY TO ABIDE BY YOUR WAVE-LENGTH NONSENSE STOP WHEN I OFFER PRAYERS TO HIM I MUST FIT INTO HIS WAVE RECEPTION STOP

Despite her plea, the situation was becoming clear: If the Almighty wanted to go on radio, he would have to play by the U.S. government's rules. Anybody who has listened to much radio or watched much television can draw his or her own conclusions about how well those rules have served the public interest, the public convenience, or the public necessity. Whatever defects unregulated radio and television might possess theoretically, it is difficult to imagine that they would be more numerous and thoroughgoing than those of the existing regulated varieties.

The NII today is in a condition much like that of radio during the 1920s. The stakes, however, are much greater. Through the NII, it may become possible for businesses and

"Emoticons" (viewed sideways) are a popular form of expression among some E-mail users. These are from the book Smileys *(1993).*

:-)
standard smiley

:-(
sad smiley

:-D
very happy smiley

:-o
amazed smiley

arms of the government to acquire an intimate knowledge of every citizen—what we love and hate, what compels us and what we ignore—and with it perhaps the ability to manipulate our needs and our behavior. Every choice we make could be recorded, as could every moment of consumer bliss or image consumption. We could be profiled in terrifying detail, almost casually, as a kind of side-effect of the network software. Viewed this way, the NII becomes the Panopticon triumphant, to borrow Michel Foucault's notion of a machine for constraining our desire within socially acceptable limits, on the one hand, and commercially viable ones, on the other.

The experience of the Internet suggests how this can be prevented. It shows that the individual users of telecommunications and computer technology can sometimes achieve a kind of victory by wresting control of the technology. Originally created by the Pentagon to keep defense-related computers connected even in the aftermath of a nuclear war, the Internet has become one of the prime sites of many kinds of individual and collective activity. Almost from the beginning, the Internet has served the individual's purposes with enormous flexibility—as much as, if not more so, than it has served the institutions that brought it into being. As personal computers became nearly ubiquitous during the 1980s and Internet connections commonplace, they unlocked possibilities entirely unforeseen by the technicians or the managers who oversaw the system. Defense Department bureaus found their employees swapping recipes; staid and reputable organizations of all sorts found their members or employees engaging in unlicensed and uncontrolled debate, discussing the theory and practice of sado-masochism or chatting about whatever they wished with people from all over the world. In short, while the technology (of computers and networks) made such things possible, it neither anticipated nor encouraged them, nor could it stop them.

Perhaps we can expect more of the same from the NII. If, as seems likely, there emerges out of today's struggles and negotiations over the new medium considerable freedom for individuals in their use of the NII, people will exploit it in currently unimagined and unsanctioned ways. To many people, some of what occurs will seem wasteful, disgusting, obscene, sexist, racist, even criminal; to others, merely vulgar and depressing. Some already lament the waste of network resources—or "bandwidth"—resulting from the storage and transmission of binary files of explicit sexual images or from "anti-social" modes of behavior such as "flaming" (i.e. sending abusive E-mail to an individual one finds annoying). Such practices stand as honorable evidence of that "certain decisive will not to be governed," and so we must protect them above all, as we must protect the speech that most offends us and the religious beliefs we find most stupid and repulsive.

Presidential smileys

=I:-)
Abe Lincoln

:(=)
Jimmy Carter

:'}
Richard Nixon

7:^]
Ronald Reagan

=:o]
Bill Clinton

In fact, because the new information technology we are creating seems to lend itself more readily to improvisation and freedom than to rigid planning and control, it is not unreasonable to hope for triumph. Still, the possibility remains that the NII could turn into a largely one-way street, one where "consumers" receive information but will not have freedom to retransmit or alter it. This is the "500 channels of TV" model, the worst scenario for the future because it implies an audience composed of inert consumers and passive paracitizens, easily manipulated by any technically adept spin doctors with access to the profiles. Many of today's cable television providers are eager to offer just this sort of service.

The history of American broadcast media is not greatly encouraging. Network and local programming alike have proceeded according to unspoken canons of propriety that defy adult standards of free speech and journalistic practice. As a result, we have a national standard of infantilized media, which allow necessary human chaos only as it sneaks through in the form of eroticized violence and violent eroticism, both typically subtextual, subliminal, and dishonest. If we wish the NII to escape such a malign fate, we should work toward an opaque and open NII, one that, for instance, allows universal and near-anonymous access, guarantees the individual the right (which the government does not currently do) and means to encrypt information, and provides individual control over content, both outgoing and incoming. Taken together, these technical attributes would combine to create an NII that might actually serve us without entangling us even more in the embrace of commercial and governmental forces.

Telecommunications and computer technologies are themselves also forces to contend with. Building the NII, we create a vast and productive niche for the enlargement of de Landa's "machinic phylum," worlds in which machines can grow and evolve, and this eventually may have profound implications for human consciousness. Even in the relatively primitive forms it takes today, information technology seems to encourage a fixation on virtual rather than real experience—on technologically mediated perception, not direct apprehension. It can also saturate us in a hypnotic image-repertoire that works to render us passive and dream-struck no matter who, if anyone, controls it.

%*@:-(
smiley with hangover

:-{#}
smiley with braces

=8->
nerd smiley

M-) :X) :-M
see no evil, hear no evil, speak no evil

Marvin Minsky, the dark knight of the information age, generally considered, along with John McCarthy, one of the founding fathers of the field of artificial intelligence, said in a speech a few years ago that he preferred virtual sunsets to real ones because the virtual sunset could be constructed so as to be perfectly enjoyable. Provocative lunacy, I thought at the time, not realizing how many people agree with him.

The virtual can seduce us because it offers the promise of being completely shaped to our wishes, while the material world remains refractory—there we suffer and die and live out fates that cannot be edited or replayed to render them more beautiful, more charming, less disastrous. The virtual worlds we can master, the material world we cannot. Even the most open model of the NII—one that does not lock individuals into passive roles as consumers and citizens—forces us to contend with this dialectic of virtual and real, and especially with the ethical dimensions of an allegiance to the virtual.

As the electronic media make us more aware of conditions around the world—or, at least, of images of such conditions—we realize how much horror exists and how

Dark Days on the Net

The many virtues of the Internet are being undermined by the system's sudden popularity and rapid democratization, staff writer Paul Wallich observes in Scientific American *(March 1994).*

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 the 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.

It is difficult even for those who ply it every day to appreciate how much the Internet depends on collegial trust and mutual forbearance. . . . Most people know, for example, that E-mail messages can be read by many people other than their intended recipients, but they are less aware that E-mail and other communications can be almost tracelessly forged—virtually no one receiving a message over the Net can be sure it came from the ostensible sender.

Electronic impersonators can commit slander or solicit criminal acts in someone else's name; they can even masquerade as a trusted colleague to convince someone to reveal sensitive personal or business information. Of those few who know enough to worry about electronic forgeries, even fewer understand how an insidiously coded E-mail message can cause some computers to give the sender almost unlimited access to all the recipient's files. . . .

In the early days, only researchers had access to the Net, and they shared a common set of goals and ethics, points out Eugene H. Spafford of Purdue University. . . . A lack of security . . . did not bother anyone, because that was part of the package, according to Dorothy E. Denning, a professor of computer science at Georgetown University: "The concerns that are arising now wouldn't have been legitimate in the beginning." As the Internet grew, however, the character of its population began changing, and many of the newcomers had little idea of the complex social contract—and the temperamental software—guiding the use of their marvelous new tool.

By 1988, when a rogue program unleashed by Robert T. Morris, Jr., a Cornell graduate student, brought most Internet traffic to a halt for several days, a clear split had developed between the "knows" and the "know-nots." Willis Ware of the Rand Corporation, one of the deans of computer security, recalls that "there were two classes of people writing messages. The first understood the jargon, what had happened and how, and the second was saying things like, 'What does that word mean?' or 'I don't have the source code for that program, what do I do?'"

Since then, the Internet's vulnerability has only gotten worse. . . . Moreover, as the Internet becomes a global entity, U.S. laws become mere local ordinances. In European countries such as the Netherlands, for instance, computer intrusion is not necessarily a crime. Spafford complains—in vain, as he freely admits—of computer science professors who assign their students sites on the Internet to break into and files to bring back as proof that they understand the protocols involved. . . .

If the Internet, storehouse of wonders, is

connected we are to it. Thus, despite our prosperity and plenty, we find ourselves intolerably affronted by images of disease and destruction. We do not wish to see starving children or piled-up bodies as we wait for our evening meal. However, through the virtual worlds we master the horrors, discovering ways to prevent them from deeply disturbing our composure. And virtuality has a wide domain. The Holocaust becomes a museum and a Spielberg movie, a spectacle, as the Situationists say,

also a no-computer's-land of invisible perils, how should newcomers to cyberspace protect themselves? Security experts agree that the first layer of defense is educating users and system administrators to avoid the particularly stupid mistakes. . . . The next level of defense is the so-called fire wall, a computer that protects internal networks from intrusion. Most major companies have long since installed fire walls, and many universities are adopting them as well. Fire walls examine all the packets entering and leaving a domain to limit the kinds of connections that can be made from the Internet at large. They may also restrict the information that can be passed across those connections. . . .

Encryption could provide not only privacy but authentication as well: Messages encoded using so-called public-key ciphers can uniquely identify both recipient and sender. But encryption software in general remains at the center of a storm of political and legal controversy. The U.S. government bars easy export of powerful encoding software even though the same codes are freely available overseas.

Within the United States, patent rights to public-key encryption are jealously guarded by RSA Data Security, a private firm that licensed the patents from their inventors. Although software employing public-key algorithms has been widely published, most people outside the U.S. government cannot use it without risking an infringement suit.

To complicate matters even further, the government has proposed a different encryption standard, one whose algorithm is secret and whose keys would be held in escrow by law-enforcement agencies. Although many civil libertarians and computer scientists oppose the measure, some industry figures have come out in favor of it. . . . The question is not whether cyberspace will be subjected to legislation but rather "how and when law and order will be imposed," says Donn B. Parker of SRI International. He predicts that the current state of affairs will get much worse before the government steps in "to assure privacy and to protect the rights people do have."

Others do not have Parker's confidence in government intervention. Marcus J. Ranum of Trusted Information Systems foresees an Internet made up mostly of private enclaves behind fire walls that he and his colleagues have built. "There are those who say that fire walls are evil, that they're balkanizing the Internet," he notes, "but brotherly love falls on its face when millions of dollars are involved."

Denning counts herself among the optimists. She lends her support to local security measures, but "I don't lose any sleep over security," she says. Farber, also cautiously optimistic, sees two possible directions for the Internet in the next few years: rapid expansion of existing services, or fundamental re-engineering to provide a secure base for the future. He leaves no doubt as to which course he favors. Spafford is like-minded but gloomier. "It's a catch-22," he remarks. "Everyone wants to operate with what exists, but the existing standards are rotten. They're not what you'd want to build on."

Even if computer scientists do redesign the Internet, he points out, putting new standards in place may be impossible because of the enormous investment in old hardware and software. So much of the Internet rests on voluntary cooperation, he observes, that making sweeping changes is almost impossible.

and we watch and weep yet are strangely exultant at the end of it all, and why not? We are alive and have our technology to instruct and amuse us. Today the corpses pile up in Bosnia (or was that Croatia?) and Rwanda, and the day's bald television images and puerile narrations haunt us, but tomorrow they will have become elements of an aesthetically rewarding film.

The NII will serve us efficiently in this regard. In Wim Wenders's film, *Until the End of the World* (1992), characters become addicted

to image technology, lost in reliving memories of their infancy through a device that turns their thoughts into pictures. The NII would not grant us this power, but it would put rich, complex sets of images at our command—"All the information in the universe will soon be accessible to everyone at every moment"—and thus generate the potential for its own kinds of addictions: to beautiful images and to virtuality itself.

Ultimately, the NII finds us being ourselves in the late 20th century: caught in the web of our own fantasies, governed by forces that inscribe their orders into our being, fighting nonetheless, through a stubborn will, to manifest something like authentic individual desire. The sharp-edged technology of the NII can cut a number of ways: It can enlarge the domain of the commodifiers and controllers; it can serve the resistance to these forces; it can saturate us all, controlled and controllers alike, in a virtual alternative to the real world.

Meanwhile, most of humanity will live and die deprived of the wonders of the NII, or indeed of the joys of adequate nutrition, medical care, and housing. We would do well to regulate our enthusiasms accordingly—that is, to remember where love and mercy have their natural homes, in that same material world. Otherwise we will have built yet another pharaonic monument to wealth, avarice, and indifference. We will have proved the technophobes right. More to the point, we will have collaborated to neglect the suffering of the damned of the earth—our other selves—in order to entertain ourselves.

Yet as William Gibson says in *Neuromancer* (1984), the canonical work of cyberpunk science fiction, "The Street finds its own uses for things," the Street referring to the unauthorized, unsanctioned play of human desire. Thus, we can approach the NII in a properly skeptical or suspicious frame of mind and yet remain open to its possibilities. After all, the Internet has shown that even a technology designed to enable the military to fight on after a nuclear holocaust can be made to serve the unfettered human imagination. With this experience to guide us, it is possible, perhaps even likely, that the same can be accomplished with the NII.