Internet and Computers

BACKGROUND

Internet and World Wide Web

Computers, not so many years ago found only in well-funded laboratories, now are a staple of many American households, businesses, and schools. The original electronic computer of just over 50 years ago weighed 30 tons and took up 1,800 square feet of floor space; today there are models that fit in one's hand. New models sometimes are many orders of magnitude faster than even their very recent predecessors. An entire industry has evolved from computers; companies that today are a household name were unknown 10–15 years ago.

In the 1990s, personal computer use has gotten a boost from the rapid growth of the Internet, which, in its simplest form, may be described as a communication system that interconnects otherwise free-standing computer networks. The modern Internet evolved from activities supported by the U.S. Defense Advanced Research Projects Agency (DARPA) during the late 1960s and early 1970s to interconnect Defense Department researchers. In 1972 DARPA researchers first publicly demonstrated the network and later that year introduced electronic mail (e-mail) to facilitate communication.

Part of the rationale behind the Defense Department network was to create a communications system that did not require point-to-point communication. Instead, traffic would be broken into small pieces, called *packets*, and each packet would have its destination's address. Packet switching, as the technology is called, is analogous to giving each of a group of travelers going to the same place directions to his/her common destination, then requiring each passenger to get to the destination by him/herself. In the case of a natural disaster or national crisis, packets (or passengers) could reroute themselves if one network link (or road) was damaged or destroyed.

The Defense Department's success lead to other computer networks being established, including BITNET, in the early 1980s, which linked college and university mainframe computers together. By 1985 the National Science Foundation had established NSFNet, interconnecting federal agencies and five university "supercomputers." As NSFNet grew, private networks on a local and regional level emerged to connect local colleges, universities, and companies to the supercomputer centers, which were in turn interconnected. In Michigan, Merit Networks, located in Ann Arbor, was one such regional entity. Beginning in 1988 Merit won a contract to manage the entire NSFNet until the large, high-speed "backbone" connections were privatized by several companies, including MCI. Today, Merit is a nonprofit corporation owned by 12 of Michigan's public, four-year universities that continues to provide Michigan schools, universities, and businesses with a connection to the Internet backbone.

GLOSSARY

Browser
A computer program—such as Microsoft® Internet Explorer™ or Netscape Navigator™—that allows users to look at, read, and even hear information on the World Wide Web.

Host
A computer connected to the Internet that provides information to users.

Internet
The global communications system that interconnects otherwise free-standing computer networks, using a common transmission protocol.

Internet service provider (ISP)
A company that provides access to the Internet.

Network
A group of interconnected computers. Local area networks (LANs) connect computers that are physically close to each other (e.g., in the same building); wide-area networks (WANs) connect computers over long distances.

Server
A computer that provides some service for other computers connected to it via a network.

World Wide Web (W W W)
A collection of interconnected servers that makes electronic files accessible with a browser.

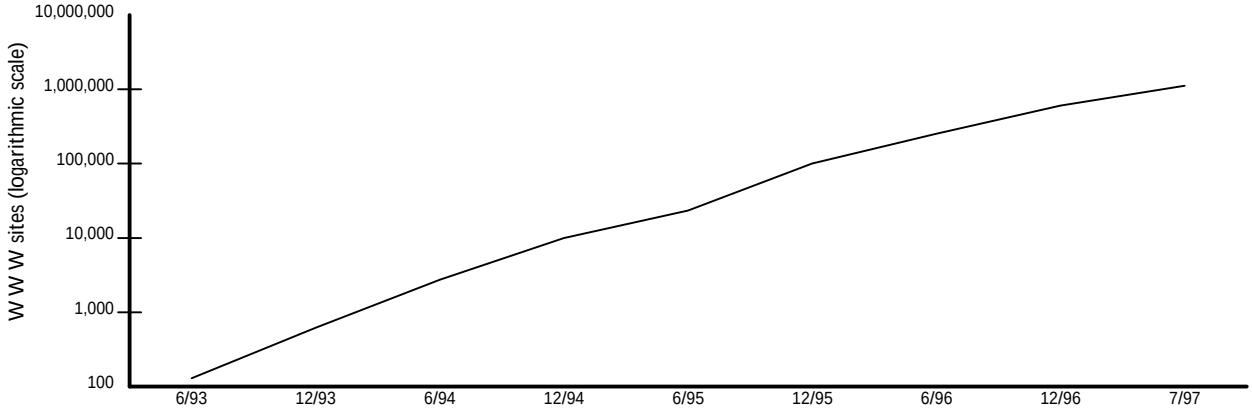
The introduction of the World Wide Web (WWW)—which today is influencing many Internet technologies and policies—is a very recent phenomenon. The WWW was created in 1991 by Swiss researchers as a way to transmit text and graphics. In 1992 there were 26 WWW servers on line; as of August 1997 there were more than 1.2 million (see Exhibit 1).

The growth of Web servers helped fuel overall growth in the number of Internet hosts—computers on the Internet that provide data (see Exhibit 2).

While Internet technology and use were escalating, major changes occurred in other areas of telecommunications, and, after long debate, Congress passed the Telecommunications Act of 1996. The massive act also incorporated the first far-reaching federal regulation of Internet content: the so-called Communications Decency Act (CDA). The CDA makes it a crime knowingly to

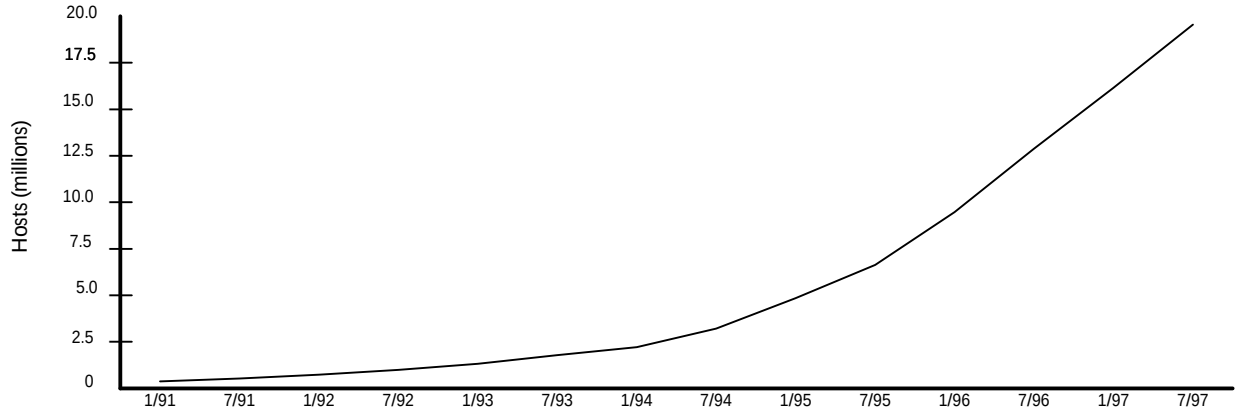
- transmit obscene or indecent material via the Internet to recipients aged under 18, or

EXHIBIT 1. World Wide Web Growth, June 1993–1997



SOURCE: Hobbes's Internet Timeline v3.1, copyright 1993–97 by Robert H. Zakon and used with permission; available on line at www.isoc.org/zakon/Internet/History/HIT.html.

EXHIBIT 2. Internet growth, January 1991–July 1997



SOURCE: Hobbes's Internet v3.1, copyright 1993–97 by Robert H. Zakon and used with permission; available on line at www.i50c.org/zakon/Internet/History/HIT.html.

- send or display on the Internet any message that depicts sexual organs or describes patently offensive sexual activity.

Several groups, including computer users and the American Civil Liberties Union, sued to block the CDA's implementation on the ground that it violated the First and Fifth amendments to the U.S. Constitution. In June 1997 the Supreme Court agreed, finding that the act's vague language would abridge the right to free speech.

DISCUSSION

As a new sector of the economy and sphere of entertainment, computers and the Internet are posing numerous challenges—as well as opportunities—for the public and policymakers.

Pace of Change

As computer performance has improved and prices have dropped, the demand for computers at home, school, and the office has exploded. Coupled with the growth of networks, computers are creating serious structural challenges for information managers. MCI, which operates part of the massive backbone that connects the smaller Internet service providers (ISPs), recorded a 3,000 percent increase in backbone traffic during 15 consecutive months in 1995–96. By late 1996 MCI was reporting that in each month the equivalent of 9 million encyclopedias was being transmitted across the MCI backbone network.

To manage these drastic changes—whether rapidly falling prices or extreme demand increases—businesses such as America Online (AOL), a large ISP, must manage their revenue and expenditures to meet the demand, while simultaneously fully recovering the cost of previous investments. This balancing act is no small challenge, as AOL discovered in 1997. Users were complaining that in trying to connect to AOL they often experienced multiple-hour delays or simply failed. Businesses that depended on AOL for corporate e-mail were unable to respond to customers, and home users were frustrated by continuous busy signals. To combat the tidal wave of demand, AOL increased its 1997 equipment budget by $100 million so as to increase its network capacity, and in early 1998 raised its monthly fee by $2.

Policymakers and the legal system are having to react to a technological environment that changes so quickly that there is no time for public consensus on common issues, extended study of legislative alternatives, or careful and cautious application of existing law. The pace of change also affects policymakers as they design public information networks. The Michigan Department of Education, for example, completed a Michigan State Technology Plan that was to cover 1992 to 1997. However, technological change outpaced the ambitious 5-year plan well before its end date. In the revised plan, completed in late 1997, the authors recommend having no end date but rather ongoing review. Other statewide plans, such as the Michigan Department of Management and Budget's Michigan Information Network Plan, face similar challenges.

To complicate matters further, even if the state could complete a plan that would withstand technological change, the Internet is not managed by a single government or corporation on which policymakers may call for assistance in implementing a plan. The Internet is filled with providers—ranging from small, one-person consulting firms to the largest telecommunications and media corporations in the world—that by agreeing to adhere to a set of technical standards for data transmission, also agree to connect their networks to one another. The allocation of domain names (e.g., *pscinc.com* or *whitehouse.gov*) is one of the few instances of centralized Internet management: InterNIC, a nonprofit venture of the National Science Foundation, AT&T, and Networks Solutions, Inc., is the sole distributor of Internet names.

One group already hard at work building the next generation of the Internet for universities is located at the University of Michigan. "Internet2," a project of the University Corporation for Advanced Internet Development, is a consortium of more than 100 U.S. research universities and several telecommunications companies. Together, the partnership seeks to develop higher-speed Internet access and new, high-technology applications for corporate and university researchers.

Privacy in the Electronic Age

One major policy question is how to transmit private information across these new electronic networks. One way is to encrypt the message, i.e., scramble it so that it is unintelligible to anyone but the sender and the intended receiver. While noting that *some* encryption is necessary for electronic commerce and privacy, many federal law enforcement and national security agencies object to letting the general public use encryption technologies that are "too powerful." For example, a sufficiently "strong" encryption could be unreadable for years to anyone without the code, rendering a law-enforcement agency's wiretap order useless until a supercomputer could crack the code; meanwhile criminals and terrorists could continue unimpeded, secure in the knowledge that their discussions were private. Supporters of permitting general use of strong encryption argue that it is a necessary part of electronic commerce: consumers will want to know that their credit card information is safe from prying eyes before purchasing an item over the Internet.

One system proposed by the U.S. government is to create a "encryption bank" that would hold one-half the solution (or key) to every encrypted message. Law enforcement agencies, after showing direct evidence or other grounds for an investigation to a judge or other independent arbiter, could have access to the key and use it to break the rest of the code in order to monitor conversations or messages. Supporters of this key-escrow system contend that requiring a judge to permit computer wiretapping is no different from the current standards for telephone and other similar surveillance requests. Opponents of such a system contend that it would be ripe for abuse by law enforcement agencies and a massive and irresistible target for computer hackers, and people are entitled to private communication without fear that government listening in.

Indecency, Pornography, Obscenity, and Free Speech

The growth of Internet-based e-mail, chat rooms, news groups, and Web servers has produced an entirely new arena for exercising free speech. Information about nearly anything in which anyone is interested—e.g., computer programs, amusement parks, AIDS prevention, sexual fetishes, or sports highlights—may be found by Internet users, and it may be accessed by all Internet users, regardless of their age or where they live in the United States or the world.

Supporters of the CDA wanted to protect children from obscene and indecent material. Because of the Internet's anonymous nature—users need not disclose (or may falsely disclose) such personal information as age, race, gender, or nationality—supporters argue that it is nearly impossible for parents to adequately protect their children from obscene material. They believe the CDA would have helped parents by placing on the *sender* the burden of keeping indecent and obscene material away from children. But the U.S. Supreme Court found that because "indecency" was not well defined, the act could abridge free speech. Under the CDA, the U.S. Supreme Court noted that "a parent allowing her 17-year-old to use the family computer to obtain information on the Internet that she, in her parental judgment, deems appropriate" still could be held in violation of the law, despite the parent having consented to—and perhaps even assisted in—retrieving the information. The Court also found that indecency's unclear definition would limit adults' right to transmit questionable material to other adults; senders have no way to know *for sure* that the receiver is indeed an adult.

One way to protect children from offensive or sexually explicit material is for parents to closely supervise their child's Internet activity. To this end, several software companies have introduced products that block pornographic sites or filter messages (e.g., Net Nanny® software). In addition, many commercial pornographic sites now require a credit card number as proof of age before transmitting material, but being able to type in a credit card number still does not *prove* that a requester is an adult.

Complicating the free speech issue even more is the Internet's interconnected nature. Traditional tests for obscenity—which include whether the average person, applying contemporary community standards,

would see some literary, artistic, political, or scientific value in the speech in question—fails on the Internet, where the "community" is the globe; questionable material is as accessible from 10,000 miles as from next door. For example, if a Michigan resident places neo-Nazi information on a Web site, can the resident be prosecuted under German law that prohibits distributing illegal or obscene speech in that country? Does requiring a Web site visitor to give a U.S. mailing address as a condition of entry constitute an adequate safeguard that the information is for U.S. distribution only?

Year 2000 Problem

A significant problem for computer and electronics producers and owners is the coming millennium. To save valuable memory and disk space, early computers treated dates in the *mm/dd/*yy format; e.g., January 1, 1998 is represented by 01/01/98. When January 1, 2000, arrives, an unknown number of computers will interpret the date as 01/01/00, or January 1, 1900, while others will recognize the date as January 1, 1980, the default date in many personal computer systems. This problem is most serious for computer programs that use dates in calculations—e.g., billing statements, interest calculations, benefit policies, or membership records. Some problems already are arising: Merchants are reporting that some older point-of-sale terminals (the devices through which credit cards are "swiped") are refusing to accept credit cards with an expiration date after 1999. The terminal reads the expiration year of 2000 as 1900, and reports that the card expired a century ago.

Fixing the problem could cost billions worldwide, because in many programs the additional date information must be added line by line. The problem's precise extent still is not known. Some observers forecast that the millennium will bring catastrophe—for example, air traffic control systems will fail, and elevators will become inoperable. Others believe that the problem was anticipated in time, and immense effort will have gone into fixing the problem; the worst problem may be a slight delay at the grocery store as one's credit card is authorized.

See also Information Technology and Society.

FOR ADDITIONAL INFORMATION

Cornell University Law School
supct.law.cornell.edu/supct
[For U.S. Supreme Court decisions]

Data and Technology Services
Michigan Department of Education
P.O. Box 30008
Lansing, MI 48909
(517) 373-4333
(517) 373-3325 FAX
www.mde.state.mi.us/tplan

Electronic Privacy Information Center
666 Pennsylvania Avenue, S.E., Suite 301
Washington, DC 20003
(202) 544-9240
(202) 547-5482 FAX
www.epic.org

Family Research Council
801 G Street, N.W.
Washington DC, 20001
(202) 393-2100
(202) 393-2134 FAX
www.townhall.com/frc

Federal Communications Commission
1919 M Street, N.W.
Washington, DC 20554
(202) 418-0200
(202) 418-0232 FAX
www.fcc.gov

InterNIC
www.internic.net
[Provider of Internet names]

Merit Network, Inc.
4251 Plymouth Road, Suite C
Ann Arbor, MI 48105-2785
(734) 764-9430
(734) 647-3185 FAX
www.merit.net

Michigan Information Network Plan
www.migov.state.mi.us/min/0-toc.html

National Coalition for the Protection of Children and Families
800 Compton Road, Suite 9224
Cincinnati, OH 45231
(513) 521-6227
(513) 521-6337 FAX
www2.nationalcoalition.org/ncpcf

Office of the Michigan Information Network
Michigan Department of Management and Budget
Victor Office Center, 5th Floor
201 North Washington Square
Lansing, MI 48913
(517) 241-0572
(517) 335-7004 FAX

University Corporation for Advanced Internet Development
University of Michigan
1210 Buhr Building
Ann Arbor, MI 48109-1340
(734) 913-4250
(734) 913-4255 FAX
Internet2: *www.internet2.edu*
UCAID: *www.ucaid.edu*