Present at the Creation

by Leslie D. Simon

The new very broadband high capacity networks . . . ought to be built by the federal government and then transitioned into private industry.
—Vice President-elect Al Gore, at the December 1992 postelection economic summit in Little Rock

Private sector leadership accounts for the explosive growth of the Internet today, and the success of electronic commerce will depend on continued private sector leadership.
—"A Framework for Electronic Commerce" (July 1997), a White House policy paper written by Ira Magaziner with advice from Vice President Gore's staff

It was an extraordinary turnabout. In the space of the four and a half years between these two statements, the most technology-literate administration in American history reversed itself on one of the century's more important technological questions. It wasn't a political change of heart that turned Bill Clinton and Al Gore around but a recognition that they were dealing with something vastly greater than

they had imagined only a few years earlier. And that "something greater" now urgently confronts the United States and other countries with important choices.

During his years in Congress, Vice President Gore had championed critical advanced research by the government in new information and communications technologies. He liked to remind people that his father, as a senator from Tennessee, had played a key role in the construction of the interstate highway system during the 1950s and '60s—a new national transportation infrastructure that transformed the American economic and physical landscape, creating millions of jobs in road and housing construction, shopping malls, and countless other enterprises. The vice president would go on to say that now the government needed to create an infrastructure for the next century—an information infrastructure built on the foundation of government programs such as the multibillion-dollar High Performance Computing and Communications Initiative.

The World Wide Web still lay over the horizon when Vice President-elect Al Gore spoke of a government-backed "information superhighway" at Little Rock in 1992.

Government efforts had played an enormous role in the birth of the Internet and its underlying technologies, from packet switching to integrated circuits. ARPANET, the original backbone of the Internet, and NSFNET, which later superseded it, were designed chiefly for the defense community and scientific researchers. Both were creatures of the federal government. But the logic of governmental leadership was overtaken by events. By 1994, in the digital equivalent of the Big Bang, cyberspace was exploding out of its original narrow confines. Suddenly, the Internet was alive with commerce, business, entertainment, education, art, and, yes, pornography.

The spark was provided by the creation of the World Wide Web, an Internet graphic tool that greatly simplified the task of retrieving and viewing information. Invented by Tim Berners-Lee at CERN, the European high-energy physics research laboratory, the Web came to life in 1993 when a University of Illinois student named Marc Andriessen released a software program called Mosaic, the parent of Netscape Navigator. Now,

instead of entering obscure instructions by keyboard and staring at screens full of monotone type, users were able to steer through a universe of words, images, and sounds with the click of a mouse button. Within an amazingly short time of perhaps eight "Web years" (Silicon Valley denizens measure time in Web years—there are four in each chronological year), office workers, high school students, retirees, physicians, and even a few politicians were sending e-mail, setting up Web sites, and surfing the Web. Suddenly, every television and magazine advertisement boasted a URL (universal record locator), or Web site address.

With efforts such as Gore's Reinventing Government program, the Clinton administration moved quickly to capitalize on the new technology, launching Web sites, for example, that eased citizens' access to government agencies. It also tried to keep government in the forefront of research. When a consortium of universities and high-technology companies in 1997 announced a joint effort to create Internet 2, a faster, advanced version of the Internet with enough bandwidth to carry the huge data files involved in scientific research, videoconferencing, and other specialized undertakings, the administration announced its Next Generation Internet program, offering researchers federal grants and underwriting research projects by government agencies.

But the Internet tsunami moved too quickly for the government to stay in front. In July 1997, the administration's "Framework for Electronic Commerce" announced the new policy: the private sector would lead the development of electronic commerce.

At the time, few saw the document as remarkable. We live, after all, in a time when the virtues of market-led development seem increasingly self-evident in the United States and abroad. But imagine the reaction if Theodore Roosevelt had called for the oil or sugar industries to be self-regulating. Or even if Ronald Reagan had called for industry to regulate cyberspace.

What the administration (and others) correctly realized, however, is that creating cyberspace is an undertaking almost without precedent. We are in effect creating a new world, a world that is virtually unbounded by physical laws, legal jurisdictions, and international borders. To leave the shaping of that world primarily to government agencies would have been folly.

Cyberspace offers industry opportunities of a kind never seen before. The modern oil industry, for example, grew out of the aggressive entrepreneurship of industry titans such as John D. Rockefeller and the intervention of governments concerned about monopoly and national security. A wrong turn—say, government policies that drove the price of gasoline sky-high or created scarcity—would have given us a very different world from today's highly mobile car culture, with its suburbs, interstates, shopping malls, and McDonald's drive-throughs. Yet, physical

> Leslie D. Simon, *a Wilson Center Public Policy Scholar, is a retired IBM senior executive who has worked with governments around the world on high-technology issues. A member of the State Department's Advisory Committee on International Communications and Information Policy, he is currently working on a book about the digital age.*

The death of distance: videoconferencing allows doctors in Canada and India to consult. Bandwidth limitations and other barriers must be overcome before such technologies become widely available.

facts limited the power of industrialists and politicians alike to determine the oil industry's future: petroleum deposits exist only in certain places and in certain quantities, and crude oil can be refined into gasoline only through chemical processes that obey physical laws. The supply would never be endless.

Today, in creating cyberspace, the physical limitations are far fewer. Cyberspace is almost entirely a creation of the mind—a vast and still largely blank slate awaiting the spark of human ingenuity. That is not to say that there is no role for government. Indeed, the choices that governments and the private sector make will almost alone determine what gets written on the slate. Those choices must be made soon. The very freedom of cyberspace from physical laws, its borderless nature, and its frenetic growth all mean that profoundly important choices must be made over the next decade. If we fail to make them in time, they will be made for us, by default.

The physical constraints on cyberspace are shrinking all the time. True, one must still view the data, graphics, or video on a flat panel or cathode-ray tube; type on a keyboard or wield a mouse; and make contact with others through webs of copper wire, optical fiber, coaxial cable, satellite dishes, and electronic switches. Yet while these physical artifacts make cyberspace possible, they do not define it, and, increasingly, do not limit its potential. High-tech companies today are racing to reduce even further our physical connections to the digital world, using techniques such as voice recognition and hand signaling. The growing global network of computers and other hardware is opening up a vast array of uses. The Internet can take the place of a post office, a telephone, a broadcast

studio, an insurance agent, a sound recording, a movie theater, an automobile dealership—almost anything anybody can imagine.

As the physical infrastructure of cyberspace fades into the background, what is important is what you see and hear and how you use it. The medium is no longer the message. In cyberspace, media can take on any form—video, print, graphics, or sound—at the whim of the user. As media converge, they become fungible background elements. Their distinctiveness is rapidly disappearing. The sharp line that existed between television and print media when Marshall McLuhan examined them earlier this century is fading rapidly. Content is now king.

National boundaries also fade into near irrelevance in the digital universe. An image or article or video created in one country can be viewed elsewhere at any time or as many times as users wish. Banking, shopping, schooling—all can be performed across national boundaries. The only services that are not transnational—at least not yet—are government services. While a Malaysian can buy delicacies from a virtual French shop, or take college-level courses from a Canadian school, he or she cannot apply for French or Canadian social security benefits. In the future, growing demand for just such opportunities may change the very notion of citizenship.

Even the Internet's physical communications web is amorphous and mutable, creating itself without regard to national borders but according to the traffic patterns that packet-switched networks are designed to optimize. These virtual and ever-changing connections are proving too sublime for government regulation. Every frame viewed or service rendered in cyberspace raises questions no nation can deal with in isolation. What if an image is not considered pornographic in one country but is in another? What if a physician in one country diagnoses a patient in another where the physician is not licensed? What if the patient wants to sue the physician for malpractice? And what if the physician's services are taxable in both countries?

A final unique characteristic of cyberspace is the speed of its development. Traffic on the Internet doubles every 100 days. It is estimated that the number of people using the Internet worldwide will grow from 100 million today to more than one billion by 2005. In 1997, there were about 2.7 trillion e-mail messages—many times more than the amount of mail delivered by the world's post offices! The volume of electronic commerce is expected to grow from about $2 billion in 1997 to more than $300 billion in 2002, to more than $1 trillion in 2010.

In the United States and other industrial countries, a good bipartisan start has been made in agreeing on some fundamental principles governing the future of cyberspace, but translating them into specific policies has been more difficult. Even after the Clinton administration announced its new emphasis on private-sector leadership last year, for example, government and industry at first were lost in mutual incom-

prehension. To industry, self-regulation and private-sector leadership initially meant only that it should continue to do what it does best—develop and sell innovative products. It would help Washington clear away policy obstacles to growth in areas such as taxation and commercial law. But that was about it.

To government, self-regulation meant that industry would take the initiative in areas such as protecting the privacy of Internet users and monitoring pornography and other objectionable content (e.g., bomb-manufacturing instructions). There are precedents for this. In the 1960s, when the nation was flooded with dubious advertising claims, the advertising industry, under pressure from the Federal Trade Commission, developed a code of self-regulation that has worked well. Now, the government, besieged by complaints about privacy violations and Internet pornography, was transferring the political heat to leading CEOs such as Intel's Andy Grove, IBM's Lou Gerstner, and Microsoft's Bill Gates. A bit unsure how to proceed—and perhaps a bit reluctant to assume such responsibilities—industry hesitated. Since then, it has begun to step up to the challenge. On the agenda for both government and the private sector are six major issues, with a host of others waiting in the wings:

Privacy: All kinds of personal information, from school records to patient medical data to local real estate and tax records, is now being digitized and made available on the Web. And vast quantities of fresh data are being used and collected through "cookies" (data about your preferences stored in your browser by a Web site you visit), "data mining" by powerful computers that allow merchants to track the buying habits of individual shoppers, and other new technologies. Privacy is now the number one Internet issue. Will individuals have control over how data about them are collected, disseminated, and used? Or will all data be public?

While the United States already has a complex system of privacy laws and regulations, industry could provide more protection tailored to the digital world, and will need to do so to avoid inviting broader government regulation. Indeed, some see government itself as the greatest threat to privacy, and past abuses by the Internal Revenue Service, as well as the Social Security Administration's handling of private information on its Web site recently, do not offer much encouragement to think otherwise.

Industry has begun to respond. The American Bankers Association, for example, has developed a privacy code for member banks, and the Information Technology Industry Council, a high-technology trade association that includes large corporations such as Xerox, Compaq, and IBM, has adopted a code for its members. These codes generally restrict what member companies can do with data they gather about their customers—such as information supplied when consumers fill out loan applications or warranty forms for their new computers—and spell out requirements for notifying the public about their policies. It is even more encouraging that an initial group of 39 companies and 12 trade associa-

tions has formed an umbrella group, the Online Privacy Alliance, to attempt to meld the activities of different industry groups. But these efforts, laudable as they are, just scratch the surface. A more comprehensive private-sector code, international in scope, together with an enforcement mechanism to punish malefactors, will certainly be needed.

Security: People will not make extensive use of the Internet to buy, sell, and borrow unless they can be assured that their credit card numbers and other details of the transaction are secure. Cryptography—coding all transmitted messages—is the principal answer, but it leads to a public-policy question: Cryptography under what terms? That question has stymied Congress and the administration. Business and civil liberties groups want no limits on cryptography, hoping to maximize the security and privacy of online communications. But the Federal Bureau of Investigation and other government agencies, legitimately worried about the uses criminals, terrorists, and others may make of encryption, favor various controls, such as limits on exports of encryption software, or even domestic controls, such as the use of a "back door" in all codes to allow government agencies to decode information under certain circumstances. Congress must end the uncertainty soon or risk greatly retarding the growth of electronic commerce.

Objectionable Content: In 1996, responding to parents alarmed by the ease with which children can find pornography on the Internet, Congress passed the Communications Decency Act, making it a crime to transmit "obscene or indecent" material over the Internet. But the Internet is a more complex place than the legislators realized. In some cases, it resembles television broadcasting, and thus is more susceptible to regulation, while chat rooms and other forms of Internet communication are more like private conversations and thus enjoy the strongest First Amendment protection. In 1997, after the American Civil Liberties Union, the Center for Democracy and Technology, and other organizations challenged the act, the Supreme Court struck it down as unconstitutional. Congress seems uncertain about what, if anything, to do next, and is currently considering laws that prohibit materials that are "harmful to minors," and that require schools and libraries to block children's access to "inappropriate materials." The private sector may hold the solution to this problem. High-tech companies have already written software programs such as Net Nanny and SurfWatch that allow parents to bar access to pornography, and a consortium of companies working with the Massachusetts Institute of Technology has created a standardized tool for achieving the same end, the Platform for Internet Content Selection. Now industry should make a bigger effort to educate parents about what their more technologically nimble children may be doing during all those hours of Web surfing and what they as parents can do to regulate it.

Access: How can we avoid becoming a nation of information haves and have-nots? Computers and Internet connections come with big price tags, and without help, inner-city and rural children, for example, may be shut out. With the advent of telephones earlier in the century, we used regula-

tion to achieve universal service. When television broadcasting arrived in midcentury, we let the market decide who got to watch. Both methods produced near-universal access. Which course should we follow now?

There seems to be agreement in Congress on the need for universal access, but not yet on the means to achieve it. This year, Congress has been trying to force the Federal Communications Commission to stop its program of subsidizing Internet hookups for schools, libraries, and hospitals, after hearing loud complaints from consumers who spotted on their long-distance phone bills a new charge to pay for the $1.2 billion subsidy. Congress, of course, had created the program in the first place. While competition and market forces will play the main role in spreading access by driving prices down, industry and government should both experiment with new ways of opening doors to the Internet—for example, by setting up cyberkiosks in libraries, community centers, and post offices.

Taxation: As more economic activity migrates on-line, politicians and tax collectors are worrying about losing tax revenues—especially those from state sales taxes and, in Europe, national value-added taxes. Who collects the tax when an on-line buyer in Iowa orders a lamp from a computer server in California that is shipped from a warehouse in Holland? How is the tax collected? How do the authorities even know about the sale? The states are beginning to stir—Florida, Connecticut, Texas, and Nebraska are among those examining taxes on Internet service providers. The Clinton administration has called for a moratorium on new Internet taxes, but Congress and the states have yet to agree.

Infrastructure: If the Internet is to reach its full potential, telephone, cable TV, and other companies will need to invest vast sums in switch-

Peering into the future

ing equipment, cable, optical fiber, and satellite networks, along with their underlying software. But the archaic laws restricting competition among such companies has discouraged investment. The Communications Reform Act of 1996, which was meant to spur telecommunications competition and innovation in advanced high-bandwidth services, has so far resulted chiefly in a tangle of court cases and a series of high-profile mergers—among them Bell Atlantic and Nynex, and AT&T and TCI—that may or may not produce the desired results. Congress and the administration need to find new means to separate the advanced technologies of the Internet from the regulatory tangle of the old world of telephony.

Beyond these six key issues are numerous others of a more technical and legal nature: intellectual property, especially copyright, digital contracts and signatures, the future governance of the Internet, and the ownership and value of government information, to name a few. Abroad, uncertainty also reigns on these crucial issues. It was only in February 1995, at a Group of Seven ministerial meeting, that Europe officially accepted the notion that, on balance, cyberspace would create new jobs. Under the forceful leadership of Martin Bangemann, the European Union (EU) Commissioner for Industry, the Europeans, along with Japan and Canada, have also embraced the fundamental premise that Internet development should be driven by the market and the private sector. As in the United States, however, the effort to implement specific policies has been slow.

Elsewhere in the world, there is less cause for encouragement. Singapore, for example, has made an exemplary push to exploit the economic potential of cyberspace, attempting to wire every home in the country with broadband coaxial or fiber-optic cable by 2000. At the same time, however, Singapore censors on-line material and registers Singaporean Web site operators. Governments everywhere feel a strong temptation to closely regulate the on-line world. Some, notably Canada and France, fret about perils they perceive to their language and culture. Autocratic and totalitarian regimes see the borderless Internet as a threat, and some, such as China, would like to limit their citizens' participation to something like a giant private network, with all content and services filtered by government.

Because cyberspace is borderless, trying to draw up laws and regulations in a national vacuum is increasingly an exercise in futility. In 1995, for example, an EU directive required member nations to create national authorities to regulate private-sector privacy policies. But European companies and citizens do business on line in other countries that lack such broad national authorities. Were these international transactions to be prohibited? The EU offered to certify that other countries provide an "adequate level of protection." But who is to say what is adequate? Some countries have no privacy protection at all, including China and some of Europe's other important trading partners. Oddly, the Europeans have chosen to aim their sights at the United States, which has its own sophisticated but confusing

legal system to regulate privacy: a mix of federal, state, and private-sector protections, including the broad consumer protection powers of the Federal Trade Commission.

Ultimately, many emerging cyberspace issues will have to be resolved by international organizations, such as the new World Trade Organization (WTO) and the United Nations Conference on International Trade Law. A good example of what such organizations can do is the 1997 WTO agreement on basic telecommunications, under which more than 60 countries committed themselves to deregulation and to increase international competition in the industry. This agreement should help strengthen the physical infrastructure needed to support the digital world. But the international road is a tortuous one. International organizations tend to move glacially, and toward the lowest common denominator. That is the bad news. The good news is that a number of them, such as the Organization for Economic Cooperation and Development, have officially embraced the emerging digital universe, leaving behind the old Luddite arguments against progress.

Now the United States and its partners must push for a quick resolution of a few key issues. A broader international consensus on the potential economic and social benefits of cyberspace is one objective, along with agreement on the need to foster new skills and schooling better suited to an information economy. An emphasis on private-sector leadership in the development and use of cyberspace is another important goal. Business must also be encouraged to develop its own rules and enforcement systems for managing privacy, objectionable content, and other challenges. A final priority is a blueprint for approaching policy issues internationally, specifying what issues need to be tackled, in what order, and in what international forum. And public officials at all levels of government in every nation and international organization must take on the personal responsibility of educating themselves so that choices can be made quickly and intelligently.

Yet all of this would represent only a beginning of our efforts to shape the emerging world of cyberspace. More and more institutions are being drawn into the digital universe every day—banking and financial services, the retail industry, elementary education, state government, and many others. It will change all of them in ways so profound as to render totally useless their current statutory, regulatory, and historical underpinnings. Digital cash and other innovations lie before us, many of them not even imagined. So do challenges such as Internet crime and information warfare. We have the opportunity to make the most of the economic and social advantages that this revolution has to offer—or, by failing to act, to waste some of its potential and do ourselves harm. We have ample warning, but do we have the will and skill to act?
