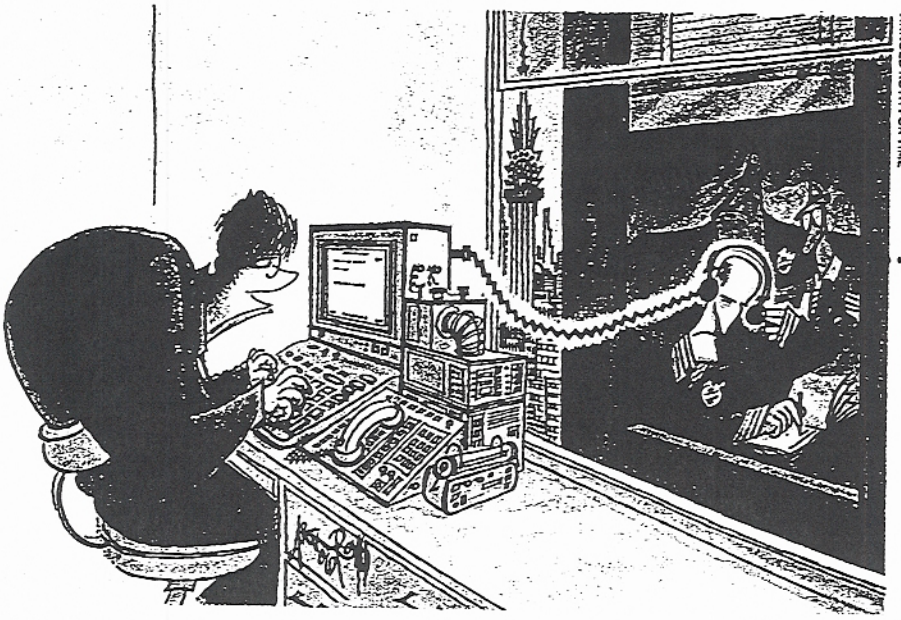
Cyberpunks and the Constitution

The fast-changing technologies of the late 20th century pose a challenge to American laws and principles of ages past

By PHILIP ELMER-DEWITT
SAN FRANCISCO

Armed with guns and search warrants, 150 Secret Service agents staged surprise raids in 14 American cities one morning last May, seizing 42 computers and tens of thousands of floppy disks. Their target: a loose-knit group of youthful computer enthusiasts suspected of trafficking in stolen credit-card numbers, telephone access codes and other contraband of the information age. The authorities intended to send a sharp message to would-be digital desperadoes that computer crime does not pay. But in their zeal, they sent a very different message—one that chilled civil libertarians. By attempting to crack down on telephone fraud, they shut down dozens of computer bulletin boards that may be as fully protected by the U.S. Constitution as the words on this page.



Do electronic bulletin boards that may list stolen access codes enjoy protection under the First Amendment? That was one of the thorny questions raised last week at an unusual gathering of computer hackers, law-enforcement officials and legal scholars sponsored by Computer Professionals for Social Responsibility. For four days in California's Silicon Valley, 400 experts struggled to sort out the implications of applying late–18th century laws and legal principles to the fast-changing technologies of the late 20th century.

While the gathering was short on answers, it was long on tantalizing questions. How can privacy be ensured when computers record every phone call, cash withdrawal and credit-card transaction? What "property rights" can be protected in digital electronic systems that can create copies that are indistinguishable from the real thing? What is a "place" in cyberspace, the universe occupied by audio and video signals traveling across state and national borders at nearly the speed of light? Or as Harvard law professor Laurence Tribe aptly summarized, "When the lines along which our Constitution is drawn warp or vanish, what happens to the Constitution itself?"

Tribe suggested that the Supreme Court may be incapable of keeping up with the pace of technological change. He proposed what many will consider a radical solution: a 27th Amendment that would make the information-related freedoms guaranteed in the Bill of Rights fully applicable "no matter what the technological method or medium" by which that information is generated, stored or transmitted. While such a proposal is unlikely to pass into law, the fact that one of the country's leading constitutional scholars put it forward may persuade the judiciary to focus on the issues it raises. In recent months several conflicts involving computer-related privacy and free speech have surfaced:

▸When subscribers to Prodigy, a 700,000-member information system owned by Sears and IBM, began posting messages protesting a rate hike, Prodigy officials banned discussion of the topic in public forums on the system. After protesters began sending private mail messages to other members—and to advertisers—they were summarily kicked off the network.

▸When Lotus Development Corp. of Cambridge, Mass., announced a joint venture with Equifax, one of the country's largest credit-rating bureaus, to sell a personal-computer product that would contain information on the shopping habits of 120 million U.S. households, it received 30,000 calls and letters from individuals asking that their names be removed from the data base. The project was quietly canceled in January.

▸When regional telephone companies began offering Caller ID, a device that displays the phone numbers—including unlisted ones—of incoming calls, many people viewed it as an invasion of privacy. Several states have since passed laws requiring phone companies to offer callers a "blocking" option so that they can choose whether or not to disclose their numbers. Pennsylvania has banned the service.

But the hacker dragnets generated the most heat. Ten months after the Secret Service shut down the bulletin boards, the government still has not produced any indictments. And several similar cases that have come before courts have been badly flawed. One Austin-based game publisher whose bulletin-board system was seized last March is expected soon to sue the government for violating his civil liberties.

There is certainly plenty of computer crime around. The Secret Service claims that U.S. phone companies are losing $1.2 billion a year and credit-card providers another $1 billion, largely through fraudulent use of stolen passwords and access codes. It is not clear, however, that the cyberpunks rounded up in dragnets like last May's are the ones committing the worst offenses. Those arrested were mostly teenagers more intent on showing off their computer skills than padding their bank accounts. One 14-year-old from New York City, for instance, apparently specialized in taking over the operations of remote computer systems and turning them into bulletin boards—for his friends to play on. Among his targets, say police, was a Pentagon computer belonging to the Secretary of the Air Force. "I regard unauthorized entry into computer systems as wrong and deserving of punishment," says Mitch Kapor, the former president of Lotus.

And yet Kapor has emerged as a leading watchdog for freedom in the information age. He views the tiny bulletin-board systems as the forerunners of a public computer network that will eventually connect households across the country. Kapor is worried that legal precedents set today may haunt all Americans in the 21st century. Thus he is providing funds to fight for civil liberties in cyberspace the best way he knows how—one case at a time. ■