IS COMPUTER HACKING A CRIME?

The image of the computer hacker drifted into public awareness in the mid-Seventies, when reports of Chinese-food-consuming geniuses working compulsively at keyboards began to issue from MIT. Over time, several of these impresarios entered commerce, and the public's impression of hackers changed: They were no longer nerds but young, millionaire entrepreneurs.

The most recent news reports have given the term a more felonious connotation. Early this year, a graduate student named Robert Morris Jr. went on trial for releasing a computer program known as a worm into the vast Internet system, halting more than 6,000 computers. The subsequent public debate ranged from the matter of proper punishment for a mischievous kid to the issue of our rapidly changing notion of what constitutes free speech—or property—in an age of modems and data bases. In order to allow hackers to speak for themselves, *Harper's Magazine* recently organized an electronic discussion and asked some of the nation's best hackers to "log on," discuss the protean notions of contemporary speech, and explain what their powers and talents are.

The following forum is based on a discussion held on the WELL, a computer bulletin-board system based in Sausalito, California. The forum is the result of a gradual accretion of arguments as the participants—located throughout the country—opined and reacted over an eleven-day period. Harper's Magazine *senior editor Jack Hitt and assistant editor Paul Tough served as moderators.*

ADELAIDE
is a pseudonym for a former hacker who has sold his soul to the corporate state as a computer programmer.

BARLOW
is John Perry Barlow, a retired cattle rancher, a former Republican county chairman, and a lyricist for the Grateful Dead, who currently is writing a book on computers and consciousness entitled Everything We Know Is Wrong.

BLUEFIRE
is Dr. Robert Jacobson, associate director of the Human Interface Technology Laboratory at the University of Washington and a former information-policy analyst with the California legislature.

BRAND
is Russell Brand, a senior computer scientist with Reasoning Systems, in Palo Alto, California.

CLIFF
is Clifford Stoll, the astronomer who caught a spy in a military computer network and recently published an account of his investigation entitled The Cuckoo's Egg.

DAVE
is Dave Hughes, a retired West Pointer who currently operates his own political bulletin board.

DRAKE
is Frank Drake, a computer-science student at a West Coast university and the editor of W.O.R.M., *a cyberpunk magazine.*

EDDIE JOE HOMEBOY
is a pseudonym for a professional software engineer who has worked at Lucasfilm, Pyramid Technology, Apple Computer, and Autodesk.

EMMANUEL GOLDSTEIN
is the editor of 2600, *the "hacker's quarterly."*

HANK
is Hank Roberts, who builds mobiles, flies hang gliders, and proofreads for the Whole Earth Catalog.

JIMG
is Jim Gasperini, the author, with TRANS Fiction Systems, of Hidden Agenda, a computer game that simulates political conflict in Central America.

JRC
is Jon Carroll, daily columnist for the San Francisco Chronicle *and writer-in-residence for the Pickle Family Circus, a national traveling circus troupe based in San Francisco.*

KK
is Kevin Kelly, editor of the Whole Earth Review *and a cofounder of the Hacker's Conference.*

LEE
is Lee Felsenstein, who designed the Osborne-1 computer and cofounded the Homebrew Computer Club.

MANDEL
is Tom Mandel, a professional futurist and an organizer of the Hacker's Conference.

RH
is Robert Horvitz, Washington correspondent for the Whole Earth Review.

RMS
is Richard Stallman, founder of the Free Software Foundation.

TENNEY
is Glenn Tenney, an independent-systems architect and an organizer of the Hacker's Conference.

ACID PHREAK *and* PHIBER OPTIK
are both pseudonyms for hackers who decline to be identified.

The Digital Frontier

HARPER'S [Day 1, 9:00 A.M.]: When the computer was young, the word *hacking* was used to describe the work of brilliant students who explored and expanded the uses to which this new technology might be employed. There was even talk of a "hacker ethic." Somehow, in the succeeding years, the word has taken on dark connotations, suggesting the actions of a criminal. What is the hacker ethic, and does it survive?

ADELAIDE [Day 1, 9:25 A.M.]: The hacker ethic survives, and it is a fraud. It survives in anyone excited by technology's power to turn many small, insignificant things into one vast, beautiful thing. It is a fraud because there is nothing magical about computers that causes a user to undergo religious conversion and devote himself to the public good. Early automobile inventors were hackers too. At first the elite drove in luxury. Later practically everyone had a car. Now we have traffic jams, drunk drivers, air pollution, and suburban sprawl. The old magic of an automobile occasionally surfaces, but we possess no delusions that it automatically invades the consciousness of anyone who sits behind the wheel. Computers are power, and direct contact with power can bring out the best or the worst in a person. It's tempting to think that everyone exposed to the technology will be grandly inspired, but, alas, it just ain't so.

BRAND [Day 1, 9:54 A.M.]: The hacker ethic involves several things. One is avoiding waste; insisting on using idle computer power—often hacking into a system to do so, while taking the greatest precautions not to damage the system. A second goal of many hackers is the free exchange of technical information. These hackers feel that patent and copyright restrictions slow down technological advances. A third goal is the advancement of human knowledge for its own sake. Often this approach is unconventional. People we call crackers often explore systems and do mischief. They are called hackers by the press, which doesn't understand the issues.

KK [Day 1, 11:19 A.M.]: The hacker ethic went unnoticed early on because the explorations of basement tinkerers were very local. Once we all became connected, the work of these investigators rippled through the world. Today the hacking spirit is alive and kicking in video, satellite TV, and radio. In some fields they are called chippers, because they modify and peddle altered chips. Everything that was once said about "phone phreaks" can be said about them too.

DAVE [Day 1, 11:29 A.M.]: Bah. Too academic. Hackers hack. Because they want to. Not for any higher purpose. Hacking is not dead and won't be as long as teenagers get their hands on the tools. There is a hacker born every minute.

ADELAIDE [Day 1, 11:42 A.M.]: Don't forget ego. People break into computers because it's fun and it makes them feel powerful.

BARLOW [Day 1, 11:54 A.M.]: Hackers hack. Yeah, right, but what's more to the point is that humans hack and always have. Far more than just opposable thumbs, upright posture, or excess cranial capacity, human beings are set apart from all other species by an itch, a hard-wired dissatisfaction. Computer hacking is just the latest in a series of quests that started with fire hacking. Hacking is also a collective enterprise. It brings to our joint endeavors the simultaneity that other collective organisms—ant colonies, Canada geese—take for granted. This is important, because combined with our itch to probe is a need to *connect*. Humans miss the almost telepathic connectedness that I've observed in other herding mammals. And we want it back. Ironically, the solitary sociopath and his 3:00 A.M. endeavors hold the most promise for delivering species reunion.

EDDIE JOE HOMEBOY [Day 1, 4:44 P.M.]: Hacking really took hold with the advent of the personal computer, which freed programmers from having to use a big time-sharing system. A hacker could sit in the privacy of his home and hack to his heart's and head's content.

LEE [Day 1, 5:17 P.M.]: "Angelheaded hipsters burning for the ancient heavenly connection to the starry dynamo in the machinery of night" (Allen Ginsberg, "Howl"). I still get an endorphin rush when I go on a design run—my mind out over the edge, groping for possibilities that can be sensed when various parts are held in juxtaposition with a view toward creating a whole object: straining to get through the epsilon-wide crack between What Is and What Could Be. Somewhere there's the Dynamo of Night, the ultra-mechanism waiting to be dreamed, that we'll never get to in actuality (think what it would *weigh*!) but that's present somehow in the vicinity of those mental wrestling matches. When I reemerge into the light of another day with the design on paper—and with the knowledge that if it ever gets built, things will never be the same again—I know I've been where artists go. That's hacking to me: to transcend custom and to engage in creativity for its own sake, but also to create objective effects. I've been around long enough to see the greed creeps take up the unattended reins of power and shut down most of the creativity that put them where they are. But I've also seen things change, against the best efforts of a stupidly run industry. We cracked the egg out from

under the Computer Priesthood, and now everyone can have omelets.

RMS [Day 1, 5:19 P.M.]: The media and the courts are spreading a certain image of hackers. It's important for us not to be shaped by that image. But there are two ways that it can happen. One way is for hackers to become part of the security-maintenance establishment. The other, more subtle, way is for a hacker to become the security-breaking phreak the media portray. By shaping ourselves into the enemy of the establishment, we uphold the establishment. But there's nothing wrong with breaking security if you're accomplishing something useful. It's like picking a lock on a tool cabinet to get a screwdriver to fix your radio. As long as you put the screwdriver back, what harm does it do?

ACID PHREAK [Day 1, 6:34 P.M.]: There is no one hacker ethic. Everyone has his own. To say that we all think the same way is preposterous. The hacker of old sought to find what the computer itself could do. There was nothing illegal about that. Today, hackers and phreaks are drawn to *specific*, often corporate, systems. It's no wonder everyone on the other side is getting mad. We're always one step ahead. We were back then, and we are now.

CLIFF [Day 1, 8:38 P.M.]: RMS said, "There's nothing wrong with breaking security if you're accomplishing something useful." Huh? How about, There's nothing wrong with entering a neighbor's house if you're accomplishing something useful, just as long as you clean up after yourself. Does my personal privacy mean anything? Should my personal letters and data be open to anyone who knows how to crack passwords? If not my property, then how about a bank's? Should my credit history be available to anyone who can find a back door to the private computers of TRW, the firm that tracks people's credit histories? How about a list of AIDS patients from a hospital's data bank? Or next week's prime interest rate from a computer at the Treasury Department?

BLUEFIRE [Day 1, 9:20 P.M.]: Computers are everywhere, and they link us together into a vast social "cybernetia." The grand skills of the hackers, formidable though they may have been, are incapable of subverting this automated social order. The networks in which we survive are more than copper wire and radio waves: They are *the* social organization. For every hacker in revolt, busting through a security code, ten thousand people are being wired up with automatic call-identification and credit-checking machines. Long live the Computer Revolution, which died aborning.

JRC [Day 1, 10:28 P.M.]: We have two different definitions here. One speaks of a tinkerer's ecstasy, an ecstasy that is hard to maintain in the corporate world but is nevertheless at the heart of Why Hackers Hack. The second is political, and it has to do with the free flow of information. Information should flow more freely (how freely is being debated), and the hacker can make it happen because the hacker knows how to undam the pipes. This makes the hacker ethic—of necessity—antiauthoritarian.

EMMANUEL GOLDSTEIN [Day 2, 2:41 A.M.]: It's meaningless what we call ourselves: hackers, crackers, techno-rats. We're individuals who happen to play with high tech. There is no *hacker community* in the traditional sense of the term. There are no leaders and no agenda. We're just individuals out exploring.

BRAND [Day 2, 9:02 A.M.]: There are two issues: invariance and privacy. Invariance is the art of leaving things as you found them. If someone used my house for the day and left everything as he found it so that there was *no way* to tell he had been there, I would see no problem. With a well-run computer system, we can assure invariance. Without this assurance we must fear that the person picking the lock to get the screwdriver will break the lock, the screwdriver, or both. Privacy is more complicated. I want my medical records, employment records, and let-

A HACKER'S LEXICON

Back door: A point of entry into a computer system—often installed there by the original programmer—that provides secret access.

Bomb: A destructive computer program, which, when activated, destroys the files in a computer system.

Chipper: A hacker who specializes in changing the programming instructions of computer chips.

Cracker: A hacker who breaks illegally into computer systems and creates mischief; often used pejoratively. The original meaning of *cracker* was narrower, describing those who decoded copyright-protection schemes on commercial software products either to redistribute the products or to modify them; sometimes known as a software pirate.

Hacker: Originally, a compulsive computer programmer. The word has evolved in meaning over the years. Among computer users, *hacker* carries a positive connotation, meaning anyone who creatively explores the operations of computer systems. Recently, it has taken on a negative connotation, primarily through confusion with *cracker*.

Phone phreak: One who explores the operations of the phone system, often with the intent of making free phone calls.

Social engineering: A nontechnical means of gaining information simply by persuading people to hand it over. If a hacker wished to gain access to a computer system, for example, an act of *social engineering* might be to contact a system operator and to convince him or her that the hacker is a legitimate user in need of a password; more colloquially, a con job.

Virus: A program that, having been introduced into a system, replicates itself and attaches itself to other programs, often with a variety of mischievous effects.

Worm: A destructive program that, when activated, fills a computer system with self-replicating information, clogging the system so that its operations are severely slowed, sometimes stopped.

ters to *The New Republic* private because I fear that someone will do something with the information that is against my interests. If I could trust people not to do bad things with information, I would not need to hide it. Rather than preventing the "theft" of this data, we should prohibit its collection in the first place.

HOMEBOY [Day 2, 9:37 A.M.]: Are crackers really working for the free flow of information? Or are they unpaid tools of the establishment, identifying the holes in the institutional dike so that they can be plugged by the authorities, only to be tossed in jail or exiled?

DRAKE [Day 2, 10:54 A.M.]: There is an unchallenged assumption that crackers have some political motivation. Earlier, crackers were portrayed as failed revolutionaries; now Homeboy suggests that crackers may be tools of the establishment. These ideas about crackers are based on earlier experiences with subcultures (beats, hippies, yippies). Actually, the contemporary cracker is often middle-class and doesn't really distance himself from the "establishment." While there are some anarcho-crackers, there are even more right-wing crackers. The hacker ethic crosses political boundaries.

MANDEL [Day 2, 11:01 A.M.]: The data on crackers suggests that they are either juvenile delinquents or plain criminals.

BARLOW [Day 2, 11:34 A.M.]: I would far rather have *everyone* know my most intimate secrets than to have noncontextual snippits of them "owned" by TRW and the FBI—and withheld from me! Any cracker who is entertained by peeping into my electronic window is welcome to the view. Any institution that makes money selling rumors of my peccadilloes is stealing from me. Anybody who wants to inhibit that theft with electronic mischief has my complete support. Power to the techno-rats!

EMMANUEL [Day 2, 7:09 P.M.]: Calling someone on the phone is the equivalent of knocking on that person's door, right? Wrong! When someone answers the phone, you are *inside* the home. You have already been *let in.* The same with an answering machine, or a personal computer, if it picks up the phone. It is wrong to violate a person's privacy, but electronic rummaging is not the same as breaking and entering. The key here is that most people are unaware of *how easy it is* for others to invade their electronic privacy and see credit reports, phone bills, FBI files, Social Security reports. The public is grossly underinformed, and that's what must be fixed if hackers are to be thwarted. If we had an educated public, though, perhaps the huge—and now common—data bases would never have been allowed to exist. Hackers have become scapegoats: We discover the gaping holes in the system and then get blamed for the flaws.

HOMEBOY [Day 2, 7:41 P.M.]: Large, insular, undemocratic governments and institutions need scapegoats. It's the first step down the road to fascism. *That's* where hackers play into the hands of the establishment.

DAVE [Day 2, 7:55 P.M.]: If the real criminals are those who leave gaping holes in their systems, then the real criminals in house burglaries are those who leave their windows unlatched. Right? Hardly. And Emmanuel's analogy to a phone being answered doesn't hold either. There is no security protection in making a phone call. A computer system has a *password,* implying a desire for security. Breaking into a poorly protected house is still burglary.

CLIFF [Day 2, 9:06 P.M.]: Was there a hacker's ethic and does it survive? More appropriately, was there a vandal's ethic and does it survive? As long as there are communities, someone will violate the trust that binds them. Once, our computers were isolated, much as eighteenth-century villages were. Little was exchanged, and each developed independently. Now we've built far-flung electronic neighborhoods. These communities are built on trust: people believing that everyone profits by sharing resources. Sure enough, vandals crept in, breaking into systems, spreading viruses, pirating software, and destroying people's work. "It's okay," they say. "I can break into a system because I'm a hacker." Give me a break!

BARLOW [Day 2, 10:41 P.M.]: I live in a small town. I don't have a key to my house. Am I asking for it? I think not. Among the juvenile delinquents in my town, there does exist a vandal's ethic. I know because I once was one. In a real community, part of a kid's rite of passage is discovering what walls can be breached. Driving 110 miles per hour on Main Street is a common symptom of rural adolescence, publicly denounced but privately understood. Many teenagers die in this quest—two just the night before last—but it is basic to our culture. Even rebellious kids understand that risk to one's safety is one thing, wanton vandalism or theft is another. As a result, almost no one locks anything here. In fact, a security system is an affront to a teenage psyche. While a kid might be dissuaded by conscience, he will regard a barricade as an insult and a challenge. So the CEOs who are moving here (the emperor of PepsiCo and the secretary of state among them) soon discover that over the winter people break into their protected mansions just to hang out. When systems are open, the community prospers, and teenage miscreants are sat-

isfied to risk their own lives and little else. When the social contract is enforced by security, the native freedom of the adolescent soul will rise up to challenge it in direct proportion to its imposition.

HANK [Day 2, 11:23 P.M.]: Barlow, the small town I grew up in was much like yours—until two interstate highways crossed nearby. The open-door style changed in one, hard summer because our whole *town* became unlocked. I think Cliff's community is analogous to my little town—confronted not by a new locked-up neighbor who poses a challenge to the local kids but by a sudden, permanent opening up of the community to many faceless outsiders who owe the town no allegiance.

EMMANUEL [Day 3, 1:33 A.M.]: Sorry, I don't buy Dave's unlatched-window analogy. A hacker who wanders into a system with the ease that it's done today is, in my analogy, walking into a house without walls—and with a cloaking device! Any good hacker can make himself invisible. If housebreaking were this easy, people would be enraged. But we're missing the point. I'm not referring to accessing a PC in someone's bedroom but about accessing credit reports, government files, motor vehicle records, and the megabytes of data piling up on each of us. Thousands of people legally can see and use this ever-growing mountain of data, much of it erroneous. Whose rights are we violating when we peruse a file? Those of the person we look up? He doesn't even know that information exists, that it was compiled without his consent, and that it's not his property anymore! The invasion of privacy took place long before the hacker ever arrived. The only way to find out how such a system works is to break the rules. It's not what hackers do that will lead us into a state of constant surveillance; it's allowing the authorities to impose on us a state of mock crisis.

MANDEL [Day 3, 9:27 A.M.]: Note that the word *crime* has no fixed reference in our discussion. Until recently, breaking into government computer systems wasn't a crime; now it is. In fact, there is some debate, to be resolved in the courts, whether what Robert Morris Jr. did was actually a crime [see "A Brief History of Hacking"]. *Crime* gets redefined all the time. Offend enough people or institutions and, lo and behold, someone will pass a law. That is partly what is going on now: Hackers are pushing buttons, becoming more visible, and that inevitably means more laws and more crimes.

ADELAIDE [Day 3, 9:42 A.M.]: Every practitioner of these arts knows that at minimum he is trespassing. The English "country traveler ethic" applies: The hiker is always ethical enough to close the pasture gates behind him so that no sheep escape during his pastoral stroll through someone else's property. The problem is that what some see as gentle trespassing others see as theft of service, invasion of privacy, threat to national security—take your pick.

BARLOW [Day 3, 2:38 P.M.]: I regard the *existence* of proprietary data about me to be theft—not just in the legal sense but in a faintly metaphysical one, rather like the belief among aborigines that a photograph steals the soul. The crackers who maintain access to that data are, at this level, liberators. Their incursions are the only way to keep the system honest.

RMS [Day 3, 2:48 P.M.]: Recently, a tough anti-hacker measure was proposed in England. In *The Economist* I saw a wise response, arguing that it was silly to treat an action as worse when it involves a computer than when it does not. They noted, for example, that physical trespassing was considered a civil affair, not a criminal one, and said that computer trespassing should be treated likewise. Unfortunately, the U.S. government was not so wise.

BARLOW [Day 3, 3:23 P.M.]: The idea that a crime is worse if a computer is involved relates to the gathering governmental perception that computer viruses and guns may be related. I know that sounds absurd, but they have more in common than one might think. For all its natural sociopathy, the virus is not without philosophical potency—like a gun. Here in Wyoming guns are part of the furniture. Only recently have I observed an awareness of their political content. After a lot of frothing about prying cold, dead fingers from triggers, the sentiment was finally distilled to a bumper sticker I saw on a pickup the other day: "Fear the Government That Fears Your Gun." Now I've read too much Gandhi to buy that line without misgivings, but it would be hard to argue that Tiananmen Square could have been inflicted on a populace capable of shooting back. I don't wholeheartedly defend computer viruses, but one must consider their increasingly robust deterrent potential. Before it's over, the War on Drugs could easily turn into an Armageddon between those who love liberty and those who crave certainty, providing just the excuse the control freaks have been waiting for to rid America of all that constitutional mollycoddling called the Bill of Rights. Should that come to pass, I will want to use every available method to vex and confuse the eyes and ears of surveillance. The virus could become the necessary instrument of our freedom. At the risk of sounding like some digital *posse comitatus*, I say: Fear the Government That Fears Your Computer.

TENNEY [Day 3, 4:41 P.M.]: Computer-related crimes are more feared because they are performed remotely—a crime can be committed in New York by someone in Los Angeles—and by people not normally viewed as being criminals—by teenagers who don't look like delinquents. They're very smart nerds, and they don't look like Chicago gangsters packing heat.

BARLOW [Day 4, 12:12 A.M.]: People know so little of these things that they endow computers and the people who *do* understand them with powers neither possesses. If America has a religion, its ark is the computer and its covenant is the belief that Science Knows. We are mucking around in the temple, guys. It's a good way to catch hell.

DAVE [Day 4, 9:18 A.M.]: Computers *are* the new American religion. The public is in awe of—and fears—the mysteries and the high priests who tend them. And the public reacts just as it always has when faced with fear of the unknown—punishment, burning at the stake. Hackers are like the early Christians. When caught, they will be thrown to the lions before the Roman establishment: This year the mob will cheer madly as Robert Morris is devoured.

KK [Day 6, 11:37 A.M.]: The crackers here suggest that they crack into systems with poor security *because* the security is poor. Do more sophisticated security precautions diminish the need to crack the system or increase it?

ACID [Day 6, 1:20 P.M.]: If there was a system that we knew was uncrackable, we wouldn't even try to crack it. On the other hand, if some organization boasted that its system was impenetrable and we knew that was media hype, I think it would be safe to say we'd have to "enlighten" them.

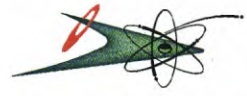
EMMANUEL [Day 6, 2:49 P.M.]: Why do we insist on cracking systems? The more people ask those kinds of questions, the more I want to get in! Forbid access and the demand for access increases. For the most part, it's simply a mission of exploration. In the words of the new captain of the starship *Enterprise*, Jean-Luc Picard, "Let's see what's out there!"

BARLOW [Day 6, 4:34 P.M.]: Tell us, Acid, *is* there a system that you know to be uncrackable to the point where everyone's given up?

ACID [Day 6, 8:29 P.M.]: CICIMS is pretty tough.

PHIBER OPTIK [Day 7, 2:36 P.M.]: Really? CICIMS is a system used by Bell operating companies. The entire security system was changed after myself and a friend must have been noticed in it. For the entire United States, there is only one such system, located in Indiana. The new security scheme is flawless *in itself*, and there is no chance of "social engineering," i.e., bullshitting someone inside the system into telling you what the passwords are. The system works like this: You log on with the proper account and password; then, depending on who you are, the system asks at random three of ten questions that are unique to each user. But the system *can* be compromised by entering forwarding instructions into the phone company's switch for that exchange, thereby intercepting every phone call that comes in to the system over a designated period of time and connecting the call to your computer. If you are familiar with the security layout, you can emulate its appearance and fool the caller into giving you the answers to his questions. Then you call the system yourself and use those answers to get in. There are other ways of doing it as well.

"THE VIRUS *COULD* BECOME AN INSTRUMENT OF FREEDOM. AT THE RISK OF SOUNDING LIKE SOME DIGITAL *POSSE COMITATUS*, I SAY: FEAR THE GOVERNMENT THAT FEARS YOUR COMPUTER."



BLUEFIRE [Day 7, 11:53 P.M.]: I can't stand it! Who do you think pays for the security that the telephone companies must maintain to fend off illegal use? I bet it costs the ratepayers around $10 million for this little extravaganza. The cracker circus isn't harmless at all, unless you don't mind paying for other people's entertainment. Hackers who have contributed to the social welfare should be recognized. But cracking is something else—namely, fun at someone else's expense—and it ain't the folks who own the phone companies who pay; it's us, me and you.

BARLOW [Day 8, 7:35 A.M.]: I am becoming increasingly irritated at this idea that you guys are exacting vengeance for the sin of openness. You seem to argue that if a system is dumb enough to be open, it is your moral duty to violate it. Does the fact that I've never locked my house—even when I was away for months at a time—mean that someone should come in and teach me a good lesson?

ACID [Day 8, 3:23 P.M.]: Barlow, you leave the door open to your house? Where do you live?

Illustration by Valerie Sinclair

BARLOW [Day 8, 10:11 P.M.]: Acid, my house is at 372 North Franklin Street in Pinedale, Wyoming. Heading north on Franklin, go about two blocks off the main drag before you run into a hay meadow on the left. I'm the last house before the field. The computer is always on. But do you really mean to imply what you did with that question? Are you merely a sneak looking for easy places to violate? You disappoint me, pal. For all your James Dean-on-Silicon rhetoric, you're not a cyberpunk. You're just a punk.

EMMANUEL [Day 9, 12:55 A.M.]: No offense, Barlow, but your house analogy doesn't stand up, because your house is far less interesting than a Defense Department computer. For the most part, hackers don't mess with individuals. Maybe we feel sorry for them; maybe they're boring. Institutions are where the action is, because they are compiling this mountain of data—without your consent. Hackers are not guardian angels, but if you think we're what's wrong with the system, I'd say that's precisely what those in charge want you to believe. By the way, you left out your zip code. It's 82941.

BARLOW [Day 9, 8:34 A.M.]: Now that's more like it. There is an ethical distinction between people and institutions. The law makes little distinction. We pretend that institutions are somehow human because they are made of humans. A large bureaucracy resembles a human about as much as a reef resembles a coral polyp. To expect an institution to have a conscience is like expecting a horse to have one. As with every organism, institutions are chiefly concerned with their own physical integrity and survival. To say that they have some higher purpose beyond their survival is to anthropomorphize them. You are right, Emmanuel. The house analogy breaks down here. Individuals live in houses; institutions live in mainframes. Institutions are functionally remorseless and need to be checked. Since their blood is digital, we need to be in their bloodstreams like an infection of humanity. I'm willing to extend limitless trust to other human beings. In my experience they've never failed to deserve it. But I have as much faith in institutions as they have in me. None.

OPTIK [Day 9, 10:19 A.M.]: In other words, Mr. Barlow, you say something, someone proves you wrong, and then you agree with him. I'm getting the feeling that you don't exactly chisel your views in stone.

HANK [Day 9, 11:18 A.M.]: Has Mr. Optik heard the phrase "thesis, antithesis, synthesis"?

BARLOW [Day 10, 10:48 A.M.]: Optik, I do change my mind a lot. Indeed, I often find it occupied by numerous contradictions. The last time I believed in absolutes, I was about your age. And there's not a damn thing wrong with believing in absolutes at your age either. Continue to do so, however, and you'll find yourself, at my age, carrying placards filled with nonsense and dressing in rags.

ADELAIDE [Day 10, 6:27 P.M.]: The flaw in this discussion is the distorted image the media promote of

A BRIEF HISTORY OF HACKING

September 1970—John Draper takes as his alias the name Captain Crunch after he discovers that the toy whistle found in the cereal of the same name perfectly simulates the tone necessary to make free phone calls.

March 1975—The Homebrew Computer Club, an early group of computer hackers, holds its first meeting in Menlo Park, California.

July 1976—Homebrew members Steve Wozniak, twenty-six, and Steve Jobs, twenty-one, working out of a garage, begin selling the first personal computer, known as the Apple.

June 1980—In one week, errors in the computer system operating the U.S. air-defense network cause two separate false reports of Soviet missile launches, each prompting an increased state of nuclear readiness.

December 1982—Sales of Apple personal computers top one billion dollars per year.

November 1984—Steven Levy's book *Hackers* is published, popularizing the concept of the "hacker ethic": that "access to computers, and anything that might teach you something about the way the world works, should be unlimited and total." The book inspires the first Hacker's Conference, held that month.

January 1986—The "Pakistani Brain" virus, created by a software distributor in Lahore, Pakistan, infects IBM computers around the world, erasing data files.

June 1986—The U.S. Office of Technology Assessment warns that massive, cross-indexed government computer records have become a "de facto national data base containing personal information on most Americans."

March 1987—William Gates, a Harvard dropout who founded Microsoft Corporation, becomes a billionaire.

November 1988—More than 6,000 computers linked by the nationwide Internet computer network are infected by a destructive computer program known as a worm and are crippled for two days. The worm is traced to Robert Morris Jr., a twenty-four-year-old Cornell University graduate student.

December 1988—A federal grand jury charges Kevin Mitnick, twenty-five, with stealing computer programs over telephone lines. Mitnick is held without bail and forbidden access to any telephones without supervision.

March 1989—Three West German hackers are arrested for entering thirty sensitive military computers using home computers and modems. The arrests follow a three-year investigation by Clifford Stoll, an astronomer at the Lawrence Berkeley Laboratory who began tracing the hackers after finding a seventy-five-cent billing error in the lab's computer system.

January 1990—Robert Morris Jr. goes on trial in Syracuse, New York, for designing and releasing the Internet worm. Convicted, he faces up to five years in prison and a $250,000 fine.

the hacker as "whiz." The problem is that the one who gets caught obviously isn't. I haven't seen a story yet on a true genius hacker. Even Robert Morris was no whiz. The genius hackers are busy doing constructive things or are so good no one's caught them yet. It takes no talent to break into something. Nobody calls subway graffiti artists geniuses for figuring out how to break into the yard. There's a difference between genius and ingenuity.

BARLOW [Day 10, 9:48 P.M.]: Let me define my terms. Using *hacker* in a midspectrum sense (with crackers on one end and Leonardo da Vinci on the other), I think it does take a kind of genius to be a truly productive hacker. I'm learning PASCAL now, and I am constantly amazed that people can spin those prolix recursions into something like PageMaker. It fills me with the kind of awe I reserve for splendors such as the cathedral at Chartres. With crackers like Acid and Optik, the issue is less intelligence than alienation. Trade their modems for skateboards and only a slight conceptual shift would occur. Yet I'm glad they're wedging open the cracks. Let a thousand worms flourish.

OPTIK [Day 10, 10:11 P.M.]: You have some pair of balls comparing my talent with that of a skateboarder. Hmm... This was indeed boring, but nonetheless: [*Editors' Note: At this point in the discussion, Optik—apparently having hacked into TRW's computer records—posted a copy of* Mr. *Barlow's credit history. In the interest of* Mr. *Barlow's privacy—at least what is left of it*—Harper's Magazine *has not printed it.*] I'm not showing off. Any fool knowing the proper syntax and the proper passwords can look up a credit history. I just find your high-and-mighty attitude annoying and, yes, infantile.

HOMEBOY [Day 10, 10:17 P.M.]: Key here is "any fool."

ACID [Day 11, 1:37 P.M.]: For thirty-five dollars a year anyone can have access to TRW and see his or her own credit history. Optik did it for free. What's wrong with that? And why does TRW keep files on what color and religion we are? If you didn't know that they kept such files, who would have found out if it wasn't for a hacker? Barlow should be grateful that Optik has offered his services to update him on his personal credit file. Of course, I'd hate to see my credit history up in lights. But if you hadn't made our skins crawl, your info would not have been posted. Everyone gets back at someone when he's pissed; so do we. Only we do it differently. Are we punks? Yeah, I guess we are. A punk is what someone who has been made to eat his own words calls the guy who fed them to him.

Hacking the Constitution

HARPER'S [Day 4, 9:00 A.M.]: Suppose that a mole inside the government confirmed the existence of files on each of you, stored in the White House computer system, PROFS. Would you have the right to hack into that system to retrieve and expose the existence of such files? Could you do it?

TENNEY [Day 4, 1:42 P.M.]: The proverbial question of whether the end justifies the means. This doesn't have much to do with hacking. If the file were a sheet of paper in a locked cabinet, the same question would apply. In that case you could accomplish everything without technological hacking. Consider the Pentagon Papers.

EMMANUEL [Day 4, 3:55 P.M.]: Let's address the hypothetical. First, I need to find out more about PROFS. Is it accessible from off site, and if so, how? Should I update my 202-456 scan [a list of phone numbers in the White House's exchange that connect incoming calls to a computer]? I have a listing for every computer in that exchange, but the scan was done back in 1984. Is PROFS a new system? Perhaps it's in a different exchange? Does anybody know how many people have access to it? I'm also on fairly good terms with a White House operator who owes me a favor. But I don't know what to ask for. Obviously, I've already made up my mind about the *right* to examine this material. I don't want to debate the ethics of it at this point. If you're with me, let's do something about this. Otherwise, stay out of the way. There's hacking to be done.

ACID [Day 4, 5:24 P.M.]: Yes, I would try to break into the PROFS system. But first I'd have someone in the public eye, with no ties to hacking, request the info through the Freedom of Information Act. Then I'd hack in to verify the information I received.

DRAKE [Day 4, 9:13 P.M.]: Are there a lot of people involved in this antihacker project? If so, the chances of social engineering data out of people would be far higher than if it were a small, close-knit group. But yes, the simple truth is, if the White House has a dial-up line, it can be hacked.

EMMANUEL [Day 4, 11:27 P.M.]: The implication that a trust has been betrayed on the part of the government is certainly enough to make me want to look a little further. And I know I'm doing the right thing on behalf of others who don't have my abilities. Most people I meet see me as an ally who can help them stay ahead of an unfair system. That's what I intend to do here. I have a small core of dedicated hackers

who could help. One's specialty is the UNIX system, another's is networks, and another's is phone systems.

TENNEY [Day 5, 12:24 A.M.]: PROFS is an IBM message program that runs on an operating system known as VM. VM systems usually have a fair number of holes, either to gain access or to gain full privileges. The CIA was working on, and may have completed, a supposedly secure VM system. No ethics here, just facts. But a prime question is to determine what system via what phone number. Of course, the old inside job is easier. Just find someone who owes a favor or convince an insider that it is a moral obligation to do this.

BARLOW [Day 5, 2:46 P.M.]: This scenario needs to be addressed in four parts: ethical, political, practical I (from the standpoint of the hack itself), and practical II (disseminating the information without undue risk).

Ethical: Since World War II, we've been governed by a paramilitary bureaucracy that believes freedom is too precious to be entrusted to the people. These are the same folks who had to destroy the village in order to save it. Thus the government has become a set of Chinese boxes. Americans who believe in democracy have little choice but to shred the barricades of secrecy at every opportunity. It isn't merely permissible to hack PROFS. It is a moral obligation.

Political: In the struggle between control and liberty, one has to avoid action that will drive either side to extreme behavior. The basis of terrorism, remember, is excess. If we hack PROFS, we must do it in a way that doesn't become a pretext for hysterical responses that might eventually include zero tolerance of personal computers. The answer is to set up a system for entry and exit that never lets on we've been there.

Practical I: Hacking the system should be a trivial undertaking.

Practical II: Having retrieved the smoking gun, it must be made public in such a way that the actual method of acquisition does not become public. Consider Watergate: The prime leaker was somebody whose identity and information-gathering technique is still unknown. So having obtained the files, we turn them over to the *Washington Post* without revealing our own identities or how we came by the files.

EMMANUEL [Day 5, 9:51 P.M.]: PROFS is used for sending messages back and forth. It's designed *not* to forget things. And it's used by people who are not computer literate. The document we are looking for is likely an electronic-mail message. If we can find out who the recipient or sender is, we can take it from there. Since these people frequently use the system to communicate, there may be a way for them to dial into the White House from home. Finding that number won't be difficult: frequent calls to a number local to the White House and common to a few different people. Once I get the dial-up, I'll have to look at whatever greeting I get to determine what kind of system it is. Then we need to locate someone expert in the system to see if there are any built-in back doors. If there aren't, I will social engineer my way into a working account and then attempt to break out of the program and explore the entire system.

BRAND [Day 6, 10:06 A.M.]: I have two questions: Do you believe in due process as found in our Constitution? And do you believe that this "conspiracy" is so serious that extraordinary measures need to be taken? If you believe in due process, then you shouldn't hack into the system to defend our liberties. If you don't believe in due process, you are an anarchist and potentially a terrorist. The government is justified in taking *extreme* action to protect itself and the rest of us from you. If you believe in the Constitution but also that this threat is so extreme that patriots have a duty to intercede, then you should seek one of the honest national officials who can legally demand a copy of the document. If you believe that there is no sufficiently honest politician and you steal and publish the documents, you are talking about a revolution.

ACID [Day 6, 1:30 P.M.]: This is getting too political. Who says that hacking has to have a political side? Generalizing does nothing but give hackers a false image. I couldn't care less about politics, and I hack.

LEE [Day 6, 9:01 P.M.]: Sorry, Acid, but if you hack, what you do is inherently political. Here goes: Political power is exercised by control of information channels. Therefore, any action that changes the capability of someone in power to control these channels *is* politically relevant. Historically, the one in power has been not the strongest person but the one who has convinced the goon squad to do his bidding. The goons give their power to him, usually in exchange for free food, sex, and great uniforms. The turning point of most successful revolutions is when the troops ignore the orders coming from above and switch their allegiance. Information channels. Politics. These days, the cracker represents a potential for making serious political change if he coordinates with larger social and economic forces. Without this coordination, the cracker is but a techno-bandit, sharpening his weapon and chuckling about how someday . . . Revolutions often make good use of bandits, and some

of them move into high positions when they're successful. But most of them are done away with. One cracker getting in won't do much good. Working in coordination with others is another matter—called politics.

JIMG [Day 7, 12:28 A.M.]: A thought: Because it has become so difficult to keep secrets (thanks, in part, to crackers), and so expensive and counterproductive (the trade-off in lost opportunities is too great), secrets are becoming less worth protecting. Today, when secrets come out that would have brought down governments in the past, "spin-control experts" shower the media with so many lies that the truth is obscured despite being in plain sight. It's the information equivalent of the Pentagon plan to surround each real missile with hundreds of fake ones, rendering radar useless. If hackers managed to crack the White House system, a hue and cry would be raised—not about what the hackers found in the files but about what a threat hackers are to this great democracy of ours.

HARPER'S [Day 7, 9:00 A.M.]: Suppose you hacked the files from the White House and a backlash erupted. Congressmen call for restrictions, arguing that the computer is "property" susceptible to regulation and not an instrument of "information" protected by the First Amendment. Can we craft a manifesto setting forth your views on how the computer fits into the traditions of the American Constitution?

DAVE [Day 7, 5:30 P.M.]: If Congress ever passed laws that tried to define what we do as "technology" (regulatable) and *not* "speech," I would become a rebellious criminal immediately—and as loud as Thomas Paine ever was. Although computers are part "property" and part "premises" (which suggests a need for privacy), they are supremely instruments of *speech*. I don't want any congressional King Georges treading on my cursor. We must continue to have *absolute* freedom of electronic speech!

BARLOW [Day 7, 10:07 P.M.]: Even in a court guided by my favorite oxymoron, Justice Rehnquist, this is an open-and-shut case. The computer is a printing press. Period. The only hot-lead presses left in this country are either in museums or being operated by poets in Vermont. The computer cannot fall under the kind of regulation to which radio and TV have become subject, since computer output is not broadcast. If these regulations amount to anything more than a fart in the congressional maelstrom, then we might as well scrap the whole Bill of Rights. What I am doing with my fingers right now is "speech" in the clearest sense of the word. We don't need no stinking manifestos.

JIMG [Day 8, 12:02 A.M.]: This type of congressional action is so clearly unconstitutional that "law hackers"—everyone from William Kunstler to Robert Bork—would be all over it. The whole idea runs so completely counter to our laws that it's hard to get worked up about it.

"I DON'T WANT ANY CONGRESSIONAL KING GEORGE TREADING ON MY CURSOR. WE MUST CONTINUE TO HAVE *ABSOLUTE* FREEDOM OF ELECTRONIC SPEECH."

ADELAIDE [Day 8, 9:51 A.M.]: Not so fast. There used to be a right in the Constitution called "freedom from unreasonable search and seizure," but, thanks to recent Supreme Court decisions, your urine can be demanded by a lot of people. I have no faith in the present Supreme Court to uphold any of my rights of free speech. The complacent reaction here—that whatever Congress does will eventually be found unconstitutional—is the same kind of complacency that led to the current near-reversals of *Roe* v. *Wade*.

JRC [Day 8, 10:05 A.M.]: I'd forgo the manifestos and official explanations altogether: Fight brushfire wars against specific government incursions and wait for the technology to metastasize. In a hundred years, people won't have to be told about computers because they will have an instinctive understanding of them.

KK [Day 8, 2:14 P.M.]: Hackers are not sloganeers. They are doers, take-things-in-handers. They are the opposite of philosophers: They don't wait for language to catch up to them. Their arguments are their actions. You want a manifesto? The Internet worm was a manifesto. It had more meaning and symbolism than any revolutionary document you could write. To those in power running the world's nervous system, it said: Wake up! To the underground of hackers, crackers, chippers, and techno-punks, it said: You have power; be careful. To the mass of citizens who find computers taking over their telephone, their TV, their toaster, and their house, it said: Welcome to Wonderland.

BARLOW [Day 8, 10:51 P.M.]: Apart from the legal futility of fixing the dam after it's been

breached, I've never been comfortable with manifestos. They are based on the ideologue's delusion about the simplicity, the figure-outability, of the infinitely complex thing that is Life Among the Humans. Manifestos take reductionism for a long ride off a short pier. Sometimes the ride takes a very long time. Marx and Engels didn't actually crash until last year. Manifestos fail because they are fixed and consciousness isn't. I'm with JRC: Deal with incursions when we need to, on our terms, like the guerrillas we are. To say that we can outmaneuver those who are against us is like saying that honeybees move quicker than Congress. The future is to the quick, not the respectable.

RH [Day 8, 11:43 P.M.]: Who thinks computers can't be regulated? The Electronic Communications Privacy Act of 1986 made it a crime to own "any electronic, mechanical, or other device [whose design] renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communication." Because of the way Congress defined "electronic communication," one could argue that even a modem is a surreptitious interception device (SID), banned by the ECPA and subject to confiscation. It's not that Congress intended to ban modems; it was just sloppy drafting. The courts will ultimately decide what devices are legal. Since it may not be possible to draw a clear bright line between legal and illegal interception devices, the gray area—devices with both legitimate and illegitimate uses—may be subject to regulation.

BARLOW [Day 9, 8:52 A.M.]: I admit with some chagrin that I'm not familiar with the ECPA. It seems I've fallen on the wrong side of an old tautology: Just because all saloon keepers are Democrats, it doesn't follow that all Democrats are saloon keepers. By the same token, the fact that all printing presses are computers hardly limits computers to that function. And one of the other things computers are good at is surreptitious monitoring. Maybe there's more reason for concern than I thought. Has any of this stuff been tested in the courts yet?

RH [Day 9, 10:06 P.M.]: My comments about surreptitious interception devices are not based on any court cases, since there have not been any in this area since the ECPA was enacted. It is a stretch of the imagination to think that a judge would ever find a stock, off-the-shelf personal computer to be a "surreptitious interception device." But a modem is getting a little closer to the point where a creative prosecutor could make trouble for a cracker, with fallout affecting many others. An important unknown is how the courts will apply the word *surreptitious*. There's very little case law, but taking it to mean "by stealth; hidden from view; having its true purpose physically disguised," I can spin some worrisome examples. I lobbied against the bill, pointing out the defects. Congressional staffers admitted privately that there was a problem, but they were in a rush to get the bill to the floor before Congress adjourned. They said they could patch it later, but it is a pothole waiting for a truck axle to rumble through.

JIMG [Day 10, 8:55 A.M.]: That's sobering information, RH. Yet I still think that this law, if interpreted the way you suggest, would be found unconstitutional, even by courts dominated by Reagan appointees. Also, the economic cost of prohibiting modems, or even restricting their use, would so outweigh conceivable benefits that the law would never go through. Finally, restricting modems would have no effect on the phreaks but would simply manage to slow everybody else down. If modems are outlawed, only outlaws will have modems.

RH [Day 10, 1:52 P.M.]: We're already past the time when one could wrap hacking in the First Amendment. There's a traditional distinction between words—expressions of opinions, beliefs, and information—and deeds. You can shout "Revolution!" from the rooftops all you want, and the post office will obligingly deliver your recipes for nitroglycerin. But acting on that information exposes you to criminal prosecution. The philosophical problem posed by hacking is that computer programs transcend this distinction: They are pure language that dictates action when read by the device being addressed. In that sense, a program is very different from a novel, a play, or even a recipe: Actions result automatically from the machine reading the words. A computer has no independent moral judgment, no sense of responsibility. Not yet, anyway. As we program and automate more of our lives, we undoubtedly will deal with more laws: limiting what the public can know, restricting devices that can execute certain instructions, and criminalizing the possession of "harmful" programs with "no redeeming social value." Blurring the distinction between language and action, as computer programming does, could eventually undermine the First Amendment or at least force society to limit its application. That's a very high price to pay, even for all the good things that computers make possible.

HOMEBOY [Day 10, 11:03 P.M.]: HACKING IS ART. CRACKING IS REVOLUTION. All else is noise. Cracks in the firmament are by nature threatening. Taking a crowbar to them is revolution. ■