Piracy

THE INTELLECTUAL PROPERTY WARS FROM GUTENBERG TO GATES

*

Adrian Johns

THE UNIVERSITY OF CHICAGO PRESS

Chicago and London

to renew and revivify itself under the Somali dictatorship of Siad Barre. Multiplying sequences of poems, adapting and responding to each other, recreated the flow of oral performances. Somalis took the tapes, recopied them, and passed them on. Listening took place in prescreened groups that formed the basis for opposition cadres.[50] One could go on listing examples indefinitely, from Ireland (the IRA purportedly ran a pirate videotape business at one point) to the USSR. The point is that in so many places different groups saw a piratical potential in the cassette for subverting centralized industry, authority, and culture. It threw together the intimate and small scale with the boundless and the visionary.

That would have lasting consequences. For as teenagers swapped mix-tape compilations in London and poets competed with each other in Africa, in Northern California cassettes were being pressed into service to build a similar kind of community of recording, sharing, and copying. But the content that interested this community was intriguingly different. The first home computer hobbyists took the principles of home copying and applied them to digital data.

16

From Phreaking to Fudding

The word most often associated with piracy at the turn of the twenty-first century was probably *software.* Software piracy, an arcane concept before about 1975, became a ubiquitous one in that generation. In the press it rivaled and then subsumed the lamentations emanating from the entertainment industry about pirated music, movies, and books, as they came to be redefined as subspecies of software. With the growth of the Internet, fears of identity theft, phishing, and the like—culminating in spectacular feats like the pirate multinational NEC—merged with those of piracy proper to make problems of credit and authenticity central to the very constitution of a global "new economy."

By the late 1970s, a fundamental fault line was emerging around digital creativity and intellectual property. Digerati themselves disagreed profoundly about the place of property in the new digital realm, and as that realm became increasingly a networked one those disagreements metastasized. At one extreme, some pioneers urged that intellectual property be built into the very code structuring the networks. At the other, some advocated its abandonment as an anachronistic barrier to creativity and community. These positions cut across conventional political affiliations. As a result, polemics about piracy came to stand as proxies for fundamental convictions about the cultural, social, and technical character of the digital domain. Images of pirates, buccaneers, Robin Hoods, and the like that had permeated expert communities in programming from at least the 1960s now took on a more serious tone as they opened a set of rifts between various proprietary regimes and some nonproprietary ones. The moral and practical realities of the digital realm evolved through the ensuing exchanges.

When contemporaries sought to understand what was happening in this transition, they often appealed to an ethos of antiproprietorial creativity that digital networks supposedly favored. That is, they sketched a cluster of morally consequential "norms" to which true digerati were supposedly committed—norms of sharing, access, and technocracy—and which characterized the emerging culture. The perspective made sense not only because it captured something about the technical properties of digital networks, but also because it evoked a widely believed account of the nature of true science. But that understanding, we have seen, was itself a consequence of mid-twentieth-century conflicts about patenting. Patent strategies in the telecommunications industries in particular had triggered the articulation of this normative account of science, which included a conviction that real research was ultimately incompatible with intellectual property. What is more significant here, however, is that alongside what may loosely be called an ideological inheritance was a practical one. Two closely related kinds of "piratical" interloping had survived the contests of the 1920s–1950s and would now play important roles in shaping the digital revolution. One was unlicensed radio. Amateur ("ham") transmission and reception remained a popular activity throughout the century, and in the 1960s pirate broadcasting enjoyed massive audiences, especially in Europe, for its laissez-faire, libertarian, and antimonopolist messages. The other, however, was older still, and its influence was to be more direct. This practice had originated in the early days of telephony, back in the nineteenth century, only to revive and acquire a new prominence, along with pirate radio, in the sixties. It was called *phreaking*.

PHREAKING

How did the digital world come to be riven between rival conventions of property and responsibility? The answer involves a history extending back beyond the development of digital technology itself, to ideals of science and media that were forged in the days of the radio and telephone trusts.

It also derives from underground practices seen by their proponents as upholding those ideals in the face of industry and monopoly. Take radio. All the principal participants in the making of the home computer either had backgrounds as ham radio aficionados or came from whole families of them (as did Stewart Brand, founder of the first online community, the WELL). Before their experiences at MIT, Stanford, or any of the other canonical sites of the computer revolution, these figures were *already* acculturated into norms of open access, technical meritocracy, libertarianism, and the sharing of information. These were the values bequeathed to amateur and pirate radio from the 1920s–1930s patent fights against AT&T and the radio trust and, in the UK, from those around the BBC, and identified, thanks to those fights, with science itself. It was consequently easy for those early digerati to see the disputes about openness and property that arose in home computing as disputes of a certain kind, for which precedents existed to suggest the stances they should adopt and the actions they should take.

The case of telephony is even clearer. Independent ("pirate") telephony survived, just as independent radio did. In the late 1960s and early 1970s, radicals revived this tradition of expertise. Ripping off Ma Bell took on an added charge for them as a statement of antagonism to the state and to capitalism. Phreaking—telephone network "piracy"—was a way to thumb their nose at the iconic leviathan of corporate America.

Nobody seems to know when the hobby began of gaming AT&T's networks. Its conventionally accepted origin was long placed in the late 1960s, when the term "phreaking" appeared in the press, and others mentioned MIT in the early part of that decade. But the practice certainly has a history a lot longer than that. Even before 1900 teenagers were caught fiddling free calls, and later in Al Capone's Chicago gangs would tweak the phone system to register an illicit bookie's line to some harmless householder. Interviews with leading phreaks in the 1960s revealed that they had learned the habit earlier, sometimes in the mid-1950s—and often in quite uncosmopolitan places too, like Kansas or Mississippi. Britain's Old Bailey had heard a conspiracy trial in 1953 against a London chemical company director who made long-distance calls by tapping the receiver rest. And MIT's phreaking could be tracked back to that decade too, as key Tech phreaks had learned the craft before they ever arrived in Cambridge. In short, the phreaks of the early 1970s were the tip of a historical iceberg. And that is interesting because in the 1950s, 1930s, or 1890s telephone piracy could not possibly have had the political meaning attributed to it in San Francisco in the Vietnam era. Instead, it starts to look much more like the enterprise of exploration that arose around early radio.[1]

Telephone piracy was certainly something portrayed by its practitioners in ethical terms long before 1970. They professed to disdain mere mercenary motives. Instead they proclaimed that they were dedicated to research, and to sharing the insights that resulted from that research. They maintained that the knowledge gained by exploring the network was justification enough for doing so without constraint. That knowledge must, of course, be made openly available—even (and perhaps especially) to AT&T's own staff. Many had a love-hate relationship with AT&T, similar to that which trainspotters cultivate with rail companies. A devotion to technical expertise irrespective of professional affiliation; the intrepid exploration of a network; the discovery of knowledge; the free sharing of discoveries with the priesthood of experts: these were the elements, to coin a phrase, of the phreaker ethic. Doubtless many phreaks stretched the point, simply wanting to place calls gratis. We know that some sold their services to homesick GIs in Vietnam. But their ethical self-portrait was nevertheless impressively consistent and specific.

Two innovations lay behind the popularization of telephone piracy in the 1960s, which seems to be when it first came to be called phreaking. First, AT&T had recently changed to a new long-distance switching technology known as multiple frequency (MF). MF used audible tones at discrete frequencies as an instruction set to tell the network's switches how to channel each call. The tones were transmitted on the same channel as the telephone conversation itself. Knowing their frequencies, it was therefore possible in principle to blaze a trail through the network simply by playing them into a receiver at the right moments. This was what phreaks sought to do. A few could whistle the required notes, but most used an electronic tone generator, perhaps embedded in a "blue box" device. The phreak simply dialed a free 800 number and then sent a tone at 2,600 Hz down the line to trick the exchange into believing that the caller had hung up. "Tandems" (switching devices) in the system emitted this note when they were inactive. Sequences of different tones could then route a call anywhere the network reached—to South America, Asia, Europe, or the Soviet Union. From the mid-sixties cassette tapes became the ideal tool for recording and exchanging these tones, making phreaks into natural allies of home tapers.

The difficulty lay in finding those other frequencies, of course. For years, the only way to discover them was by trial and error, or by asking a more experienced explorer. But in 1960 a house journal of Bell Labs, the *Bell System Technical Journal,* published them in an ill-advised moment of scientific openness.[2] By coincidence, much the same thing happened a little later in the British Post Office's counterpart journal. Alert readers realized that they had found the equivalent of "open sesame." (That there were amateur readers poring over these abstruse journals, incidentally, confirms that a community already existed.) A legend subsequently arose that Bell Labs tried to recall all the copies of the issue. True or not, it was too late. Following the revelation, phreaking grew into a widespread activity.

As it grew, phreaking developed its own pantheon. Perhaps the most admired member was a blind African American, Joe Engressia (who died in 2007 under the name Joybubbles). Engressia had briefly hit the headlines while a student at the University of South Florida, because he had discovered that he could whistle the crucial MF tones into a receiver with perfect pitch, and thereby maneuver through the network without the need for electronic gizmos. He became the focus of countless urban legends, some of which were true (or true-ish). It became a rite of passage for phone explorers all over the United States to place a call to him using their homemade MF devices and cassette recorders. He would put them in touch with each other, and so an underground network grew.

Northern California became a major node for this network under the leadership of an ex-military technician named John Draper. Draper was one of the many who had been involved in radio before he turned to the telephone system. He had been a radar and radio engineer for the air force, stationed in remote Alaska, where free telephoning proved invaluable. After that he had worked at a variety of technology companies, including Cartrivision, the Palo Alto company that had tried to market a videotape device ahead of Sony's Betamax. He also engaged in pirate broadcasting, calling himself San Jose Free Radio.[3] It was because of his pirate radio work that he came into contact with Engressia's phreaks, one of whom heard his signal and got in touch. When it turned out that a plastic whistle distributed free with the breakfast cereal Cap'n Crunch happened to produce exactly the 2,600 Hz tone needed to initiate a phreaking odyssey, Draper adopted the moniker as his *nom de phreak.* As "Cap'n Crunch" he became another legendary presence.

In the early 1970s phone explorers coalesced with a counterculture keen to make ostentatious gestures against the mainstream broadcasting and entertainment industries. The best-known declaration of war was perhaps that by the so-called Air Pirates, a group of San Francisco cartoonists who published skillfully rendered imitations of 1930s cartoons portraying Disney's icon taking drugs and having sex (the corporation pursued them so humorlessly that it provoked a backlash from another outfit calling itself the Mouse Liberation Front).[4] In the same year, Abbie and Anita Hoffman's Youth International Party—the "Yippies"—seized upon phreaking as an ideal tool for a parallel effort. Not only would it help connect fellow Yippies together, they reasoned, but the practice itself suited their ambitions for media. Their point was that underground media must be a commons, with any organ free to reproduce the contents of any other. Hoffman's own guide for would-be revolutionaries, *Steal This Book*—published by "Pirate Editions"—advocated "outlaw" radio and TV stations, which should be linked through (unpaid) telephone lines to form a nationwide "people's network." They would form "the vanguard of the communications revolution." "One pirate picture on the sets in Amerika's living rooms is worth a thousand wasted words."[5] To make this pirate revolution work, experts ("technical freaks") would be needed, and Hoffman recommended that readers find them in the world of amateur radio. He also directed them to *Radical Software,* a periodical emanating from a New York group of artists in the brand-new home-production medium of videotape. Operating oxymoronically as the Center for Decentralized Television, *Radical Software* was heavily influenced by Marshall McLuhan and Buckminster Fuller, and also by Norbert Wiener's antiproprietorial vision of information. The magazine proclaimed in the first lines of its first issue the imperative to universalize access to information, not least by abjuring copyright. It included what it called a "pirated" interview with Fuller, and invented a symbol to represent the "antithesis" of ©. The symbol was a circle containing an *X* (for *Xerox*). It meant "DO copy."[6]

Phreaking thus became a fixture of the counterculture. The Fabulous Furry Freak Brothers experimented with it (fig. 16.1). More than that, it promised to provide a means by which the counterculture might achieve two ends at once: it could counter mainstream media and achieve coherence in its own right. After all, what better way to combat Ma Bell's "improper control of the communication" than by merging phreakdom with the Yippies' characteristic combination of practical jokery and earnestness? Even as *Steal This Book* hit the streets, Hoffman and a New York phreak going by the pseudonym Al Bell began to publish a regular underground journal entitled *The Party Line.* Their intent was to proselytize about "the phone company's part in the war against the poor, the non-white, the non-conformist, and in general, against the people." In practice, each monthly issue was devoted to encouraging the mass adoption of phreaking. It twinned technical notes with screeds, reciting "Corporation ripoffs, establishment fucks, healthful hints, names and addresses of our friends who wish to be known, new services, new devices and plans for them." The journal endured for over a year until it was renamed TAP, for Technological American Party—or, later, Technological Assistance Program, apparently because banks refused to open accounts under the earlier name. It became a principal nexus for phreaks at large and continued to appear into the 1980s.[7]

FIGURE 16.1. The Fabulous Furry Freak Brothers try phreaking. A. Hoffman, *Steal This Book* (New York: Pirate Editions, 1971), 137. Reprinted by permission of Gilbert Shelton.

By about 1971—and in practice well before that—phreaking constituted a self-conscious community that "met" in the virtual space of the network and had global reach. It was, as the anthropologist Christopher Kelty has rd is someone who uses a telephone to talk about telep

said of more recent open-source communities, a "recursive" public, in that it solidified around expert interventions in its own basic infrastructure.[8] The community ostentatiously embraced the claims of the old radio amateurs to openness and knowledge seeking. They aspired to be, and by training often were, practitioners of science. "Like scientists conducting experiments," it was said, "the phone phreaks report results to each other." In Britain, evidence of a similar community surfaced when the Post Office considered adopting a technology akin to that of the Bell system; a public-spirited Cambridge undergraduate cropped up to warn of its vulnerability. It soon turned out that details of the entire British telephone network had been lodged in Cambridge University's mainframe—evidence that these phreaks were computer adepts. In 1973 an Old Bailey judge, faced with a dockful of such reprobates, remarked that the temptation seemed similar to that of heroin addiction. He acquitted the lot, but only after asking them for the access codes to his local exchange. One of the lucky perps—a recent Oxford physics graduate—went home and wrote the episode up for *New Scientist* (fig. 16.2).[9]

The Party Line may have had one unintended consequence that was very significant indeed. That October, phreaks suddenly found themselves in the limelight thanks to an exposé published in *Esquire*. "There is an underground telephone network in this country," the magazine revealed.[10] Journalist Ron Rosenbaum introduced readers to the major contours of the phenomenon, and even interviewed the supposed inventor of the blue box himself—who recalled that he had been "fooling around with phones for several years" before he came across the *BSTJ* at his university, "a well-known technical school." Rosenbaum hinted at connections to Yippie-style political activism, but did not pursue them, noting Cap'n Crunch's anxiety lest he reveal secrets to a "radical underground" that he claimed was on the verge of learning how to freeze the entire U.S. telephone network. The focus was instead on phreaks as explorers. Many of them had apparently come to phreaking from dabbling in radio experimentation. As one put it, "any idiot in the country with a cheap cassette recorder" could blaze a trail anywhere in the world. Phreaks apparently explored the network, discovered knowledge about its properties, and swapped their knowledge (and tapes) with each other. Discoveries, they held, must be shared between those recognized by the group as experts. The phreaks presented themselves as a kind of technical vanguard, liberated from bureaucratic protocols and free to follow where their expertise

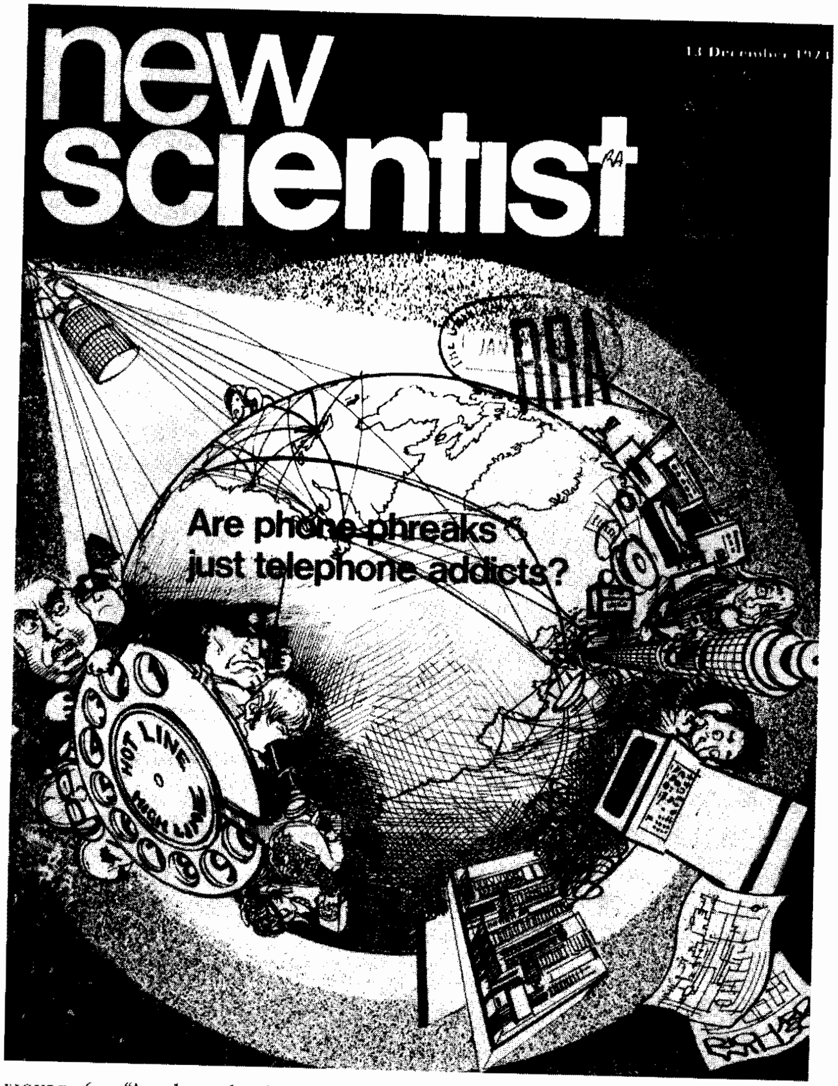

FIGURE 16.2. "Are phone phreaks just telephone addicts?" *New Scientist* 60, no. 876 (December 13, 1973). © *New Scientist* magazine. Reprinted by permission.

led them. They seemed to see their role as akin to that of pop-culture heroes. They would spring up wherever there was a problem, reveal it (and its solution) to the amazed gratitude of the plodding Lestrades of Ma Bell, and then disappear again into their secret identities. They abhorred the system for its conformity, inelegance, and complicity with the government, while at the same time admiring its scale and complexity and wanting to "perfect" it. The attraction lay in solving technical problems—in playing the game—and not a few could envisage acting as anti-phreak detectives, were they to be asked. There was more than a little self-consciousness about such protestations, of course, yet they were impressively consistent.

Now, *Esquire* revealed, the phreaks were headed in a new direction: into the world of computers. Affirming as usual that the mere possibility of making free calls had never interested him, Draper claimed that what *had* attracted him to phreaking was the possibility, dangled before him by the Californian phreaks, that it was a way to contact a computer. By the early seventies he was veering between flat denials that he ever practiced phreaking any more and professions that "if I do anything it's for the pure knowledge of the System." He elaborated: "I do it for one reason and one reason only. I'm learning about a system. The phone company is a System. A computer is a system, do you understand? If I do what I do, it is only to explore a system. Computers, systems, that's my bag. The phone company is nothing but a computer."

Mark Bernay, another pseudonymous phreak, similarly attested that he had "gone beyond" telephony and was now "playing with computers more than playing with phones." He had found himself a programming job, only to be fired for carrying out phreak-like explorations in the company's computer system as the Midnight Stalker. An informer had turned him in (he seemed more upset by the low-tech banality of this than by the fact of being caught). The possibility had briefly been raised that he might be rehired as an investigator of other intruders, but it had been swiftly vetoed, and, Bernay admitted, justifiably so. "My personal thing with computers is just like with phones," he ended by remarking. "The kick is in finding out how to beat the system, how to get at things I'm not supposed to know about, how to do things with the system that I'm not supposed to be able to do."

The crux of the *Esquire* report was that many phreaks were taking this same step. They had found to their delight that they could use the simple computers now appearing on the hobby market to extend their phreaking explorations into new zones. They could dial up other computers, out there in the corporate or even military sphere, and discover a further class of terrae incognitae connected to the Bell network. This extension of phreaking into digital systems was set to be "the wave of the future," Rosenbaum guessed. And the implications if he was right might well be

considerable. The phreaks' philosophy of sharing, access, technical virtuosity, and a buccaneering disregard for rules might do to the computer—still at this point a symbol of high-modern bureaucratic rationality—what it had tried to do to telecommunications in the 1920s–1960s.

Rosenbaum concluded by trying to coin a name for this new level of exploring. He suggested *computer freaking*. The name made sense, because, as he put it, the activity "suits the phone-phreak sensibility perfectly." But it never caught on, for the simple reason that the practice already had a name. It was called hacking.

HACKING

When asked where phreaking had originated, many in the early 1970s suggested that it came from the Massachusetts Institute of Technology. The notion revealed the extent to which hacking and phreaking had already converged, for MIT was well known to be the *fons et origo* of hacking. Yet it also had a basis in fact. Small numbers of students arriving at MIT in the late 1950s and early 1960s had enjoyed phreaking, and they were the same students who originated digital hacking too. They found their intellectual home in the Tech Model Railroad Club (TMRC), which maintained a train set in one of the Institute's buildings. The layout included an extraordinarily elaborate electronic communication system, built from components donated by Western Electric, the manufacturing arm of AT&T. Model locomotives at MIT were therefore controlled by the same switching technologies that the phone phreaks exploited. It did not take these students long to discover that they could explore MIT's own phone network using TMRC techniques. By 1963 a TMRC acolyte named Stewart Nelson (who had experimented with phones and radio in Poughkeepsie before arriving at MIT) had made the obvious next step, using a PDP-1 computer to sing MF tones into the AT&T network. Soon the students had made their way into systems across the nation. Department of Defense contractors were a particular target.[11]

The subsequent trajectory of hacking from Cambridge to Palo Alto and beyond has been well known since Steven Levy's classic *Hackers*. Originally a term for a practical joke of the childish but technically neat kind long popular at places like MIT and Caltech, it now came to mean the virtuoso feats of computer cognoscenti—those who neglected every other aspect of life in order to tweak digital systems to create elegant solutions ("hacks") to tricky problems. At a time when computers were still largely the preserve of specialist technicians, these young virtuosi held a basic commitment to direct "hands-on" experience in order to produce their hacks. Emulating the communities of radio amateurs and phone experimenters, they insisted on the importance of freedom to engage directly with the technology itself. Accessing technologies and sharing the resulting knowledge was in their view essential for technical and even social progress. Moreover, when even the most basic tools—like an assembler—had to be concocted by the group itself, asserting proprietorial authorship made no sense. They upheld the (Wienerian) view that their work should resemble the unimpeded flow of information inside the system. The computer game, Spacewar, that emerged from this conviction has been called the first piece of open-source software.[12]

Hacking took on a different form in Palo Alto. It did so because the Bay Area had a history of its own in radio and telecommunications, which extended back to the AT&T patent conflicts and the culture of radio experimenters. In the 1920s–1930s, local companies there had fought the big East Coast combines. The best-known of them, the Federal Telegraph Corporation, employed amateur radio enthusiasts even before WWI; Lee De Forest developed vacuum tubes there that became central to the broadcasting industry. In the twenties FTC continued to defy the radio trust, recruiting radio amateurs to assist in circumventing patent restrictions while winking at local emulators of its own technology. A Palo Alto industry dedicated to advanced technologies developed alongside it that was antithetical to patent pools.[13] The cluster of research institutions that subsequently emerged in the area drew on this tradition. The three principal sites—Douglas Engelbart's Augmented Human Intellect Research Center, ex-MIT professor John McCarthy's Stanford Artificial Intelligence Laboratory, and, a little later, Xerox's Palo Alto Research Center—embraced an understanding of the computer as another key to a liberating democratization of thinking and acting. The commitment to openness therefore shifted from a technocratic maxim to a democratic one. It became a mode of emancipation at once practical, self-improving, and utopian.[14] Achieving a broad level of access for "the people" to networked computers, under an ideal of democratic research, was more important than the MIT ideal of deep access for a small cadre of technical adepts.

What emerged from that shift in emphasis was a new kind of computer. The "home computer," as it was christened, was as alien and unsettling a thing as the home pirate, and for similar reasons. As in Cambridge, however, a merger of phreaking and hacking was central to defining the new technology. It occurred at a range of extramural and sometimes transient social settings, including various homes, Kepler's bookstore (a place reminiscent of the bookshops and coffeehouses of Restoration London), and a Free University that offered courses on "How to End the IBM Monopoly."[15] In print, there was of course Stewart Brand's *Whole Earth Catalog*, a guide to "tools" useful for readers impatient with the conformities of American consumerism. Launched in 1969, the catalogue touched on an extraordinary range of topics, from cybernetics and communication theories to agriculture and medicine, with an eclectic individualism purportedly inspired by Buckminster Fuller. It grew with successive editions until by 1971 it was almost 450 pages long. Its influence was demonstrated by the People's Computer Company, a project overseen by Brand and Robert Albrecht (whom Ted Nelson hailed as the "caliph of counterculture computerdom"). The PCC was both a publication and an institution. As a publication, it was produced on the same printing equipment as the *Whole Earth Catalog*, using similar pagecraft to proselytize for a cognate message. It even reprinted *Catalog* material verbatim. As an institution, it developed from an older project, "Community Memory," that had deployed public terminals linked to a mainframe, the hope being that they would become both communications devices—pathways by which citizens could establish links with each other—and portals to information. Community Memory had been the project of one Lee Felsenstein, a computer enthusiast with an upbringing full of radio experiments. PCC offered a more concretely social site: a storefront center where people could come in to learn about and use computers, with regular gatherings and events.[16]

The PCC made it a proclaimed principle of its operation that software should be available free to the participant community, and that their further uses of it should also not be constrained. The group's programming language exemplified this conviction. The PCC created a "Tiny BASIC" for the most popular kit computer, the Altair 8800. The language was a "participatory project," announced in the PCC newsletter and published there in full as it developed. Readers sent in their own suggestions and modifications, which were incorporated to improve the code. Soon a photocopied Tiny BASIC newsletter was being circulated to a mailing list of four to five hundred readers. This grew into an authoritative magazine entitled (by its printer) *Dr. Dobb's Journal of Tiny BASIC Calisthenics and Orthodontia,* launched as a vehicle for "the design, development, and distribution of free and low-cost software for the home computer." Like the PCC itself, it was the manifestation in public of a community defined by its sharing of information and code.

Meanwhile, Brand had begun to find the demands of running the *Whole Earth Catalog* wearisome. He decided to end it, and to do so with a bang. He threw a "demise party" for 1,500 guests at the Exploratorium. The event became one of the most storied moments in countercultural and computer history alike. At the height of the party, Brand, cloaked in a black cassock, announced that $20,000 remained in the kitty and invited the attendees to come up with a way to spend the money. There followed hours of argument, by turns utopian, angry, and desultory. The exchanges were still going on inconclusively as dawn broke. The choice seemed to boil down to some kind of communications project—radio or print—or a donation to Native Americans. It was then that a bearded man stood up, introduced himself simply as a "human being," and told them they were all missing the point. His name was Fred Moore. An enthusiast for computers as educational tools, Moore was currently teaching classes at the PCC after a spell of aimlessness in the wake of a prison term for draft resistance. What really mattered was not the money, he now declared, but the sharing of skills and knowledge for the common good. The "union" of partygoers was far more significant than any cash they might distribute. Money actually got in the way—a point Moore drove home by setting fire to a fistful of dollar bills. It was an inspired intervention, although not necessarily in the sense that Moore wanted. The survivors of the party were so impressed that they decided to hand the cash over to him. He suddenly found himself in charge of an unwanted trove that amounted, all told, to some $30,000. Moore took it away and buried it in his back garden.[17]

From then on Moore and a few comrades would meet periodically to lend parcels of this money to worthy projects. Their meetings were long and tortuous—"a kind of verbal *Whole Earth Catalog,*" one participant said. Moore found the process excruciating. He took to circulating missives to his fellows imploring them to show "cooperation and trust." His pleas also posed the question of how best to define property in a new technology such that the rules for their venture might be comprehended—a problem that was becoming more pressing in the PCC itself. As the operation began to divide into two camps—one more interested in advancing technology,

the other dedicated to using computers to empower communities—Moore joined with an engineer named Gordon French in a bid to revive what they recalled of the original sensibility. Moore and French posted notices everywhere they could think of inviting like-minded enthusiasts to what they called an "amateur computer users group—Homebrew computer club . . . you name it." It would be open to anyone who was both interested in building a computer "or some other digital black-magic box" and enthusiastic about sharing information, working together, or "whatever."

The first meeting of the new group, on March 5, was a success. In subsequent months turnout increased by leaps and bounds. Before long more than four hundred people were coming, and the group had to relocate to SLAC's auditorium.[18] Lee Felsenstein—the pioneer of Community Memory—became its unofficial compere. The Homebrew Computer Club, as it was soon called, fast became a principal center for Californian hacking.

For the committed, like Felsenstein, norms of information sharing and hands-on invention were more than just countercultural platitudes. They related rather specifically to the kinds of convictions voiced by Ivan Illich, the one-time Catholic priest whose Centro Intercultural de Documentación in Mexico served to facilitate conversations among skeptics of technological and corporate modernity. Running through Illich's work was a call for individuals to retain creative autonomy in the face of the cultural homogeneity that he believed corporate technologies tended to foster. He wanted to develop an "autonomous and creative" interaction, as he put it, both among people and between people and their surroundings. "Conviviality" of this kind implied living "a life of action," and one full of active creativity rather than receptive consumption. Books, media, and machines were all to be regarded as "tools," not as delivery devices. So society should seek to design and adopt "convivial" technologies. For Illich the telephone network was a prime example of a convivial technology, as long as the charges were low and access free. A still better example was the audiocassette. In Bolivia, Illich lamented, the government had established a television broadcaster at great cost, which reached some seven thousand sets spread among a population of 4 million. The same money could have been used instead to provide cassette recorders to eight hundred thousand citizens, along with blank cassettes and a huge library of recordings. Not only would far more people have benefited, but the resulting generativity

"network" would have been of a radically different, decentralized kind. Input by citizens, literate and illiterate alike, would have been normal. Its principle would have been creativity, not receptivity. That was what it was to be convivial—and in Illich's terms freedom required conviviality.[19] Illich likewise believed that conventional education was receptive and commoditized, and therefore illiberal. He proposed replacing schools by "webs"—computer-based "reticular structures for mutual access"—that would facilitate open-ended and creative interactions. They would resemble enthusiasts' clubs. Some might establish "skill exchanges" at which laypeople could gather to learn about technical tools, perhaps in storefronts. In a city like New York, convivial computing of this kind would permit a culture of reading to be created democratically, rather than on the basis of a "selection by some Chicago professors."

The problem was that modern industry did not produce convivial technologies. It preferred "a world of things that resist insight into their nature." Concealed inside closed boxes—or inscribed in silica—technology was becoming ever less convivial. The prime example was radio. Boxing radios had commoditized know-how, he thought, producing "a non-inventive society." But in its early days radios had been open and convivial, Illich recalled, and a radio enthusiast (what the BBC had called a pirate listener) had often made every set in the neighborhood "scream in feedback." For Illich that howl was a sign of a kind of freedom that had then been widely distributed, had survived for a while in science ("the one forum which functioned like an anarchist's dream"), but was now almost extinguished there too. He wanted to return to the culture it had signaled. In short, Illich proposed that the "the principal source of injustice in our epoch" was not Vietnam, Soviet communism, or South American dictatorships, but "tools that by their very nature restrict to a very few the liberty to use them in an autonomous way." The possibility of establishing a convivial society rested on opening boxed machines to revive the spirit of those pirate listeners. Intellectual property of this kind must be superseded in order to build the "web-like structures" essential for a free society. Illich was not sanguine about the prospects of achieving this—he mused that only Mao's Communists had the clout to do it. But he nevertheless maintained that "while democracy in the United States can survive a victory by Giap, it cannot survive one by ITT."[20]

Illich defined a vision for some early digital pioneers, like Felsenstein. Yet, contrary to much hacker mythology, enthusiasts in the early days were never united in opposing intellectual property per se. Ted Nelson's *Computer Lib/Dream Machines* of 1974, the foremost example of countercultural computer literature, is revealing of the tensions involved—tensions that would end up shaping digital culture itself. A visionary manifesto for the power of engagement with computers, Nelson's book was in one sense a clear articulation of the principle of computer conviviality. It was also, as he put it, a "blatant" imitation of "the wonderful *Whole Earth Catalog.*" Yet at the same time it condemned phone phreaks and copyright radicals alike. "Why is it always the guys with the cushy and secure jobs who tell you tweedle de dee, ideas should be free," Nelson asked. He advocated applying copyright to programs, and advised readers always to append a copyright symbol to their own code. So strongly did Nelson feel on the subject that his Xanadu project—a prophetically grandiose plan for a kind of designed hypertext web—incorporated into its design a form of compulsory licensing. Had Xanadu succeeded, it would have built a particular kind of intellectual property system into the very infrastructure of what became the Internet. It would have solved the network piracy problem by making piracy technically impossible—even while mandating openness at the same time. There was a distinctly Victorian air to the idea. "You publish something, anyone can use it, you always get a royalty automatically," Nelson proclaimed: "Fair."[21]

THE DISINTEGRATION OF CONVIVIALITY

The enduring fame of the Homebrew Club derives from its having been the location where phreaking combined with hacking to create a new kind of computer. All participants were welcome to adopt copies of software or hardware designs, as Felsenstein said, on the condition that they brought back more. One passionate advocate named Dan Sokol would even give out handfuls of new chips at meetings. Software was swapped and shared on cassettes, with similar norms to those of home taping. Later, when the Club developed its own relatively formal library of tapes, it had to create artificial rules covering the proprieties of collection and circulation. "The library is really a software exchange," it advised, and members should not "steal" or copy software protected by copyright.[22] But at first there had been no such commitment. "It was the same as ham radio," Felsenstein revealingly remarked. And Steve Dompier, a Berkeley electrical engineer and close friend of Draper, made that link clear when he utilized the interference an Altair created to play rudimentary music through a radio receiver. When Felsenstein embarked on a project to design and build a computer to suit this environment, he used off-the-shelf parts so that users would not be dependent on particular corporations or sources.[23]

Felsenstein's project was soon overshadowed by another new device —one that, in bringing the convergence of phreaking and hacking to fruition, would also foster the disintegration of conviviality. A Hewlett-Packard engineer named Allen Baum brought along a former school friend and now fellow HP worker, Stephen Wozniak, to an early Homebrew meeting. Wozniak had been a computer and electronics buff since his schooldays, a booster for the ill-fated Cartrivision video system, and a radio ham to boot—an activity that he later described as "protecting the airwaves from radio pirates." In 1971, he had also collaborated with Steven Jobs on a rather different enterprise. *Esquire*'s article about phreaking had caught Wozniak's attention, and they had found in SLAC's library the *BSTJ* article containing the list of MF tones. They built their own devices to produce the tones, recorded them onto cassette tape, and set about exploring the phone network in the spirit of the phreaks. He and Jobs also sold a few black boxes in Berkeley's student dormitories; they were once robbed of one at gunpoint. Wozniak then resolved to track down the mysterious Cap'n Crunch who had described in *Esquire* the appeal of exploring the network in terms of its being a giant computer. Draper took the initiative and introduced himself first. By the time of the Homebrew Club he, like Wozniak and Jobs, had made the transition in earnest. He ostentatiously refused to engage in phreaking, but had become a regular at the PCC. Draper became a fixture at Homebrew too.[24]

oxes

For all that he repudiated phreaking, Draper did help explore the network, not in aid of speech, now, but of data. For example, he helped out an outfit called Call Computer that provided a system allowing people with terminals at home to log into a distant mainframe and communicate with each other. He arranged for the Homebrew Club to have its account on this system. He would also drop more daring hints from time to time about connecting to Arpanet, which had recently been established to provide robust networked communications for the Defense Department. Draper claimed that he could navigate through the telephone system into Arpanet, and thence to MIT's computers, where he could run routines that were too demanding for local machines. Introduced by Wozniak to Sokol, Draper also helped him connect his own computer to the network without contracting enormous phone bills—a moment when the principle of access won out over Draper's reluctance to get involved in something that was sure to get an unsympathetic reception if it were detected. Sokol showed his gratitude by giving Wozniak a boxful of chips and gear suitable to be connected to a Motorola 6800 processor. He took the trove, twinned it with a new MOS 6502 rather than the Motorola chip, and began to build a computer. He would bring the machine to Homebrew to show his progress. He wrote his own version of BASIC for it, which he likewise distributed free at the club; some of its routines were published in *Dr. Dobbs*. As the computer gradually took shape, it became clear that Wozniak's design would be much more powerful than the Altair, and Jobs began to push for selling it commercially. Working frantically, the two of them arrived at a functioning version and put it on the market. They advertised the openness of the design as a distinctive "philosophy," announcing that—unlike Altair—they would continue to "provide software for our machines free or at minimal cost." It was called, of course, the Apple.

Wozniak immediately went to work on a new version, which became the Apple II. Another outcome of extensive Homebrew conversations, the design was immediately recognized as remarkable, and today's cognoscenti still hail it as an archetype of elegant ingenuity. Much of its TV terminal ware originated in a design Wozniak had come up with a year earlier to help Draper hack into Arpanet, however. And some of the video circuitry ultimately derived from his own phreaking box. Not only was the Apple II a cultural emanation of the conjunction of hacking and phreaking, therefore; the machine itself that launched the home computer revolution owed a debt to phreak technologies. Moreover, Draper now became one of Apple's first employees. He was given the task of designing a telephone interface for the hot-selling computer. When he produced something that looked just like a phreak's blue box, however, the young company forthwith scrapped it and dismissed him. Draper went home and continued to experiment, using his own Apple to explore the phone network in search of distant computers. Automating the search, in a few days he logged twenty thousand calls. The telephone company's tracking device sounded the alarm, and the police came to pick him up. Draper thus became the first network hacker ever to be arrested.

As Draper's fate implies, the norms of openness, access, and engagement were coming under intense pressure as microcomputing boomed.

More participants at Homebrew now saw its conventions not as moral principles in their own right, but as means to an end. They treated the club as a proving ground for what would ultimately be commercial ventures, aimed at a mass audience that was envisaged as meekly receptive. The Apple II design was not hostile to interventions by users—Wozniak had been careful to include expansion slots—but neither did it invite them, let alone require them in the way that earlier machines had. It came as a complete system, with BASIC in ROM. Radically opposed ways of proceeding now began to resolve themselves. One was friendlier to nonexperts, and ultimately proprietorial. Apple took this route, and Commodore would take it further with its PET. The other maintained the principled commitment to conviviality—to openness and tweaking. Felsenstein's machine, named the Sol, exemplified this. Its design, a refinement of Felsenstein's earlier public terminals, embodied the convictions of popular radio experiment and the *Whole Earth Catalog*. The success of Apple (and soon of Microsoft) made the second path all the more problematic. A parting of the two ways was imminent. Moore departed in 1975 as entrepreneurial pressures grew, and the Sol became first a niche machine and then an outright failure.[25]

in II+

The existence of an alternative had become clear only three months after Homebrew began meeting regularly. The manufacturer of the Altair, MITS, held a publicity show for the machine in Palo Alto. Hobbyists had begun to grumble at the slow pace of improvements to the Altair design, and Homebrew aficionados were increasingly inclined to see MITS as monopolistic and secretive. Some had already paid for a BASIC that had not shipped, and others complained that MITS was tying the program to sales of memory boards that they said did not work, allegedly in a bid to crush Felsenstein's independent effort. Being asked to pay money for bad technology was a cardinal offense, especially when it involved a notoriously monopolistic tying strategy—and all the more when enthusiasts could get a workable BASIC from the PCC for $5. When the MITS crew arrived at a Palo Alto hotel in June 1975, then, several Homebrewers were surprised to find there what seemed to be a working version of BASIC. One enterprising individual—it has never been clear who—noticed a paper-tape copy of the program and "borrowed" it. It found its way into the hands of Sokol, perhaps the staunchest advocate of openness of all, especially when, as he believed was the case here, software had originated in public research. Sokol made more than seventy copies overnight and brought them to the next Homebrew meeting. A feeding frenzy ensued. The code immediately became part of the Homebrew moral economy, in which borrowing one copy was fine as long as one returned two. The problem was that unlike most code that circulated in this way, the BASIC was proprietary. It was the first product from a small company based in Albuquerque, named Micro-Soft.

The BASIC had been a rush job. When William Gates and Paul Allen had brought their raw creation to MITS—by this point desperately in need of a BASIC—they had not even had a chance to make sure it worked. But it had, well enough for MITS to sign up for it and offer a royalty. Gates, twenty, had then more or less dropped out of Harvard to pursue the opportunity. But royalty income had proved far lower than he had anticipated. In fact, MITS seemed to be selling only one copy of Micro-Soft's BASIC for every ten Altairs. It was therefore in a context of crisis that Gates got word that the language had been distributed throughout the very community that ought to have furnished his market. When the editor of a newly formed *Altair Users' Newsletter* asked for his reaction, Gates decided to respond aggressively. He published an open letter to hobbyists that assailed not just the particular perpetrators of the "theft" (as he called it), but, in sweeping terms, the culture that endorsed such actions. Its premise was that a vast potential "market" for microcomputing was being stymied by a lack of good, reliable software, along with the documentation and education that would enable users to make the most of it, and that only a proprietary regime could justify the substantial investments needed to produce those things. Gates claimed that his own BASIC had taken a year and $40,000 of computer time to create, with results the quality of which correspondence from users amply confirmed. But those users had not played their part by actually buying the program. "Most of you steal your software," Gates bluntly accused. What they saw as openness and collaboration was now "theft" pure and simple. Far from being justified by MITS's monopolistic behavior, it was itself a moral offense. It was simply not "fair." Rerecorders of programs gave all hobbyists a bad name, Gates insisted; they should be "kicked out of any club meeting they show up at." The possibility that conviviality might be a principled position was silently trumped by an assertion of this distinct moral community. That a unified authorial body (be it a single writer or a company) and a centralized, industrial system of production were essential to produce "quality" software was implicit and necessary to Gates's case. It was this author that the act of sharing was unfair to, and this system that must be created to allow home computing to thrive.[26]

Gates's letter inaugurated a mini-campaign on Micro-Soft's part, with a successor declaration issued a few months later, and a speech that he gave in March. The effort was never likely to achieve much by itself, however. As Dompier remarked, "complaining about piracy didn't stop anything," because sharing software was "like taping music off the air."[27] Gates himself tacitly conceded as much: he made sure to insulate his company from practices of this kind by signing no more royalty deals. But the publicity served its greater purpose. It made explicit the tensions already present in hobbyists' conventions, and forced recognition of the economic implications of the hobbyists' moral economy. The *Homebrew Computer Club Newsletter* voiced qualified approval of his position, for example, even though it prefaced its own printing of the letter by reminding readers that with the PCC's version "you can homebrew your own BASIC." Yet the more committed still gave Gates a hostile reception. Many were convinced that the BASIC they were sharing was in truth a public good anyway, having been developed on publicly funded machines. It was not just that Gates had called them thieves, therefore, but that an expropriator of common property had called *theirs* a morality of theft. Gates's statement would go down in computer lore as the canonical declaration of a rift over intellectual property and access that would divide the digital world from then on.

FEAR AND LOATHING ON THE NET

Out of the early years of home computing emerged rival approaches to creative property, including those that decreed its outright rejection. Some were aboveboard and would prove themselves as viable modes of creativity. Others were underground, but they too have proved lasting. What made this possible was not the advent of the personal computer, but the later arrival of affordable and reliable digital networking.[28] By the mid-1980s, home computer enthusiasts could buy not only an IBM PC, Apple, or other micro, but also a telephone modem to go with it, and they could connect to the first bulletin boards and networks. Rates of data flow were tortoise-like by today's standards, but they were sufficient for text-only work. Information could be exchanged, and, it was increasingly claimed, communities built. By the mid-1990s, awareness of a single

Internet—descended from the Arpanet that had so fascinated Draper—was becoming widespread. The first browsers were arriving to engage with a graphical World Wide Web. The different approaches to property became more entrenched and the opposition between them, if anything, more emphatic. In the process, a link between credit and property that had been forged in the eighteenth century was finally broken.

Indeed, the situation confronting early Net users was reminiscent of that facing authors and booksellers in the eighteenth century itself. Claims about the sacredness of authorship and a new age of reason had been loud and legion then too. Pirates had been attacked for offenses that ranged beyond literal theft and impugned credit, fidelity, and authenticity. Practices comparable to what are now termed identity theft or phishing (the imitation of institutions) were rampant. Printed communication was hailed as emancipatory, rational, and enlightened in principle, but in practice seemed riddled with problems. Any community claiming to be constituted by print—such as the public sphere—had to tackle such problems if it was itself to be credible. To solve them required not just laws and philosophies, moreover, but street-level nous. As Kant implied, piracy threatened the basic possibility of public reason by perpetrating a kind of ventriloquism. Similarly broad and deep claims were made about the new digital realm of the 1990s. The existence and nature of online collectivities became topics of hot debate. The reality, extent, and epistemic implications of piratical practices were held up as not only challenges to intellectual property—though those challenges were widely declared to be fundamental—but as threats to the possibility of a rational online public. The need to articulate the moral economy of digital networks became acute.

The best known of the early networked communities was the Whole Earth 'Lectronic Link, or WELL, a Sausalito group cofounded by Stewart Brand. Before long other online collectives—Usenet, MUDs, MOOs, and the like—were multiplying. The earliest BBS (bulletin board system) was older, having been created by two Chicagoans in the late 1970s as a substitute for swapping cassettes. Some of these groups, like the WELL, were fairly small and localized; others were larger and adopted fictional locations, leading at length to ventures like *Second Life*.[29] It did not take users long to testify that they felt themselves approaching the McLuhanite dream of having the psyche merge into a global electronic net. More influential language for articulating online communities, however, evoked concepts of community and frontier. Their principal exponent, Howard Rheingold, was a WELL veteran who came up with the expression "virtual community" in 1987 in a successor volume to the *Whole Earth Catalog.* Rheingold's representation of an emergent frontier domain—at once a village full of diverse skills, bound together by an "informal, unwritten social contract," and an unsettled landscape of new stakes and homesteads—became probably the most widely adopted model for these pseudo-societies. A prime principle was that members should act like digital versions of barn-raising Amish, sharing information in order to help each other build their online homesteads. But this principle, Rheingold warned, would be sorely pressed by corporations as they took up the rhetoric of online communities to sell themselves. Corporate sites tried to persuade customers that they were engaging in a "community" when all they were really doing was receiving company messages. A true community demanded that its members *work* to cling to the ideal of creativity rather than receptivity—an eminently Miltonic stance, one might say. A "battle for the shape of the Net" was apparently about to ensue.

In that looming struggle another enemy also threatened. If the WELL was one adaptation of the convivial ideals of the seventies, a hacker underground represented another, less respectable adaptation. Its roots lay more with the radical phreaks of Hoffman's ilk—as Bruce Sterling put it, *Steal This Book* had become the "spiritual ancestor of a computer virus."[30] Although much hyped by the press, the black-hat hacker crowd was real and numerous. A BBS to champion it was launched as early as 1980; it went by the name 8BBS and was dedicated at first to phone phreaking. By the mid-1980s, such boards had proliferated, often taking on explicit piratical identities: Pirate-80, Pirate's Harbor, and Pirates of Puget Sound were three among dozens, perhaps hundreds, of BBSs devoted to this scene. They issued pirated code and tips about phone phreaking cheek by jowl. The curious could trawl through these sites for phreak codes, which then became tokens of exchange warranting entry into various groups, much as arcane alchemical recipes had acted as passports to philosophical clubs in the mid-seventeenth century. Contacts could be made through these actual pirate and phreak groups via the BBSs. Some of the sites even acquired public notoriety—none more so than the Legion of Doom, which was named after the old gang led by Superman's foe, Lex Luthor. Originally a gathering of phone phreaks, like many of the online cracker groups, the Legion of Doom moved from phreaking into hacking. Like most of

them, it affected the techno-elitist libertarianism and the language of exploration that had been such a feature of phreaking. It even affected the same lexical tics, in particular the ubiquitous *ph.* Above all, Legion of Doom hackers and like-minded digerati appropriated wholesale the phreaks' presumptuous claim—itself descended from interwar radio culture—that as practitioners of the scientific method they should be supported, not restrained. A much-reissued posting of 1986 variously titled "Conscience of a Hacker" or "The Hacker's Manifesto" declared all this explicitly. It was the work of a Legion of Doom hacker named The Mentor. Hackers were firstly explorers of a telephone system, it claimed—a system that ought to be cheap for all, but had been hijacked by "profiteering gluttons." Hence hackers were resistance fighters. But at the same time they were scientists. The Mentor laid claim to the persona of the lone researcher persecuted by an uncomprehending and conformist society. "We explore," he insisted: "We seek after knowledge . . . and you call us criminals."[31] And he had a point. When the police moved against the Legion, they found that its members had generally not stolen anything. Even the more serious pirates to whom the Legion did lead them turned out to have circulated copies of commercial software for free.

As more and more phreaks found each other online, so a digital counter-public came to constitute itself. Hackers developed a number of flamboyantly libertarian periodicals aimed at the knowing. The best known were *Phrack* (a conjunction of *phreak* and *hack,* launched in 1985) and *2600* (named for the fundamental phreaking tone, and proud to claim a pirate identity, as shown in fig. 16.3). The latter was edited by a then-mysterious individual calling himself Emmanuel Goldstein, after the Trotsky figure invoked in the hate rallies of Orwell's *Nineteen Eighty-Four.* His real name was Eric Corley, and he had long been involved in amateur radio. There was even a *Legion of Doom Technical Journal,* parodying the old *Bell System Technical Journal* that had opened the door to the whole phreaking phenomenon. These journals comprised "philes"—independent submissions—more than conventional articles. Today, a generation later, they make fascinating reading. Through the mid-1980s they tracked the convergence of phreaking, coding, and piracy into a single enterprise, captured popularly—but incorrectly, many insisted—by the term "hacking."[32]

By the end of the 1980s the received meaning of the term *hacker* had therefore shifted. It now referred to what digerati distinguished as a *cracker* or "black-hat" hacker—someone who stealthily intruded into online

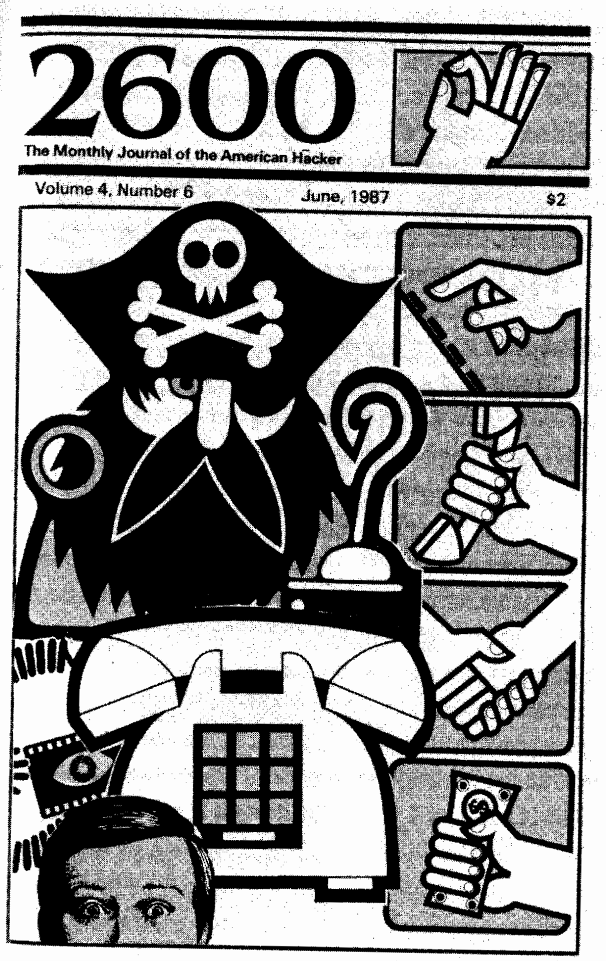

FIGURE 16.3. Piracy, phreaking, and hacking. *2600* 4, no. 6 (June 1987), cover. Reprinted by permission of *2600*.

computer systems for mischievous ends. When hacking in this demi-monde sense became a focus of serious police and public attention, it was by virtue of its identification with phreaking. In 1989 a probation office in Florida found its calls being rerouted to a phone-sex line in New York. The telephone company investigated, and found that hackers had been not just phreaking its lines, but, in doing so, reprogramming its digital systems. At much the same time, Clifford Stoll's *The Cuckoo's Egg* told the story of a KGB-inspired phreaking/hacking espionage ring. And the first large-scale online virus (technically, a worm) affected some six thousand networked computers. As they proliferated across the media, such episodes galvanized fears about the vulnerability of online information generally. More specifically, they stoked concerns about the amoral character of technically expert groups able to manipulate such systems.[33] Rumors began to fly that the Legion of Doom intended to crash the entire telephone system—that old threat hinted at by Draper long before. When the long-distance network did crash on the following Martin Luther King Day, a hacker attack was immediately suspected, although in fact it turned out to be a fault in the system. New laws and police actions multiplied against a projected threat by criminal or even seditious hackerdom.

This caused considerable soul searching among proponents of online sociability. In the late 1980s and early 1990s repeated debates took place about the implications for digital communities, and about the responsibilities that digital expertise carried with it. They focused on what became the vexed question of the day: whether there was a hacker "ethic." A direct adoption from Merton's portrait of science, the contention that there was such an ethic took its rise from Levy's *Hackers,* which was overtly premised on the idea. But the point of the exchanges that now ensued was to determine whether the norms of such an ethic—assuming it existed—were consequential. Scientists, on a Mertonian account, were not particularly virtuous as individuals, but their work was shaped by moral norms that were upheld and enforced by the scientific community at large. Did something like this hold for hacking? If so, could it be exploited to sustain digital community?

The best-known exchange on these lines was a "conference" held in the WELL in 1989 under the aegis of *Harper's Magazine.*[34] Its immediate trigger was the panic over the first widely distributed worm but the exchange had time to develop broader themes, with participants arguing, changing their minds, and at length diverging irreconcilably. They included a number of veterans, Lee Felsenstein among them. Richard Stallman took part from MIT. Emmanuel Goldstein and two crackers going by the monikers Acid Phreak and Phiber Optik also contributed. The initial subject was the hacker ethic itself, which they variously construed, credited, and disdained. Most accepted that hacking was characterized by contempt for obstacles to technical progress. That was what lay behind its commitment to the free exchange of information, and hence its repudiation of intellectual property. Hackers appeared antiauthoritarian because they claimed the right and ability to "undam the pipes" and allow information to flow freely—a very Wienerian image. "Everything that was once said about 'phone phreaks' can be said about them too," observed one participant. Hacking was reliant on the home, added another, because without privacy it could not exist—a contention suggestive in turn of Kantian ideals of Enlightenment. Nonsense, declared Goldstein: "we're just individuals out exploring." In the end, taking such speculations to an extreme, a few speakers elevated hacking into a supercultural category. It was simply inventive creativity in general, particularly that which involved redeploying existing machines to new uses. Its inventor had been the prehistoric cave dweller who first "hacked" fire. On this basis one participant suggested that the commitment to shared knowledge might represent a primordial human desire for connection. "That's hacking to me," concluded Felsenstein, transfiguring the practice in a different way: "to transcend custom and to engage in creativity for its own sake."

But if hackers were creators, what limits and responsibilities should they acknowledge? This was a major question, with real and substantial political implications. "There's nothing wrong with breaking security," Stallman proposed, "if you're accomplishing something useful." And perhaps crackers *were* doing useful service. The real problem, some suggested, was that institutions and corporations were quietly collecting data on citizens without their awareness or consent, and then treating the data as their own property. In that context, hacking into databases was a moral obligation—it was the only way to reveal a greater problem. Media hysteria notwithstanding, after all, crackers rarely went after private households. "Hackers have become scapegoats," Goldstein charged. "We discover the gaping holes in the system and then get blamed for the flaws." The real expropriation took place long before any hacking was done, and the only way to reveal it was to break rules. "I know I'm doing the right thing," he declared, "on behalf of others who don't have my abilities." In other words, an Internet invasion might be a "manifesto" of public empowerment.

This provoked the disintegration of the colloquy. Clifford Stoll, the exposer of the espionage ring, asked drily whether there had once been a "vandal's ethic." His point was that electronic neighborhoods were "built on trust," as real ones were. Hackers eroded that foundation. No community could survive their "spreading viruses, pirating software, and destroying people's work." A contributor calling himself Homeboy went further still. "Are crackers really working for the free flow of information," he asked, "or were they in effect "unpaid tools of the establishment?" At this point, eight days into the conference, John Barlow (author of the *Declaration of the Independence of Cyberspace*) suddenly denied point-blank that a system's flaws could justify hacking into it. A rapid escalation of insults ensued, until Phiber Optik interrupted the flow by posting Barlow's own credit history online. "If you didn't know that they kept such files," he demanded, "who would have found out if it wasn't for a hacker?" Professedly intended to show the civic necessity of piratical hacking, the gesture dramatically refuted itself by bringing the conversation to a grinding halt.

Felsenstein summed up the outcome in a spirit of exasperation. "If you hack, what you do is inherently political," he admonished—but hacking alone, pursued without real political interventions, was futile. The most notable attempt to provide a normative account of digital piracy as a form of scientific citizenship concluded on this dispiritingly realistic note. Without real-world social coordination, a hacker was merely a wannabe "techno-bandit."[35]

FUDDING

The transformation of hackers from anarchic geniuses into criminals and terrorists (language that was leveled even in the WELL) coincided with the rise to dominance of proprietorial approaches in a networked digital economy aspiring to global reach. Issues of trust, access, and security were of central importance to both. As in the eighteenth century, those who could create and sustain trust in a piratical environment stood to win. There were opportunities in this. Hackers could claim to be public agents. The corporate world, meanwhile, could make money by touting "trusted systems" and deploying claims about security. Another part of that world could develop businesses of prevention, detection, and policing. And at the same time, alternatives to proprietorial software proliferated, staking their own moral and economic claims. Richard Stallman at MIT became their best-known and most forthright advocate. Stallman held that the creation and circulation of "free" software—that is, code independent of proprietary restrictions—was a matter of the constitution of communities. He complained that in the digital realm exclusive properties made "pirates" out of what otherwise would be merely good, helpful neighbors. That is, the question of property was, as always, a matter of political philosophy, with the "pirate" label indicating that this was the modern counterpart to debates about perpetual rights and freedom of speech in the Enlightenment. Stallman's was quite a radical position, however, and commercial and would-be commercial allies grew leery of it. In 1998 they came up with the alternative designation "open source." Open-source software was not quite the same thing as free software, because open-source denizens could countenance the integration of code into subsequent products distributed on a proprietary model.[36] But the two did share the ideal of the programmer as citizen and craftsperson, and they would often be paired together under the acronym FOSS (for free and open-source software).

Proprietary software concerns struggled to come up with a strategy to deal with open-source work. Some, IBM being the most prominent, reconciled with open source. Microsoft did not, and as it rose to dominance it struggled to appreciate the nature of the challenge. A remarkable revelation of its strategic perceptions came in the fall of 1998, by which time open source had proved itself a lasting enterprise. That October, an internal memorandum was leaked to the open-source proponent Eric Raymond. It had been written by a Microsoft official named Vinod Valloppillil, and bore the title *Open Source Software: A (New?) Development Methodology?* A second document appeared shortly after, with more following in later months.[37] Together, these "Halloween documents," as they became known, demonstrated that (contrary to Microsoft's public stance at the time) the corporation saw open-source conventions as posing a serious challenge. More significant, however, was what they revealed about Microsoft's efforts to articulate the nature of that challenge and respond to it.

Open source, the initial memorandum conceded, had advantages "not replicable with our current licensing model." It therefore presented "a long term developer mindshare threat." Contrary to what was then Microsoft's public stance, large projects drawing upon communities of expertise extending across continents had already demonstrated the viability of FOSS, and robust legal mechanisms such as the GNU Public License were sufficient to sustain them. "Very dramatic evidence" existed already indicating that the quality of open-source software equaled or exceeded that of proprietary. Not least, the Internet operated largely atop open-source code. In short, open source had the all-important asset: "credibility." Valloppillil reasoned, therefore, that Microsoft was in the difficult position of having to "target" not a specific competitor, but

a "process," and one that had earned the trust it enjoyed. He considered buying a solution: Microsoft could simply monitor open source discussion groups and hire all the outstanding coders (AT&T's old prewar strategy in telecommunications). But that was less a satisfactory response than a backhanded compliment to the virtues of FOSS. His real proposal was more radical.

Valloppillil mooted a strategy of "de-commoditizing" the standards by which commonly used programs interacted with each other. These standards (good examples would be the TCP/IP protocol used in Internet communications, or the various compression algorithms used for audio and video files) were—and remain—basic infrastructure for the digital world. The common perception that digital culture is *intrinsically* universal rests on their being *in practice* shared across manufacturers and nations. The Halloween strategy against FOSS would be for Microsoft to generate its own protocols that could be sold as better than any current standard, and to encourage programmers to write to them. This would inevitably render the standard nugatory, and thus make it very difficult for authors to produce code that would run predictably across different systems. Open source's vital asset of credibility would attenuate quickly in that situation. It was a plausible proposal, and in fact Microsoft adopted a similar strategy to combat the potential of Java to supplant desktop with web computing. When the Halloween documents were revealed, open-source advocates assailed the idea as devious, Machiavellian, and technologically corrosive. The outcry was so fierce that Microsoft found itself forced to disown it.[38]

A more interesting contention about credibility, however, went relatively unnoticed amid this furor. The Halloween memo rested on a distinction between experienced programmers and users. A few experts might feel more secure with access to source code, it conceded. But the laity might well prefer what it called "the trust model + organizational credibility"—and rationally so. That is, the vast mass of lay users would probably vest their trust in not the code itself (which was inaccessible to them whether "open" or not) but the institution that authored and vouched for it. If Microsoft documented that an API (an interchange protocol between programs) acted in a certain way, then few would doubt that it did. Even an expert would reasonably credit a corporate author rather than exert an impractical prerogative to check every subroutine. Writ large, trust in the corporation might well supplant a supposed ability to vet code for oneself. Individual expertise could almost never stand against collective in practice. The point depended, of course, on open source being seen as a mass of individuals rather than an institution in its own right—but that played precisely to its advocates' own libertarian self-image. In effect, the argument confronted the open-source community's championing of democratic access with the contention that trust, as much as individual knowledge, was the more fundamental basis of social and epistemic order, even in technical communities.[39] Raymond suspected that the contention was flawed—only managers relied on "trust," he maintained, while real developers preferred access. But he conceded that this was a strategy by which Microsoft might actually win.

Significantly, however, although Valloppillil's proposal made the competition over credibility into one recognizable in terms of prior computer-industry experience, it acknowledged that Microsoft could *not* win simply by dusting off and reusing tactics familiar from previous generations. The most traditionally insidious strategy in the industry was that known as *fudding*. The acronym FUD ("fear, uncertainty, and doubt") had originally been coined in the sixties apropos of a practice of the old monolith, IBM. It referred to the craft of insinuating suspicions about the longevity, security, and reliability of an opponent's software in order to deter the laity from buying it. The idea was that middle managers would prefer not to take risks in software purchasing, so that if they perceived uncertainties then they would opt for the security of a known program rather than buying a perhaps better alternative. The power of the strategy rested on a link between authorship and credibility that had been forged over centuries of piracy debates. Moreover, it ought to be more effective than ever now, as piracy and cracking encouraged a belief that the Net was a risky, uncertain place. And indeed, fudding was widely recognized to be a pervasive tactic in the Internet's early years. It represented the Net as a viper's nest.

But it turned out that open source was better at resisting snakebites. What the Halloween documents really showed, in the end, was that open source had broken the lockstep between credibility and authorship. Distributed creativity defied an identification that had prevailed since piracy conflicts had forged it in the early Enlightenment. In fact, open-source programs were not only less vulnerable to viruses than Microsoft's, but faster to react to them. If delocalized authorship meant resilience and adaptability, as it now seemed to do, then the very fear that fudding

conjured up might work *against* proprietary authors, even those as huge as Microsoft. Strong intellectual property in this realm created uncertainty of its own. Fudding was therefore suddenly futile at best. By the same token, the moment when open source proved itself was the moment when its biggest opponent recognized that the basis of credibility had shifted in this fundamental way. That was why the Halloween document had to consider resorting to an apocalyptic strategy of undermining the very infrastructure of digital networks. Only by challenging technical standards could authorship and credit be secured together again.

Aware of the threat, Raymond urged that open-source proponents respond by developing "trust" protocols of their own. They could not rely on openness itself. Instead, they would have to develop a culture of named authors of credit, or "publishers of good repute" like O'Reilly or Addison-Wesley in the world of print (implicitly, that of scientific print). This culture, he surmised, might "substitute for 'trust' in an API-defining organization." The resemblance of this strategy to criteria of trust that were proposed in earlier, predigital eras was remarkable. A digital world might not be so revolutionary after all: the battlefront would once again be between candidates for credibility in a piratical field.

In sum, the origins of the digital culture we now inhabit—the culture in which piracy is the defining transgression—were shaped by questions of creativity and community, and those questions were cast at the critical moment in terms of an ethos. That this was so was an outcome of the mid-century debates about telecommunications, patent monopolies, and the nature of science. Thanks to the practices from which those debates arose, the domestication of creativity was already valorized and set against a conformist, corporate world of "media" long before digital hacking arose. More specifically, the practices out of which hacking did emerge were those of radio, telephone, and home piracy. Many among the early digerati were committed to libertarian ideals they found originally in pirate or ham radio. Phreaking formed a practical bridge between telephone exploration, on the one hand, and digital exploration, on the other. And the first home computer enthusiasts adopted both the cassette technology and the convivial customs of the home tapers. The effects were manifold, but issues of credit—of trust, authorship, and authenticity—were central to them. For example, expertise no longer went with professional identity. It was once again radically unstable, and peer opinions, abstracted from place and affiliation, were said to be the only guide to its true location. Where to find authoritative opinions, however, and how to tell them from the spurious, were of course pressing problems.

The corporate world tried to exploit these questions in various ways, of which fudding was one. Fud played on the uncertainties of (business) users to encourage a safety-first reversion to the association between authorship and credibility. It worked for a while, but seemed likely to fail against the distributed form of authorship that had arisen out of those mid-century pirate principles and established itself over the Net. Open source enjoyed "long-term credibility" because publics understood it to carry less likelihood of instability, lower vulnerability to attacks, and less chance of being cast adrift in the future. The ground had shifted—not just because of technological change, but because of deep-rooted cultural convictions that affected how new technological possibilities were exploited.

One suggested response to this rather radical change was to move to a strategy based on another central element in modern science and technology: standards. The idea was to treat standards not as things to which to conform, but as things to exceed. Had it been pursued, this would have undermined the uniformity of digital networks. That is, it would have endangered the very property that is often taken to be the intrinsic, defining virtue of the Internet, permitting its global reach. It would have done so in order to reassert a tie between authorship and credibility. That tie seemed by now to be the axiom of good order in creativity and commerce. How to reconcile it with the powers of the Internet remains a central question of our time.

17

Past, Present, and Future

Daniel Defoe created the first classification of intellectual piracy almost exactly three centuries ago. He sorted it into a handful of simple categories like abridgment, epitomizing, and reprinting in smaller fonts.[1] Today any corresponding taxonomy would extend to a vast array of sins—phishing, identity theft, biopiracy, seed piracy, and so on. It would surely baffle even someone as worldly as Defoe. Because more things fall under the aegis of intellectual property today than ever before—including recordings, algorithms, digital creations, genes, and even living organisms—practices that until relatively recently would not have seemed even potentially piratical may now be deemed actually so. Meanwhile, as the information economy has grown, so it seems that piracy has metastasized beyond anyone's ability to understand and master it. Some of its species are industries in their own right. In political and economic rhetoric the accusation of piracy has become the indictment of the age, and a ubiquitous element in the framing of national and international trade politics.[2]

The story of piracy has two major implications in this context. The first derives from the point that intellectual property exists only insofar as it is recognized, defended, and acted upon. That is, it is a practical matter. It takes shape not only through the stipulation of laws and treaties, but also through the actions societies take to put those laws and treaties into effect in homes, offices, factories, and colleges. Challenges demand

August 19, 1983, A23; Lardner, *Fast Forward,* 233–34; J. Lardner, "Video Wars," *Washington Post,* May 2, 1982, F1; Lardner, "Tales of a VCR User," *Washington Post,* June 16, 1982, D1.

39 P. F. Drucker, "Japan's Choices," *Foreign Affairs* 65, no. 5 (Summer 1987): 923–24; C. Johnson, *MITI and the Japanese Miracle: The Growth of Industrial Policy, 1925–1975* (Stanford, Calif.: Stanford University Press, 1982), 313–14.; M. Crichton, *Rising Sun* (New York: Knopf, 1992); G. Friedman and M. Lebard, *The Coming War with Japan* (New York: St. Martin's Press, 1991); P. Choate, *Agents of Influence* (New York: Alfred A. Knopf, 1990); R. Kearns, *Zaibatsu America: How Japanese Firms Are Colonizing Vital U.S. Industries* (New York: Free Press, 1992). The definitive rebuttal of the whole genre is *Economist* editor Bill Emmott's *Japanophobia: The Myth of the Invincible Japanese* (New York: Times Books, 1993).

40 C. Sims, "Wounded by Patent Piracy," *New York Times,* May 13, 1987, D1.

41 Kearns, *Zaibatsu America,* 15–23; Y. Miwa and J. M. Ramseyer, *The Fable of the Keiretsu: Urban Legends of the Japanese Economy* (Chicago: University of Chicago Press, 2006), 54–58.

42 C. V. Prestowitz, *Trading Places: How We Allowed Japan to Take the Lead* (New York: Basic, 1988), 206–7, 214; Lardner, *Fast Forward,* 238, 260.

43 "Sony's Morita Bashes Back," *Business Week,* October 16, 1989, 58; S. Wagstyl, "Chief of Sony Tells Why It Bought a Part of America's Soul," *Financial Times* October 4, 1989, 4.

44 *Congressional Record,* H8486-7; E3783-98 (November 13–14, 1989); E3952-2 (November 17, 1989); *New York Times,* August 4, 1989, A7; F. Lewis, "Japan's Looking glass," *New York Times,* November 8, 1989, A31; "Shintaro Gephardt," *Wall Street Journal,* November 14, 1989, A22. For the Japanese context, see M. F. Low, "The Japan That Can Say No: The Rise of Techno-Nationalism and Its Impact on Technological Change," in *Technological Change: Methods and Themes in the History of Technology,* ed. R. Fox (Amsterdam: OPA/Harwood, 1996), 210–24.

45 N. Wade, "America's Japan Problem," *New York Times,* October 5, 1989, A30; L. Summers, "Tough Talk from Tokyo: What to Do When Japan Says No," *New York Times,* December 3, 1989, A2; C. H. Farnsworth, "Japanese Author Brushes Up His Image with Journey to U.S. Enemy's Lair," *New York Times,* January 29, 1990, A16.

46 S. Ishihara, *The Japan That Can Say No,* trans. F. Baldwin (New York: Simon and Schuster, 1991), 8–12, 141, 145; *New York Times,* January 18, 1990, D8.

47 H. S. Becker, *Art Worlds* (Berkeley: University of California Press, 1982).

48 G. Davies, *Piracy of Phonograms,* 2nd ed. (Oxford: ESC Publishing, for European Commission, 1986), 7–8, 12–13, 16, 33–35; R. Wallace, "Crisis? What Crisis?" *Rolling Stone* 318 (May 29, 1980): 17, 28, 30–31; G. Davies (for IFPI), *The Private Copying of Phonograms and Videograms* (Strasbourg: Council of Europe, 1984), 17–18, 22–23, 34.

49 P. Manuel, *Cassette Culture: Popular Music and Technology in Northern India* (Chicago: University of Chicago Press, 1993), 65, 67–69, 79, 83, 85–88, 148–49. I am grateful to Ravi Sundaram of the Sarai project in Delhi for a presentation entitled "The Copy Itself" that he gave at the University of Chicago in early 2007. In print, see his "Uncanny Networks: Pirate and Urban in the New Globalisation in India," *Economic and Political Weekly,* January 6, 2004.

50 M. Foucault, "The Revolt in Iran Spreads on Cassette Tapes," in J. Afary and K. B. Anderson, *Foucault and the Iranian Revolution* (Chicago: University of Chicago Press, 2005), 216–20, esp. 219; A. Stille, *The Future of the Past* (New York: Farrar, Straus and Giroux, 2002), 182–99.

16 FROM PHREAKING TO FUDDING

1 D. Campbell, "Are Telephones Addictive?" *New Scientist* 60, no. 876 (December 13, 1973): 756–60, esp. 758; B. Sterling, *The Hacker Crackdown: Law and Disorder on the Electronic Frontier* (New York: Bantam, 1992), 12–14.

2 C. Breen and C. A. Dahlbom, "Signaling Systems for Control of Telephone Switching," *Bell System Technical Journal,* 39, no. 6 (November 1960): 1381–1444.

3 S. Wozniak and G. Smith, *iWoz* (New York: W. W. Norton, 2006), 107; http://www.webcrunchers.com/crunch/.

4 B. Levin, *The Pirates and the Mouse: Disney's War against the Counterculture* (Seattle: Fantagraphics, 2003).

5 A. Hoffman, *Steal This Book* (New York: Pirate Editions, 1971), 119, 144.

6 *Radical Software* 1 (1970), 1: www.radicalsoftware.org.

7 *Youth International Party Line* 1 (June 1971); 8 (February 1972); editor's page at http://cheshirecatalyst.com/tap.html.

8 C. M. Kelty, *Two Bits: The Cultural Significance of Free Software* (Durham, N.C.: Duke University Press, 2008), 28–29.

9 Campbell, "Are Telephones Addictive?"

10 R. Rosenbaum, "Secrets of the Little Blue Box," *Esquire,* October 1971, 117–25, 222–26.

11 S. Levy, *Hackers: Heroes of the Computer Revolution* (New York: Penguin, 2001 [1984]), 50–52, 94–95.

12 J. Markoff, *What the Dormouse Said: How the Sixties Counterculture Shaped the Personal Computer Industry* (New York: Viking, 2005), 85–87; Levy, *Hackers,* 23, 39–49, 60, 88, 124–36.

13 T. J. Sturgeon, "How Silicon Valley Came to Be," in *Understanding Silicon Valley: The Anatomy of an Entrepreneurial Region,* ed. M. Kenney (Stanford, Calif.: Stanford University Press, 2000), 15–47, esp. 44.

14 Markoff, *What the Dormouse Said,* 94–97, 103–4.

15 Markoff, *What the Dormouse Said,* 28, 116; Turner, *From Counterculture to Cyberculture,* 70; T. Roszak, *From Satori to Silicon Valley* (San Francisco: Don't Call It Frisco Press, 1986), 8–9.

16 T. Nelson, *Computer Lib/Dream Machines* (Chicago: T. Nelson, 1974), DMX; M. Orth, "Whole Earth $$$ Demise Continues," *Rolling Stone,* March 16, 1972; Turner, *From Counterculture to Cyberculture,* 69–73, 78–97, 113–14; Levy, *Hackers,* 159.

17 T. Albright and C. Perry, "The Last Twelve Hours of the Whole Earth," *Rolling Stone,* July 8, 1971; Levy, *Hackers,* 197–98; Markoff, *What the Dormouse Said,* 197–99, 261–62.

18 Markoff, *What the Dormouse Said,* 275–87.

19 I. Illich, *Deschooling Society* (New York: Harper & Row, 1971), 77; I. Illich, *Tools for Conviviality* (New York: Harper & Row, 1973), 18–21.

20 Illich, *Tools for Conviviality,* 11–12, 16, 43, 109; *Deschooling Society,* 19–20, 72–104. Giap was the South Vietnamese General Vo Nguyen Giap; ITT was International Telephone and Telegraph, a conglomerate originating in telephony patents and associated with conservative causes, including the anti-Allende conspiracy in Chile.

21 Nelson, *Computer Lib/Dream Machines,* CL59, DM3, DM58; T. Nelson, *Literary Machines,* 5th ed. (Swarthmore, Pa.: T. Nelson, 1983), 2/35, 2/37–38, 2/54, 4/4–6. For the relation between classical (J. S. Mill) liberalism and hacker ideologies, see E. G. Coleman, "The Social Construction of Freedom in Free and Open-Source Software: Hackers, Ethics, and the Liberal Tradition" (Ph.D. diss., University of Chicago, 2005), 196–200.

22 *Homebrew Computer Club Newsletter* 2, no. 13 (January 19, 1977), 3. For Felsenstein's debt to Illich, see "Convivial Cybernetic Devices: From Vacuum Tube Flip-Flops to the Singing Altair," *Analytical Engine* 3, no. 1 (November 1995), at http://opencollector.org/history/homebrew.

23 Levy, *Hackers,* 186.

24 Wozniak and Smith, *iWoz,* 28–29, 93–111; Markoff, *What the Dormouse Said,* 271–73; Levy, *Hackers,* 244–46. See also Wozniak's own reminiscences at www.woz.org.

25 Levy, *Hackers,* 251–54, 271–74; Turner, *From Counterculture to Cyberculture,* 115; Markoff, *What the Dormouse Said,* 275–87.

26 B. Gates, "An Open Letter to Hobbyists," *Homebrew Computer Club Newsletter* 2, no. 1 (January 31, 1976). See also S. Manes and P. Andrews, *Gates: How Microsoft's Mogul Reinvented an Industry and Made Himself the Richest Man in America* (New York: Doubleday, 1993), 91–96, and (for a more slanted reading) J. Wiley and J. Erickson, *Hard Drive: Bill Gates and the Making of the Microsoft Empire* (New York: Wiley, 1992), 101–7.

27 Levy, *Hackers,* 230.

28 The most thoroughgoing argument for the transformative economic effect of networks is Y. Benkler, *The Wealth of Networks: How Social

Production Transforms Markets and Freedom* (New Haven, Conn.: Yale University Press, 2006).

29 For the elaborate synthetic realities that these have developed into, see E. Castronova, *Synthetic Worlds: The Business and Culture of Online Games* (Chicago: University of Chicago Press, 2005).

30 H. Rheingold, *The Virtual Community: Homesteading on the Electronic Frontier* (Reading, Pa.: Addison-Wesley, 1993), 56–59, 133–34, 310; Turner, *From Counterculture to Cyberculture,* 156–62; Sterling, *Hacker Crackdown,* 45–47, 50.

31 *Phrack* 1, no. 7 (September 25, 1986), 3; Sterling, *Hacker Crackdown,* 67, 73–77, 83, 85–87.

32 Sterling, *Hacker Crackdown,* 63–67, 88–95; http://www.2600.com/. Old issues of many of these organs, including *Phrack* and the *Legion of Doom Technical Journal,* are sometimes accessible at http://www.textfiles.com/magazines/.

33 Sterling, *Hacker Crackdown,* 55–57, 100–101; Turner, *From Counterculture to Cyberculture,* 167.

34 "Is Computer Hacking a Crime?" *Harper's Monthly* 280, no. 1678 (March 1990): 45–57; Rheingold, *Virtual Community,* 44; Turner, *From Counterculture to Cyberculture,* 167–70.

35 "Is Computer Hacking a Crime," 53. For Barlow's *Declaration,* see P. Ludlow, ed., *Crypto Anarchy, Cyberstates, and Pirate Utopias* (Cambridge, Mass.: MIT Press, 2001), 27–30.

36 S. Weber, *The Success of Open Source* (Cambridge, Mass.: Harvard University Press, 2004), 47, 114; R. M. Stallman, *Free Software, Free Society: Selected Essays* (Boston: GNU Press, 2002), 16.

37 http://www.catb.org/%7Eesr/halloween/index.html.

38 At the time of writing, however, rumors are flying that Microsoft may be trying the strategy again with its Silverlight program, this time targeting Adobe's Flash standard for online video. The importance of uniform standards for science and technology has been a leitmotif of much recent work: see, for example, B. Marsden and C. Smith, *Engineering Empires: A Cultural History of Technology in Nineteenth-Century Britain* (New York: Palgrave MacMillan, 2005).

39 S. Shapin, *A Social History of Truth: Civility and Science in Seventeenth-Century England* (Chicago: University of Chicago Press, 1994), 410, 415–16.

17 PAST, PRESENT, AND FUTURE

1 D. Defoe, *An essay on the regulation of the press* (London: n.p., 1704), 19–21.

2 See especially A. C. Mertha, *The Politics of Piracy: Intellectual Property in Contemporary China* (Ithaca, N.Y.: Cornell University Press, 2005), 35–76.

3 B. Norris, "Video Report," *Sight and Sound* 52 (1983): 106–8; R. Murphy,