1 THE SHAPE OF THE NETWORK

The Graft

Here is how you tear up railroad track. "The jaw of a giant loader plucked up railroad ties in its teeth. A wheelbarrow-like contraption sucked up bolts and spikes, and spit them out. Guys in hardhats snipped off power cables and yanked down wire fences."[1] Stripped for metal during World War II, railroads are now stripped for tax reasons. Gradually, thousands of miles of track have been abandoned since peaking at 254,000 miles in 1916;[2] the pace has only sped up since deregulation in 1980. In photographer Mark Ruwedel's *Central Pacific #18* (1994), you can see the track bed exposed and eroding (figure 1.1). A pile of bent trestles along the side disrupts the symmetry of the composition. The familiar parallel lines of a railroad track heading to the vanishing point seem to signal another vanishing: the railroad, that technology of the machine age, itself heading for obsolescence.

But the relatively recent gouges and tire marks in Ruwedel's photograph suggest that the railroad has not been swept aside entirely by new technologies. In fact, the relationship between old and new is a complicated one, because beneath the abandoned railroad bed from the nineteenth century lies fiber-optic cable, technology of the twenty-first century. In 1978, the track's owner, the Southern Pacific Railroad, realized that it could sell excess capacity on its network—heretofore used for internal communications, such as train signaling—to corporate customers. A few years later, the Southern Pacific spun off this telecommunications division, the Southern Pacific Railroad Internal Network; its new acronym was SPRINT. Around ten years later, it spun off a second company, Southern Pacific Telecommunications Company, later renamed Qwest, to run fiber beneath its rights-of-way. Together,

Figure 1.1
Mark Ruwedel, *Central Pacific #18*, from the series *Westward the Course of Empire*. Gelatin silver print, 8 × 10 in., 1994. Courtesy of Mark Ruwedel.

the corporate descendants of a single railroad company comprise two of the six major fiber-optic carriers of the US Internet (figure 1.2).[3]

This chapter begins by contending that new and old medias are layered on top of each other, just as the railroad track is layered with fiber-optic conduit. The process of media change causes "old media" to be forgotten in our cultural memory, almost as if a box has been buried, and then the map or route to it abandoned. We know or remember it is there somewhere, but are unable to see it. Though digital technologies seem to change faster than the observer can record, its physical traces are slower to change. By examining the physical geography of digital networks, we can see the spaces where the old has been displaced, and where new media, such as that of the Internet, are layered, adjacent, or even intertwined with far older mediums. Buildings and built landscapes, such as railroad tracks and other infrastructures, are the slowest medium of all, taking years to construct and then an order of magnitude longer to decay. Paradoxically, because space is arguably

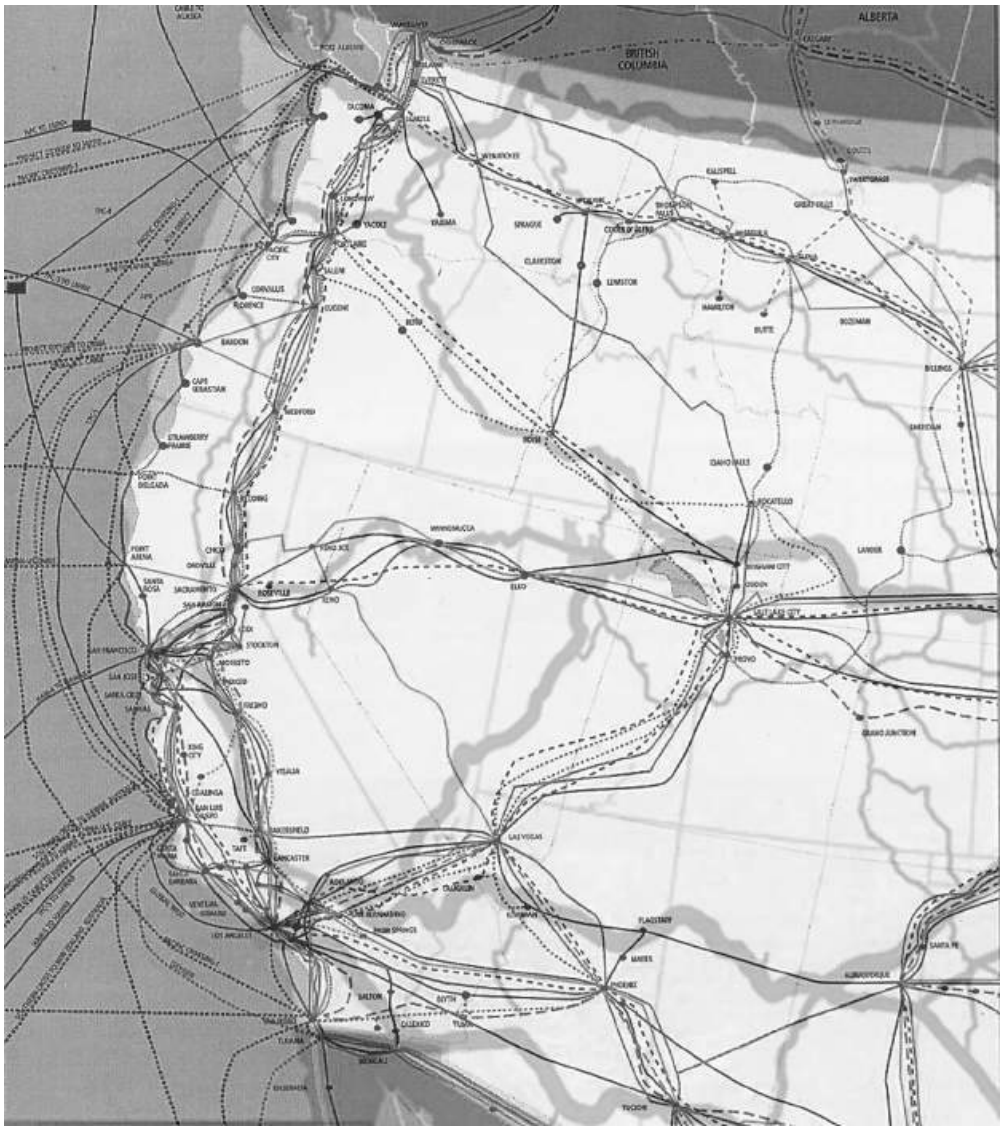

Figure 1.2

Overlay of fiber-optic routes and railroad routes. *Sources:* KMI Corp., "North American Fiberoptic Long-Haul Routes," 1999; U.S. Department of Transportation, Federal Railroad Administration, 2010. (KMI was acquired by CRU Group, crugroup.com, in 2006.)

always being made obsolete by the daily practice of bodies walking through and interacting with space, the built environment may be an ideal location for observing displacement and media change.

It may appear odd to begin a book about digital networks by following the transcontinental rights of way granted in the 1860s by the Pacific Railway Acts. I do so, however, to offer a puzzle: even as digital networks seem to annihilate or deterritorialize physical space, space seems to continually

reappear, often as an unwanted flaw in the system.[4] A new $1.5 billion fiber-optic cable across the Arctic will shave between twenty and sixty milliseconds off the route from Tokyo to London for stock market traders, but the toxic metals used in their electronics inevitably end back up in the bodies of laborers manning poorly regulated disassembly plants in China.[5] Their bodies are absent from the picture, just as the Chinese bodies of railroad workers are absent from nineteenth-century railroad photographs.

When cloud computing enters into the picture, this puzzle becomes particularly complicated, because the cloud buries or hides its physical location by design. The cloud is so named because the Internet has traditionally been represented as a cloud in network diagrams: it "has no fixed topology and typically covered varying geographic areas."[6] The cloud thus offers a vision of globalization that follows the dictates of a multinational corporation—a coalition of geographic areas that move capital and resources through the most efficient path. Just as it is cheaper for Apple to use Ireland as its tax domicile to avoid paying US taxes on its French operations, for example, it is more efficient for Facebook to serve some of its Japanese customers from a Singapore data center.

But if the cloud has turned geography into the virtual flows of market capital, it has also spawned a number of equally virtual political movements that challenge this vision. At the same time that networks describe the newly dematerialized corporate structures, they also have shaped capital's seeming opposite: antiglobalization protests. The loosely organized Occupy Wall Street protests seemed, like the Internet, to be resistant to the "hierarchical centralization of 'the mob,'" even creating, one political scientist claims, a new form of "cloud protesting."[7] Yet as much as the Occupy protests were enabled by social media, they have also been very much about occupying specific buildings, public places, and locales. As Etienne Balibar points out, any sort of deterritorializing communications technology is dialectically related to its opposite: "the constitution of a network is also of course a reterritorialization."[8]

If the cloud represents a new reconfiguration of the relationship between place and placelessness, it is clear that relationship directly affects the organization of contemporary power. What this chapter attempts to do is to offer a more precise structure of the cloud, one that accounts for both aspects of this dialectic. It starts by asking a simpler question: where is the cloud's network in physical space?

Because of geographic limitations, the route from Salt Lake City to the San Francisco Bay Area has been the final leg in a number of American transcontinental networks, and therefore it offers a rich site for exploring the layering or copresence of multiple technologies. That route was the last segment of the railroad and telegraph systems, joined at Promontory, Utah, in 1869; the telephone system, joined at Wendover, Utah, in 1914, which AT&T, referring to the railroad's Golden Spike, celebrated as the "Golden Splice"; the national television network, dubbed the "electronic Pony Express" and completed in 1951; and finally the ARPAnet, a predecessor to the Internet, which joined the University of Utah to the Stanford Research Institute in 1969. (A transcontinental communications system was, as one might expect, impeded by the difficulty of the terrain; harsh weather, even the lack of available water, made this route the last to be constructed. Salt in the air corroded telephone electronics, while gophers were reported to have attacked coaxial cable casings.[9])

The location and extent of the network fundamentally affected the network's shape and structure. Before the transcontinental system came into place, each type of network contained pockets of isolation or asynchrony: nineteenth-century mail networks were unreliable and, consequently, western states were often out of date with news in the East; midcentury television stations showed primarily local programming and broadcast local news; even ARPAnet's research nodes were built for different computing capabilities: Utah's facilities were for computer graphics, while the Stanford Research Institute specialized in databases.[10] In almost every case, the completion of the network across the desert had profoundly centralizing tendencies: the railroad tied the nation's goods and passengers together, standardizing clocks in the process by creating "railroad time"; telephone service gave rise to the largest and wealthiest monopoly on earth, the Bell System; television broadcast schedules were coordinated to deliver a uniform American audience to advertisers.

Yet ARPAnet and the eventual Internet seemed to be different. With its distributed structure, it seemed to resist centralization; indeed, its structure held the potential to radically transform the shape of communications. In his seminal paper "On Distributed Communications Networks" (1962), computer scientist Paul Baran offers a diagram that illustrates three major network topologies, from centralized ("star") to decentralized ("tree") to distributed ("mesh" or "cloud") (figure 1.3).[11] It has become virtually an article of faith among scholars of new media that network design has progressed from the

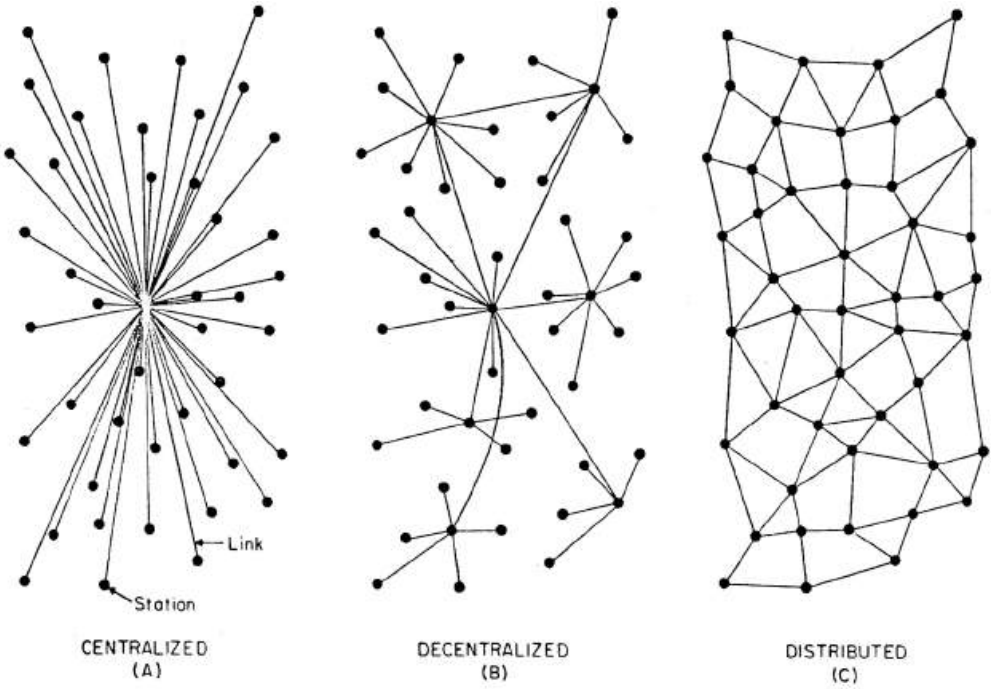

FIG. 1 — Centralized, Decentralized and Distributed Networks

Figure 1.3

Paul Baran, "Centralized, Decentralized and Distributed Networks," 1962. Reproduced with permission of The RAND Corp.

first to the last shape over time, resulting in a distributed network called the Internet.[12] As evidence, these scholars cite the movement away from the centralized, command-and-control structures of US Air Force computer rooms to ARPAnet and the contemporary Internet. This model of rupture remains a seductive myth because it explains the dispersion of power through the formal qualities of the computer networks that supposedly enable it.

One problem, however: the distributed network, as designed by Baran, was never built. Stephen Lukasik, former director of ARPA, points out that Baran's proposed system "had many features still sorely lacking in the public Internet forty years later: redundancy to withstand heavy attacks yet fail gracefully as links were severed; high reliability; security."[13] Indeed, a truly distributed network is almost impossible to create, because of economic, political, and even geographic considerations (it is hard to run fiber-optic cable across mountains). As a result, virtually all traffic on the US Internet runs across the same routes established in the nineteenth century, a point

that is readily visible when looking at network diagrams, which have changed remarkably little since Baran's day. It is worth remembering that the fiber-optic cables that run from Salt Lake City to the San Francisco Bay Area are in the same position they always have been, since the telegraph: in the immediate vicinity of railroad tracks.

(I have been using the case of the US Internet because it is both the largest and most-developed network and also the network that most scholars describe as "open" and distributed. In cases such as the Chinese Internet, described as the Party-controlled "Great Firewall of China," it should be clear that there is nothing inherently decentralizing about Internet technology. As I suggested in my introduction, the relative lack of attention to non-Western Internets results in the elision of place from "the Internet," and the collapse of a multitude of networks into a single, monolithic cloud—itself an ironically centralizing ideology.)

What we realize is that the structure of the US Internet is bifurcated. On a logical level, we see communication patterns that may resemble a distributed network—although the fact that cloud computing concentrates our files into the data centers of a few underlying service providers, such as Google and Amazon Web Services, complicates this theory.[14] This seemingly distributed network is built, however, on top of a layer that can only be centripetal in nature, whether approached from the question of access—one or two broadband companies per population center, such as Comcast and the local telephone monopoly; the market dominance of a handful of wireless carriers, such as Verizon and AT&T—or from the level of infrastructure, where six telecommunications companies control the vast majority of the routes.[15] And so the introduction of interoperable protocols such as Internet Protocol, or IP, is like the situation of railroad barons: when they began to widely adopt standard gauge after 1863, interoperability between their networks only increased their concentration of power.

Seen properly, the structure of the Internet resembles a *graft*: a newer network grafted on top of an older, more established network. In this metaphor, preexisting infrastructures, such as the rail network, are like rootstock, while the newer fiber-optic cables resemble the uppermost portion, known in horticulture as the scion. Neither half, rootstock or scion, describes the full story; yet it is almost impossible to look at the whole. Looking at the shape of the more recent and more visible part, the distributed network, is like looking up at tree branches silhouetted against a bright sky in a low-angle shot of

a forest. From below, looking at the newest growth, the branches appear to resemble a series of loosely but densely interconnected structures—possibly even a rhizome, a mesh, or a cloud. (Looking at the older part, we see only a single, centralized trunk.) But these two parts are integral and interconnected: the scion takes life and nutrition from the grafted rootstock, and the qualities of the rootstock (sturdiness, survivability, its connection with terrain) transport themselves in indirect ways to the scion. To look at the middle point of union, to think both parts at the same time, is not just "arboreal"; it is historical.[16]

As a graft, the Internet is always already a historical object, and the next stage of its development is never a complete rupture from its past. As such, when scholars liken the shape of power to the shape of the network, citing its manifestations in protest movements or terror groups,[17] they inevitably refer to the distributed network, the top layer, or the scion. But territorial politics also threaten to periodically erupt from below, entering the root structure of the present in the way that the Latin *terrere* enters the etymology of both territory and terror.[18] Rather than dismiss these threats as aberrations from a now-forgotten past, we might understand them as part and parcel of the structure of the graft. For one increasingly begins to suspect that the rapid proliferation of networks may be common cause of both "electronic" and "territorial" wars.

It is this book's contention that the graft may have more than a descriptive use; the graft may also serve as a method of analysis, a way of uncovering a structural relationship between power and networks. To understand the irruption of war (specifically, the older, nominally obsolescent variety concerned with territory) into network culture, I will move between the present day and the Cold War era when the Internet's predecessor networks were designed. Looking for the legacy of electronic wars in the empty spaces of the desert West, we will find our first case study in 1961, the first documented moment of the American telecommunications network coming under attack; after that, we will briefly consider another Cold War infrastructure that has shaped the Internet: the interstate highway system.

But let us first set the table for this discussion by reviewing the historical claims that surround the Internet's origins, one that Alexander Galloway sums up as follows: "the Internet was invented to avoid certain vulnerabilities of a nuclear attack."[19] The old shape of war, exemplified by cities such as Hiroshima or Nagasaki, is a "strategic massing of power," easily targeted in

an atomic strike. But for Galloway as for other scholars including Hardt and Negri, the "Internet has a different diagram than a nuclear attack; *it is in a different shape*. And that new shape happens to be immune to the older."[20] Like the just-so stories of how tigers got their stripes, or rhinoceroses their horns, there is something captivating in this story of how the network got its shape. The idea of the bomb appears to explain a number of things: the network lacks a central location because a center would make a good target. Urban planners responded to the atomic threat by dispersing industrial targets away from urban centers;[21] and this dispersion also seems to influence an entirely new invention: the network as Internet.

Indeed, the claim may even appear self-evident when one reads Paul Baran's first paper (1960) on survivable communications networks, a paper published two years before his now-famous diagram of network shapes (figure 1.3). In it, Baran imagines how to maintain some continuity of government in the worst-case scenario, and describes, as an example, a distributed network of congressmen scattered across the country. Some—many, even—are killed in a nuclear strike, but the surviving members of Congress may be able to cast votes from their home offices. This paper opens with a steely evocation of survival after the mushroom clouds dissipate: "If war does not mean the end of the earth in a black and white manner, then it follows that we should do . . . all the things necessary to permit the survivors of the holocaust to shuck their ashes and reconstruct the economy swiftly."[22]

It is because of Baran's 1960 paper that one of the most widely held beliefs about the Internet began to propagate. Yet by now, this claim has been well debunked; it comes out of a series of confusions, between Baran's 1960 paper and a paper written two years later, and between the Internet and its earlier incarnation, ARPAnet. (ARPAnet scientists cited, but did not implement, Baran's 1962 paper, and even in that 1962 paper, Baran had moved away from the nuclear rhetoric of his previous paper. Weapons salvoes were now merely a special case of a more general principle, that of link reliability and interference.[23]) Baran's network was never built, and we are several generations removed from its nuclear logic.

If the Internet never had this nuclear-proof shape, then why do scholars continually tell or write this idea back into existence? In other words, I'm interested less in debunking the myth than in the reason that it persists in digital culture, reanimated in the popular imagination of a digital cloud shaped like the elegant mesh of Baran's diagram. There is, in short, a

collective desire to keep the myth alive despite evidence to the contrary. This desire, after all, is symptomatic not only of how media historians explain the Internet's origins, but is, more generally, symptomatic of our method. To want another opinion; to doubt received history; to read history against the grain; these are all signs, in academia, of good scholarship.

I purposely bring up the question of media scholarship rather than the network itself because it's important to recognize that scholars are implicated in an intellectual quest that is not far from paranoia—a word that is not meant as a pejorative. Where else can one find the belief that a single idea, the network, links "drug cartels, terror groups, black hat hacker crews," with "corporate management techniques, manufacturing supply chains, advertising campaigns," except inside a Thomas Pynchon novel?[24] But on a more general level, how else can we take the act of interpretation—the act of finding meaning within disorder, the "reflex of seeking other orders behind the visible," as Pynchon once glossed paranoia—that scholars of digital culture, myself included, so often engage in? I am surely not the only teacher who has been accused by a student of engaging in conspiracy theories when I read too much between the lines of a text or shots of a film, or when I piece together information from disparate sources and disciplines to weave a web or a network.

Let me pause here to underscore a semantic point. I'm intentionally engaging in some slippage between network as a physical object (the Internet) and network as a metaphor for knowledge, because, I'm arguing, the network is always more than its digital or physical infrastructure. The network is a primarily the idea that "everything is connected," and, as such, is a product of a system of belief. The reader will readily observe that when I use the word "network," I mean something a little different from its common definition. Because reality can never match up to that system of belief, because, in fact, not everything is connected, the network exists primarily as a state of *desire*.

Studying the metro Detroit area in 1972, the architect and urban planner Constantinos Doxiadis declared: "Our child, our city is sick. We look only at the symptoms and we do not understand the causes. We are frightened. The mother goes out in the street and screams."[25] To illustrate his point, this architect printed photographs of a spider's web before and after ingesting amphetamines; the second picture, taken twelve hours after ingestion, is compared to Detroit's road network, one of the symptoms of postwar

dispersion from an urban core. A bad network is likened to a bad drug trip. The messy road network demands, for Doxiadis, a single solution. "We must coordinate *all* of our Networks *now*. All networks, from roads to telephones."[26] Yet the solution—a network of networks, the same desire that led to what we now call the Internet—is itself a malady; it is Doxiadis's case that causes critic Mark Wigley to retroactively label him as one of the first patients suffering from "network fever."[27] Network fever is the desire to connect *all* networks, indeed, the desire to connect every piece of information to another piece. And to construct a system of knowledge where everything is connected is, as psychoanalysis tells us, the sign of paranoia.

In other words, network fever cannot be separated from the network, because the network is its fever. The cloudlike nature of the network has much less to do with its structural or technological properties than the way that we perceive and understand it; seen properly, the cloud resides within us. It is crucial to keep this in mind as we enter the Cold War era in the next section; there, we will examine the first moment when the American communications network became part of the nation's critical infrastructure, something to be protected against foreign (even nuclear) attack. While I have put paranoia on the table as a potential lens through which to understand the network, I'm not trying to establish that a Cold War network was paranoid——a tautological definition if there ever was one. Rather, I hope to understand how a specific way of thinking networks and connectivity in 1961–1962 has continued to structure our vision to this day, long after the physical network has been dismantled and replaced by a new one. Just as abandoned railroad tracks have left a barely visible channel across the desert West, these Cold War forms linger inside the cloud but are visible only in their absence. It is to these ghosts that I now turn.

"Strange and Unusual Fits," 1961

There was, in fact, one recorded attack on the network, but it did not come from a missile hurtling through the air, or anything nuclear-related. On May 29, 1961, an edgy nation woke up to discover that three microwave towers had been dynamited by unknown saboteurs the previous morning. Crucially, these relays, located in remote locations in the Great Salt Lake desert, not only glued together the transcontinental telephone system, but also formed part of the national defense circuit. For a tense four hours, the explosion

affected everything from the Strategic Air Command and the Conelrad emergency warning system to Associated Press teletype and civilian radio circuits. Various rumors suggested that it could have been the work of Soviet agents—General Maxwell E. Rich, commander of the Utah National Guard, thought that the Soviets might be monitoring how fast the nation responded to an emergency, while an unnamed military officer on the scene recalled that Soviet trawlers had once dredged up submarine cables.[28] Air Force General Curtis LeMay cited a published report stating that the perpetrators bore the hallmarks of training from an East German school of sabotage.[29]

Whoever the culprit was, the reaction was swift and immediate. Six states deployed soldiers and national guardsmen to their relay stations and signal towers; as a precaution, Bell facilities as far away as Illinois received armed sentries. In Los Angeles alone, a nervous sheriff summoned all seven thousand deputies to report for duty. The governor of Utah rushed to inspect the scene of destruction, which left concrete and aluminum debris twisted into the volcanic rocks, a sharp smell of battery acid in the air, and—most oddly——a white field of Styrofoam bits, a result of the microwave lens's unusual construction.[30] *Newsweek* captured the scene well: "The desolate wastes of the Great Salt Lake Desert suddenly swarmed with investigators—civil and military."[31] Meanwhile, temporary circuits had to be installed: a Globemaster cargo plane landed the same evening at Wendover Air Force Base carrying more personnel and portable microwave equipment; so much equipment, in fact, that the phone technicians wondered how they would load them onto their company trucks.

This was the first act of sabotage directed against the nation's transcontinental communications circuits, and it signaled a shift in the way the nation understood communications: previously invisible lines in the desert had suddenly been exposed. The centralized Bell System upon which the nation relied had begun to exhibit cracks, even if its officials rushed to assure the nation that defense circuits had been rerouted within ninety seconds. (The actual response time turned out to be far longer.) More important for our story, the bombing of the Bell System occurred during a moment when scientists were designing distributed networks to survive similar attacks. In other words, the bombing made real a largely abstract fear—that war might destroy a centralized communications network. Because this was front-page news, Baran almost certainly read about it as he was revising a paper that he would publish as "On Distributed Networks" a year later.[32] So two things

happened that year: the technological network came into being, simultaneously with another kind of network—network understood as conspiracy.

A group calling itself the American Republican Army eventually took credit for the attack. It was later discovered to be an army with a "rather slim" membership of two, namely, Jerome Brouse, age fifty-one, a construction worker with a grudge against AT&T's monopoly, wearing a fake six-shooter in his holster, and a partner, Dale Chris Jensen, age thirty-three. Yet because the bombing affected the system as a whole, the 1961 event seemed, at the time, to result from something rotten in the political system. Writing for the *New Republic*, journalist Gerald Johnson saw the bombing as symptomatic of a national "atmosphere of conspiracy." Why shouldn't a nation see everything as a "counterplot" or "plot," Johnson asked, when it had been told by its government that "half the world is engaged in a great and infamous plot against it, and that it can trust nobody?"[33] The secretive atmosphere of government breeds a corresponding rise in secret societies, Johnson wrote; the supposed left-wing plots by Communists create a corresponding rise in right-wing groups such as the American Republican Army.

Before the culprits were caught, another rumor circulated that the bombing was a test by another branch of the government: a rumor almost too strange to believe outside an "atmosphere of conspiracy," yet a rumor matched and even exceeded by later conspiracy theories on the supposed governmental origins of the Kennedy assassination and 9/11. Yet there was something specific about the Bell System as the locus of conspiracy. Conspiracy, by definition, is concerned with systems; it connects seemingly unrelated pieces of information, weaving them into systems. In 1961, the Bell System was not only the largest and wealthiest corporation in the world (as *Life* proudly noted the following month), but it was also the technological system by which corporations, governments, and individuals spoke to each other. The bombers in the American Republican Army called AT&T a "cartel," but it turned out to be far more: AT&T *was* the Pynchonesque system of paranoia in which "everything is connected."

Push a little further into the story of the bombing and we begin to see something unexpected. A seller of janitorial supplies sporting a Castro-style beard and imagining himself as an entire army triggers the actual army to respond; there is an almost comical relationship between the very routine business of AT&T and the gravity of a national emergency. As the legal records show, accident and emergency are intimately connected, and the two

ends of the spectrum can be flipped at any moment. To see what I mean, let us turn to the halls of the Senate.

On June 7, about a month later, the Senate Internal Security Subcommittee (SISS) took up a bill to safeguard defense communications, which had almost certainly been rushed to the docket because of the attack. Bill 1990's sponsor, Senator Thomas Dodd of Connecticut (who would later be indicted for corruption by the same committee), was absent, but submitted a written statement opening with an ominous description of "a person or persons unknown" who had sabotaged "3,000 interstate communications" circuits in Utah and Nevada, many of which, Dodd continued, were essential to military and civilian defense.

Dodd's bill was a relatively simple one that extended the anti-sabotage law to all defense-related circuits, not just federally owned ones; in fact, it was a resubmission of a bill that hadn't made it to the Senate floor the previous year because of time limitations. But it was a strange hearing: with the bombing on everyone's minds, photographs of the attack were appended to the Senate record. What ought to have been routine business became a matter of grave national security, yet, at the same time, the senators wondered what to do if the destruction turned out to be the result of a worker on strike or even a prankster: "some boy that likes to hear something pop off," or who might "stub the toe of a Western Union messenger."[34] Comical scenarios, perhaps, but to this day, crucial communication lines are disrupted accidentally all the time, typically by a farmer or a construction worker digging with a backhoe: in 2009, the *Washington Post* reported on the phenomenon of black Chevrolet Suburbans arriving at construction sites. Suited government agents tended to show up minutes after an accidental cut of a classified (and thus unmarked) fiber route.[35] The *Post* even offered a name for classified cable routes: "black wire." So the distinction between the emergency and the accident was already wearing thin in 1961, and fifty years later, it seems to have eroded away entirely.

Moreover, in the hearing, it wasn't clear what defense system—or what circuits—they were talking about securing. The senators and the military men approached this question first with a list of examples and acronyms, among them the Ballistic Missile Early-Warning System (BMEWS), the mid-Canada line, the Distant Early Warning (DEW) Line, the Missile Defense Alarm System (MIDAS), etc. But the confusion was an epistemological one: General DuPlantis testified that "it is impossible to define 'what is operated

and controlled by the United States.'"[36] For if a law is written to protect engineered military circuits, that same law "could be interpreted to extend to the entire communications systems" of the Bell System, Western Union, and any other company. Any circuit could, at any moment, become a military circuit. In the event of an emergency, one circuit may take an alternate path; a Des Moines outage might affect both St. Louis and Kansas City. Responding to a question by Senator Roman Hruska—what *is* the network?—DuPlantis testified, in dialogue reminiscent of a Beckett play:

> *General DuPlantis:* Sir, you would never be able to define the system that you had reference to since it is subject to call. As I tried to explain in this rerouting process which goes on all the time, you can't put your finger on the circuits that you will call up. You know where the terminal ends are, but these circuits will take devious paths from minute to minute . . .
> *Senator Hruska:* And if some damage to any part thereof occurred, it would be considered damage within the meaning of the law, would it not?
> *General DuPlantis:* If you could define which ones you had reference to.
> *Senator Hruska:* Well, if they are so comprehensive that it could be any of them.
> *General DuPlantis:* This could be true, but it would be very difficult.
> *Senator Hruska:* I understand the circuitous business.
> *General DuPlantis:* That it goes round and round and you don't know where it goes from minute to minute.[37]

One imagines a slight note of exasperation from the general. Because of the new design for switching networks, the circuits varied from "minute to minute." Thus, for DuPlantis, as it is for scholars of contemporary networks, it was impossible to pin down what the system "is"; the system reroutes itself depending on the need. It is a logical overlay, rather than a physical thing; it is a process, not a static moment; it is a matter of what should not be covered, rather than defining what it does cover. The network is an idea that is resistant to knowing.

The practical result, for DuPlantis, was that the law *must* apply to all circuits, because this is the very design of the network. Concerning the question of "what our requirements for seizure would be," DuPlantis testified: "This, of course, is very nebulous, but . . . we can say we have a requirement for all of it."[38] What could conceivably count as part of the network is "very nebulous," echoing the word's Latin origins in *nebule*, cloud: a cloudlike vision that

is simultaneously vague and also universal. In the 1950s, AT&T successfully sued an undertaker who gave away a plastic cover for its telephone books for violating its monopoly on telecommunications: it claimed that its network extended even to the act of picking up the Yellow Pages.[39] Like the AT&T lawyer who stumbled across the plastic cover by accident, the committee, too, saw the network in everything that could conceivably be involved in communications, from AT&T lines to Western Union messengers. "All of it": the prime symptom of network fever.

What we take from this hearing is that war circuits are indistinguishable from civilian circuits, because, in a time of emergency, everything will be part of a war circuit. Although the modern packet-switched network had yet to be invented, the idea of the network was beginning to radically reconfigure the relationship between military and civilian spheres, the state of war and the state of exception. And while the rest of this book will explore this issue in more detail, I want to dwell on the implications of DuPlantis's testimony. For there is something richly evocative about his description that "these circuits will take devious paths from minute to minute."

What did DuPlantis mean by "devious"? Attempting to explain this to the senators, the counselor remarked that he had once made an emergency call from Washington to Seattle that needed to be patched through via Atlanta and Minneapolis.[40] In fact, DuPlantis responded, it is even more devious than the counselor's example; machines automatically route calls around broken circuits, so that paths deviate from the norm all of the time. A physical route is suppressed in favor of the logical route; the networked path deviates from the straight path. It is indeed a "circuitous business," as the senator put it.

But there is another context, of course; one that will go a long way toward explaining why the network is a matter of internal security, rather than international security; why there are no discussions of nuclear strikes but plenty of discussion on the limits of regulation. For the word "devious" has a peculiar resonance in the context of the Internal Security subcommittee. Recall that this is the same committee that had become notorious for its inquisitions of "subversives" and communism; the deviant, in this context, would have referred to those who chose a political path deviating from the norm. Serving as the Senate counterpart to the House Un-American Activities Committee (HUAC), the SISS had originally been chartered to investigate acts "including, but not limited to, espionage, sabotage, and infiltration of persons who are or may be under the domination of the foreign government

or organization controlling the world Communist movement or any movement seeking to overthrow the Government of the United States by force and violence."[41]

In today's digital culture, deviance is commonly associated with sexual deviance. This is what animates Wendy Hui Kyong Chun's study of the "cyberporn" scares of the 1990s, where anxiety about the network comes from the twenty-first-century paranoid subject, who metaphorically understands fiber-optic cable as nerves of light that penetrate his body and produce a deviant sexual response.[42] And this direction may be a productive one to pursue, as SISS had spent a good part of the 1950s investigating homosexual "deviants" in the State Department as part of the so-called Lavender Scare.

But what the Senate record shows is perhaps less expected: fully half of the June 7 hearing on network security was taken up by a discussion of another kind of political deviation, organized labor. Indeed, the final two witnesses called to the hearing were the president of the Commercial Telegraphers' Union and the counsel for the American Civil Liberties Union. The witnesses were concerned that telecommunications workers exercising their legitimate right to strike might, under the new law, be detained for national security reasons, even as they pledge to suspend those rights, out of patriotism, during a time of war.[43] And the last time the Bell System had been disrupted was during a period of labor unrest—the only time before Wendover that the robustness of defense circuits had been tested. During a 1957 Communications Workers of America strike, a worker acting on his own had dynamited Southern Bell lines in Jackson, Mississippi; this, General Bestic remembered, was the last time he testified about defense communications. The same committee's investigations of alleged Communists in Southern labor unions were undoubtedly still on his mind.

The network that the committee saw was the network within the network, as it were: the shadow of organized labor over the telephone lines, what filmmaker Caroline Martel, in her documentary on female phone operators, called "the phantom operator." And, indeed, there was a long-standing connection between the threat of labor and the misrouted message. In 1907, *Le Cri Postal*, the newspaper of the Postmen and Telegrapher's union, made this fear explicit: "What you will never be able to prevent is that some fine day the letters and telegrams from Lille take a little stroll around Perpignan. . . . What you cannot avoid is that the telephone wires be simultaneously tangled

and the telegraphic instruments take strange and unexplainable fits. What you will never prevent is that ten thousand workers remain at their places, but with their arms crossed."[44]

The crossed signals of a network become the crossed arms of labor; the "strange and unexplainable fits" that indicate a technical glitch are the paths that the wires will take absent the maintenance that labor puts into it. Though the histories of labor and telecommunications have been intertwined from the start, the former tends to drop out of its telling, and infrastructure has come to exclusively stand for computer machinery. Even as labor itself has been written out of the network's history, however, the tangled wires haunt the senders of the signals. Signals are sent to one place only to reappear elsewhere; the counselor's emergency calls travel through Atlanta to eventually get to Minneapolis. The goal of the distributed (or "self-healing") network is that circuits will automatically reroute themselves without human intervention—a design that is at the very heart of the cloud, where networks, servers, and applications alike can crash or fail without requiring intervention. But behind this is an ideology that the tangle of wire with worker can be permanently separated.

I have used the example of labor to correct a mythology that focuses on the network as a Cold War weapon against Soviet threats. But the larger issue at stake is that what I am calling the network—a way of thinking the connectedness between individual events—is always an "internal affair," a matter of thinking internal deviations. Whether this is the State Department worker suspected of homosexuality, or the worker suspected of belonging to part of a devious network, the network is always already internally focused. This is a complicated point because, again, I am using the network as a specific epistemological stance: one that, as Chun has argued, "does not respond to an overwhelming, all-seeing power but rather to a power found to be lacking—rotten and inadequate, always decaying. Paranoid knowledge similarly responds to technologies' vulnerabilities, even as it denies them."[45]

Earlier we observed that epistemological difficulty—the "very nebulous," cloudlike nature of definitions—is what led the committee to define everything as part of the network. The perfect network is where everything is connected and the network is omnipresent; "network fever" afflicts military planners and media scholars alike. This fantasy of the universal network has, at its core, the principle of deviance: of having a break or a rot somewhere in the network, of having circuits—or people—that are unreliable and

untrustworthy, of not being able to know for sure "where it goes," or who is breaking it.

What I mean by the network's nebulousness is the opacity through which any given circuit is seen, a usage that recalls the well-known phrase "the fog of war." This opacity means that the paranoid subject can't tell friend from enemy, and is threatened by that which allows friend and enemy to mix. If friend can appear as enemy and vice versa, then the paranoid subject may lash out against certain manifestations of this phenomenon. But the ultimate target of her anger is the system behind these phenomena. In other words, the paranoid subject's goal is to bring down this system. Yet to expose this system is also to unravel the system of paranoid knowledge—the connections between two seemingly unrelated persons, ideas, or events—that she has laboriously woven together. Because creating the system of connections is synonymous with exposing or unraveling the system, creating the system is synonymous with the act of pulling it apart.

But the irony, of course, is that this is a system that she has herself constructed: it is a way of mapping the external world onto an internal system of knowledge, a cognitive map that attempts to explain the world's totality. This map is deeply self-referential; at its center is a dot that always reads YOU ARE HERE, for the map is ultimately a way of translating the external world into the paranoid subject's own body. Or as Richard Hofstadter wrote in his now-classic essay on paranoia in American politics, "It is hard to resist the conclusion that this enemy is on many counts the projection of the self."[46] This is what makes paranoia a type of autoimmune disease. It would be one thing if the system were external to the paranoid subject; but the system is *her* system of knowledge. Only she can see the connections, and only she can unravel it. So what the paranoid subject seeks to destroy is something entirely internal to her; it is her worldview, indeed, her body, that is destroyed.

As rumor went, the 1961 bombing was a symptom of one branch of government attacking another. As outlandish as this fantasy was, it nevertheless revealed the paranoid logic taken to its extreme, in which the state attacks itself, as if ridding itself of its internal diseases. The paranoid principle, in which everything is connected, is intimately related to its opposite, a world where nothing is connected. In extreme cases, a paranoid system of knowledge will attack its own system of connectivity—most literally, the communications network that it had once built—in order to unravel this world of

connectivity. Paranoia, by definition, contains the seeds of both radical connectivity and radical disconnection.

Just as certain autoimmune diseases, such as multiple sclerosis, attack the body's nervous system—the body's communications network—we might expect the target of a paranoid structure of power to be its own telephone networks, or even the Internet. Theory is not intended to have predictive value, but one recent case is nevertheless suggestive. When Egypt's rulers found themselves threatened by mass protests in the winter of 2011, they dispatched the intelligence service to the Ramses Exchange in Cairo, a building that housed a data exchange for Egypt's leading Internet service providers, to shut down the Egyptian Internet. The popular media surmised that its providers were coerced through various technological weapons, such as attacking the BGP routing tables that direct Internet traffic. But it appears that the security services took a simpler approach: on January 28, 2011, at 12:28 a.m., breaker switches were thrown and routers powered down; phone calls to the providers convinced any less-connected holdouts to terminate service. (In other words, the most-connected providers were the most vulnerable to this shutdown.) Cell phone service was also cut, though it was restored the next day, and the Internet was not operational until February 2, six days later.

During those six days, many businesses could not function; banks and the stock exchange had trouble processing electronic transactions. *Forbes* later estimated that the country had lost roughly $110 million in direct revenue, including call-center jobs that were shifted to New Zealand; the total economic damage was something closer to $1 billion.[47] Warigia Bowman reported that, in the absence of the network, "people were forced to rely on traditional means of communication, including knocking on doors, going to the mosque, assembling in the street, or other central gathering places"—places such as Tahrir Square.[48] Far from tamping down the protests, the regime's Internet shutdown may have inadvertently hastened the regime's downfall.

Jacques Derrida has suggested that the common logics after 9/11, such as "terrorism," have increasingly begun to align otherwise disparate movements into a paranoid system. This paranoia, Derrida argues, is ultimately a type of autoimmune disease in which "repression . . . ends up producing, reproducing, and regenerating the very thing which it seeks to disarm": the war on terror, for example, only produces the very terrorism it is meant to eradicate.[49] It would be incorrect to consider terror a new phenomenon that has arisen since the weakening of nation-states after the Cold War. Perhaps

the first historical moment of modern terrorism, Derrida argues, was the Reign of Terror, carried out in the name of the French state. Since terror, in other words, is an integral part of how a state wields sovereign power, terrorism after 9/11 must be understood within that context.[50]

Thus when scholars write about a new form of distributed power invented to immunize us from the nuclear strike, and, more generally, from the older forms of war that it represents, something seems to go awry. The supposed immunity of the Internet instead leads to what Derrida calls "that strange behavior where a living being, in quasi-suicidal fashion, itself makes to destroy its own protection . . . its own immunity."[51] Years after the Internet supposedly immunizes us from nuclear threat, that threat returns in the form of networked viruses that target the turbines of Iranian nuclear reactors, a cyberwarfare tactic that the *New York Times* described as a first step toward "mutually assured cyberdestruction."[52]

The implication of Derrida's analysis is that the most extreme cases of repression may produce the most extreme response. Seen in this light, the Egypt case become even more interesting. Numerous commentators claimed that the so-called Internet kill switch in Egypt could never happen in more democratic and networked environments, such as the United States. Set aside, for a moment, the rather patronizing nature of these proclamations. What I want to argue is the opposite: precisely because the United States is more interconnected, it is more prone to extreme responses. Take perhaps the most networked region in the country, the San Francisco Bay Area, where proximity to the giants of Silicon Valley, such as Cisco, Google, Apple, and so forth, has caused it to be a test bed for technical and government experiments on pervasive networking.

Planners noticed one hole in the network, though: the underground, and specifically the underground transit system. The Bay Area's public transit system, BART, installed wireless antennae in underground stations as early as 2004. Later, it expanded the network to the tunnel beneath San Francisco Bay, so commuters could check their e-mail or make phone calls while crossing from San Francisco to Oakland. But the excess of network connectivity resulted in a familiar scenario. On July 3, 2011, a BART policeman fatally shot a forty-five-year old homeless man wielding a knife. A previous incident, where a white BART policeman fatally shot an unarmed African American man in 2009, had sparked region-wide protests and riots and had resulted in an eventual manslaughter conviction; this time, inflamed citizens gathered

on online message boards to discuss protest actions. This chatter made BART officials nervous. Early on the morning of August 11, the day of another planned protest, BART spokesman Linton Johnson sent an e-mail to his transit police: "A whole heck of a lot their ability to carry out this exercise is predicated on being able to communicate with each other. Can't we just shut off wireless mobile phone and Wifi communication in the downtown stations? It's not like it's a constitutional right for BART to provide mobile phone and Wifi service."[53]

Later that morning, after overcoming some dissent, BART's general manager decided to hit the kill switch. In an unprecedented move, cell phone service was shut off system-wide, from the airport through downtown stations. And tactics that had originally come from labor, sending the network into "strange and unexplainable fits," had now been co-opted by management. For contractual reasons, Verizon, Sprint, and AT&T, the three carriers then inside the BART system, were forced to comply. The protest never occurred.

One of the main rationales for the existence of BART's wireless network was that an earthquake might strike while commuters were trapped in the underwater tunnel.[54] BART deployed the network in the name of public safety and then disabled the network in the face of the protest, again in the name of public safety. The BART case may be the first in a series of autoimmune responses to network fever. Rather than reading this shutdown as a one-time exception or an overreaction, I am suggesting that it reveals something systemic about the way that paranoid imagination of networks manifests itself, when the network of Internet-enabled protesters is again conflated with the communications network. Over half a century earlier, a similar flare-up of network fever had authorities wondering whether they could cite a wartime law preventing the disruption of interstate communications to quash a San Diego labor strike against Pacific Telephone and Telegraph in 1947—because Congress had not technically declared the war over, nearly two years after V-J Day.[55] Just as labor strikes were once conflated with the invocation of war, the present moment has increasingly seen different political scenarios flattened into a sparse set of terms: war, terror, protest, network.

The logic that ties the "network of networks" represented by Al Qaeda–affiliated movements with the "cloud protesting" of Occupy, for example, is a sad reminder of this sparseness of language. What we urgently need is a richer vocabulary that captures the complexity of each social movement, a language that is less interpretive than phenomenological. To see what I

Figure 1.4
Still from Francis Ford Coppola, *The Conversation*, 1974.

mean, I offer a fictional example that captures both the extremes of paranoia and possibly a way out.

Francis Ford Coppola's 1974 film *The Conversation* tells the story of a surveillance expert who monitors other people's phone calls and picks up acoustic signals with a boom mike to reconstruct their conversations. This expert is an interpreter who pieces together the network of people supposedly involved in an assassination plot. In the final sequence, he receives a telephone call containing sounds of him alone in his San Francisco apartment, and realizes he has been deceived; he is the one who has been under surveillance (figure 1.4). The camera shows Gene Hackman tearing his own apartment apart looking for the bug, an autoimmune response to the paranoid gaze (or the paranoid ear, in this case). Hackman has hit the breaking point and crossed over to madness.

Commentators have often focused on the madness and on the camera that pans back and forth, like a surveillance camera, as some sort of morality tale: the coldness of technology, or the emotional deadness of the main character. But I'm most drawn to a minor detail, to the question of why Hackman plays a saxophone solo for the surveillance camera. I'm resistant to any claims about the ontology of jazz, but I do think that the contingency of Hackman's alto sax offers a poignant way out of the double-bind of networks and paranoia. To be clear, the music doesn't suggest a way of opting out of the network—indeed,

he plays for the camera, and, by implication, for the people watching him. On the soundtrack, there is a simple chord sequence, which Hackman hears as a sort of delusion. And we hear the sequence, too, a sign that we are also implicated in his web of paranoia. Hackman improvises to the chord sequence on the soundtrack, and as improv, there isn't a score; there isn't even a professional musician as such, since Hackman himself is playing the music as an amateur: a strange intrusion of live performance into a canned soundtrack. Hackman's character is still clearly mad; the piece he plays is a deviation, a nonlinear path. Yet he no longer follows that path to make meaning. The reason that the solo is almost completely ignored by film critics is probably because there is nothing left to interpret. It is simply an act of madness.

Instead, the solo is, like the title of this section, full of "strange and unexplainable fits." Partially released from the desire for interpretive meaning, the solo serves to produce only one thing: pleasure. And perhaps that is enough of a lesson to us. If we are not able to escape the throes of network fever, we might as well take pleasure from its deviances.

Truckstop Networks (Portola Valley, California)

Take pleasure, or at least make art. In the 1960s through the 1970s, several groups of engineers from California were trying to find an alternative to the centralized network. Not all of these engineers were working for RAND or other military-funded laboratories, however; many of them were artists. And for them, as for much of the rest of the country, the networks they were designing did not necessarily involve digital data. Instead, at that moment, *television* was the centralized system that needed to be subverted or at least radically redesigned. Network television was a monolithic schedule of programming pumped out by NBC, CBS, ABC, and, until it folded, DuMont: national broadcasters that homogenized the flow of information. The studios broadcast content to the home; information flow was a one-way street—at least before a 1969 Federal Communications Commission decision allowing community access television (CATV), better known as cable. Television delivered the network. But video and cable had the potential to hijack it.

In 1970, the same year that computer scientist John McCarthy asked whether home computer networks could lure TV viewers away from the tube with alternative sources of information, an artist group called Raindance Corporation proposed a "Center for Decentralized Television."[56] A playful

parody of the RAND Corporation's 1964 design for a decentralized digital network, its name suggested the design's paradoxically centralizing tendencies. Formed in response to news that the RAND Corporation had begun to study cable networks (or, as one contributor speculated, was developing mind-control techniques), the video collective wrote: "We believe culture needs new information structures, not just improved content pumped through existing ones," and their unrealized "Center" would have served as a regranting agency for video artists.[57] An early issue of the collective's newsletter, *Radical Software*, suggests the thrill of imagining new information structures: the typography of Frank Gillette's piece, "Loop-de-Loop," depicts arrows twisted to form loops that lead nowhere. Claude Ponsot illustrates an article about the structure of cybernetics and guerilla tactics with whimsical mathematical diagrams dubbed "Klein worms," after the topologically impossible Klein bottle. We are still within the ballpark of Baran's network diagrams, but just barely (figure 1.5).

These earlier moments of reconfiguring the network structure hold uncanny parallels to modern-day digital networks. The first page of *Radical Software*'s first issue is an excerpt from Gene Youngblood's book, *The Videosphere*; a later advertisement summarizes his book as a description of a "single unified system, a 'decentralized feedback communication network'" that would unite five different mediums: cable TV, portable video, storage networks, "time-shared computer utilities," and "the domestic satellite system." Youngblood's videosphere is often understood metaphorically, as a reiteration of Marshall McLuhan, but here Youngblood turns his attention to specific networks: the FCC's decision to allow MCI (then called Microwave Communications Inc.) to compete with AT&T by renting CATV circuits; a "'quasi-laser' broadcasting system . . . [that] transmits up to 15 miles," a technology pioneered by MCI that will anticipate fiber-optic cable; the US Defense Department satellites, along with Soviet and the commercial Comsat networks. Youngblood's union of heterogeneous networks is eerily similar to the union of satellite, land, and radio networks that was dubbed, five years later, the Internet. Add in the "time-shared computer utilities" and storage networks (considered in the next two chapters), and you have the cloud.

Excited by the potential of this new technology, the late 1960s and early 1970s became a test bed for questions that would preoccupy network culture: If you could design a two-way, "feedback network," could you even out the structures of power and create a more participatory media environment?

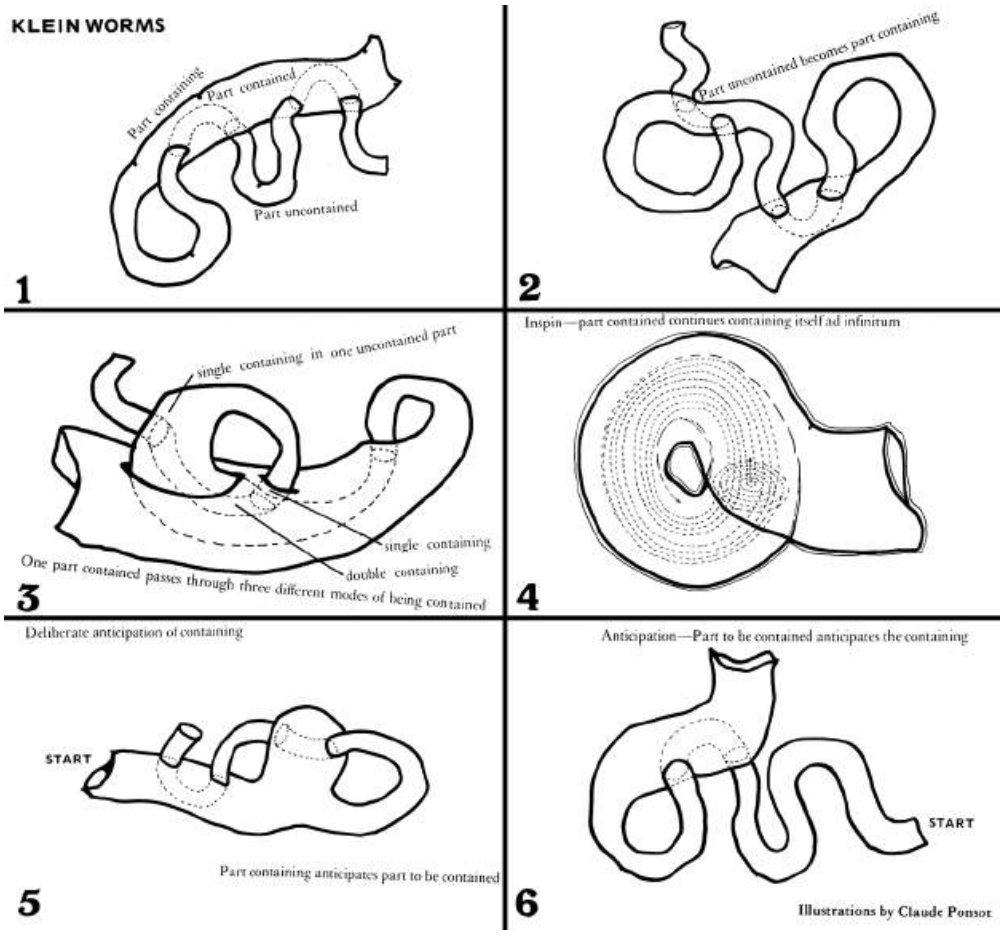

Figure 1.5

Paul Ryan and Claude Ponsot, "Klein Worms," in *Radical Software* 1, no. 3 (1971); Labadie Collection, University of Michigan Library.

And if you could change the media, would its viewers see differently? These are large questions, but ones that have lost their potency over time because so many of these structures have come into fruition: viewers feed back images and videos to television shows all the time, as with citizen-generated videos that regularly air on CNN, and YouTube has become an even more eclectic repository for images than cable ever was. We take distributed networks, and their properties, such as two-way interaction, for granted; the rhetoric of the artists is too utopian to be taken as more than a product of its time. And as David Joselit reminds us, while video and cable may be a "cautionary tale regarding the Internet's claims as a site for radical democracy," it is an embarrassing lesson to learn—particularly given how quickly cable, like the Internet, became commercialized and assimilated into the system of power it once claimed to subvert.[58]

These artistic attempts to critique and reconfigure the network of television at the same time as ARPAnet and the Internet suggest that a larger, generalizable discourse about networks was at play in the late 1960s and early 1970s, and that it wasn't limited to computers and digital technology. Essayist Joan Didion aptly summed up the massive social upheaval in the late 1960s by invoking Yeats: "The center was not holding."[59] Despite a smoothly functioning marketplace and a high GNP, the gravitational pull of these economic mechanisms no longer seemed enough. That decentralized networks were created in response—whether as alternatives to the centralized system of information distribution, or as buttresses meant to uphold the center by dispersing its power—does not strike me as a coincidence.

While the publics of the Internet were not yet present in the early 1970s, the publics created by television—the network user, here understood as a viewer of television and video—nevertheless registered the shifts in the network's shape. For the advent of new media in the late 1960s and early 1970s was felt primarily as the advent of news media—for instance, recall news reports from the 1972 Democratic and Republican National Conventions by the amateur group TVTV (Top Value Television), wielding the new Sony handheld video recorders named Portapaks. We tend to lose sight of this because a scholarly focus on the specificity of the network's *mediums* (its wires or logics or apparatus) has led to its inevitable separation from the network's *media*, the sense of mass or communications media.[60] To recuperate this larger discourse of the network, I turn to one of *Radical Software*'s collaborators, the San Francisco–based collective Ant Farm (Chip Lord, Doug Michaels, Hudson Marquez, and Curtis Schreier). Ant Farm's proposal for a media distribution structure called a "Truckstop Network" allows us to see how fertile the ground was for alternate network structures. The caveat is that my abbreviated consideration of a single Ant Farm project misses not only the rest of their work, but also contemporaneous examples from the rich history of video, such as artist Dan Graham's "feed-forward" cable network (ca. 1972); Austin Community Television (ACTV, 1972–), which fed directly into the cable's "head-end," or distribution center; Stan VanDerBeek's live performance/call-in piece for WGBH-Boston, *Violence Sonata* (1970); or the Videofreex pirate TV station in the Catskills, Lanesville TV (1972–1977), that attempted to hack or reconfigure the shape of the network system. For interested readers, I direct them to books that take up this subject in more depth.[61]

With this caveat in mind, let us move to 1970, when a modified Chevrolet van with a clear plastic bubble and a distinctive antenna hit the road. Serving as Ant Farm's temporary home for a year, it contained a TV window, a videotape setup, silver roof-mounted speaker domes, and a dashboard-mounted camera, all hardware "reminiscent of a B-52."[62] It was quickly named the Media Van, and it became an integral part of what they eventually dubbed the Truckstop Network. Ant Farm bought several of the new Portapaks and went on tour, stopping at several colleges, shooting video of "dancing chickens, an okra farmer, a ground-breaking in Scottsdale, aspiring pop singer Johnny Romeo belting out a ballad in the Yale School of Architecture."[63] If commercial television refused to broadcast these video images, the Media Van would bring the network directly to the audience's door.

This van drove off during a moment of transition for highway culture. Through the 1960s, Jonathan Crary argues, the automobile and the television worked hand-in-hand in popular culture to conceal the growing complexity of capitalist representation. A highway route had an effect much like television, acting as a sort of TV channel that seemed to enable a driver/viewer's autonomy by giving him or her the power to choose—even as it cloaked the mechanism of capital behind it.[64] In the 1970s, Crary continues, television "began to be grafted onto other networks . . . the screens of home computer and word processor," and the computer's window replaced the car's window as the predominant space of the virtual.[65] Though the ideal of car culture had begun to sour—a matter brought to a head by the 1973 oil crisis—it was precisely the highway's identification with Cold War surplus and rusted roadside attractions, and its lack of newness, that made it fertile ground for artistic reappropriation.[66]

Thus Truckstop Network was more than a road trip tour; it was also a statement about mobility itself. Standing on the hinge between auto window and computer window, it proposed a countrywide network of truck stops for "media nomads." Placed just off the highway, each truck stop would offer an array of services for those living on the road: housing, electricity, and water; truck repair and a communal kitchen; and also communications services—computers and video equipment—seen, "like food and gas, as nutrients necessary for survival."[67]

Indeed, the computer aspect was essential to this plan: not only would it link all the truck stops, or "nodes," in Ant Farm's parlance, into a nationwide "communication network," but it would also direct the visitor to the services

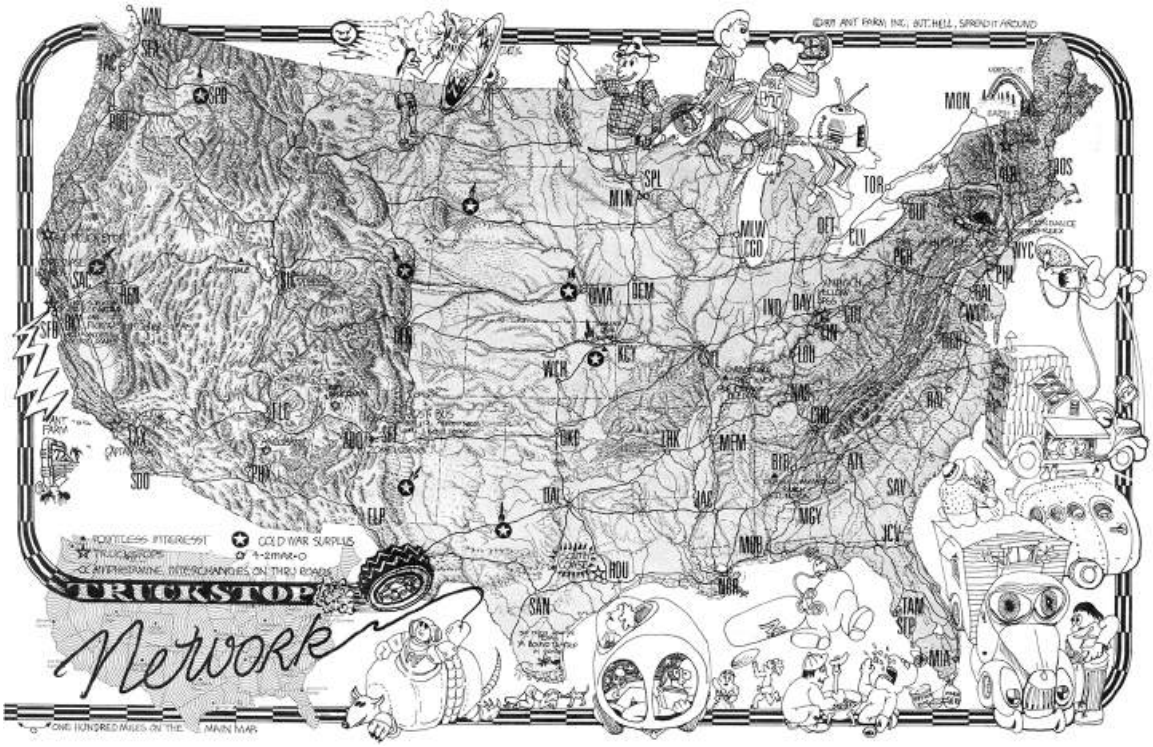

Figure 1.6

Ant Farm, *Truckstop Network Placemat* (recto), 1971, Ant Farm, offset printing on paper (2-sided); 17 × 11 in.; University of California, Berkeley Art Museum and Pacific Film Archive. Photo: Benjamin Blackwell. © Ant Farm. Courtesy of Chip Lord.

available at other truck stops—a woodworking shop, or astrology lessons, for example.[68] Truckers could be sent to other nodes via several highway directions; a placemat passed out to audiences on the Ant Farm tour maps several of these cross-country routes, including the "Overland Route" (Chicago to Salt Lake City to San Francisco Bay) and the "Sunset Route" (Los Angeles to New Orleans) (figure 1.6). On the flip side of the placemat, a star identifies potential Cold War surplus sites that could be reused as nodes, an act of reappropriating what Mark Wasiuta describes as the nation's "expanding computerized military network and its underground command centers."[69] A sketch for one of these sites, identified as a former desert missile silo near Wendato (likely Wendover, Utah), contains plans to transform layers of the silo into various layers for maintaining software (film/video) and hardware (auto/bus), all wired via a solar dish to its nervous system/core.[70]

For Ant Farm, the interconnections turned each node into a "physically fragmented . . . 'city'" of media.[71] Distributed across the country in places

where "land is cheap and codes are lax in between the cities"—one thinks of the arid wheat field in Amarillo, Texas, where they executed their most famous piece, Cadillac Ranch, or the California deserts where they set up inflatable structures—the Truckstop nodes would be connected by the simplest yet most robust piece of Cold War infrastructure, the interstate highway.[72] And by placing the nodes at the side of the highway, it was possible to build an existence where the journey was the destination, and where the motion of the network was the point of the network. Cars traveling between the nodes thus became packets; remaining in constant motion, each packet would not stop at one node for long before traveling to another node. In other words, packet-switching.[73] Without a centralized node (although at one point Ant Farm envisioned a central computer to direct traffic), the network would constantly move information from point to point while avoiding the concentration of information in any one place. Moreover, the nodes were cheap, inflatable, and flexible. In effect, Ant Farm had envisioned an anarchic, distributed network for mobile living.

We may be tempted to dismiss this plan for "mobile living" as New Age artist cant. But Truckstop Network articulated an idea of mobility that would soon profoundly shape cloud computing. For the first Internet protocol was not developed through ARPAnet, as one might expect, and as most network historians claim, but through the physical act of driving on the open road. With its fixed nodes of bunker-sized computers and fixed links, ARPAnet was the quintessential piece of "closed-world" infrastructure. Instead, military researchers envisioned soldiers going mobile. Though there is no evidence that researchers at the Stanford Research Institute (SRI) saw any of Ant Farm's media productions, they nonetheless shared a similar vision: media would need to be produced and consumed on the road.

For SRI's engineers, this meant retrofitting a "bread truck" style van to test the difficulty of broadcasting and receiving network signals on the move. They wanted to see if, for instance, their packet radio connection would remain intact if the van went under a highway overpass.[74] (Packet radio is an early version of today's cellular networks.) Rigged on the inside with a DEC LSI-11 computer and two packet radio transmitters, the SRI van (figure 1.7) ran its first successful test in August 1976, six years after Ant Farm's own Media Van (figure 1.8). The test was of a protocol that would bridge the aerial network—the Packet Radio Network, or PRnet—with the ground-based ARPAnet. It was the first time two disparate computer networks were

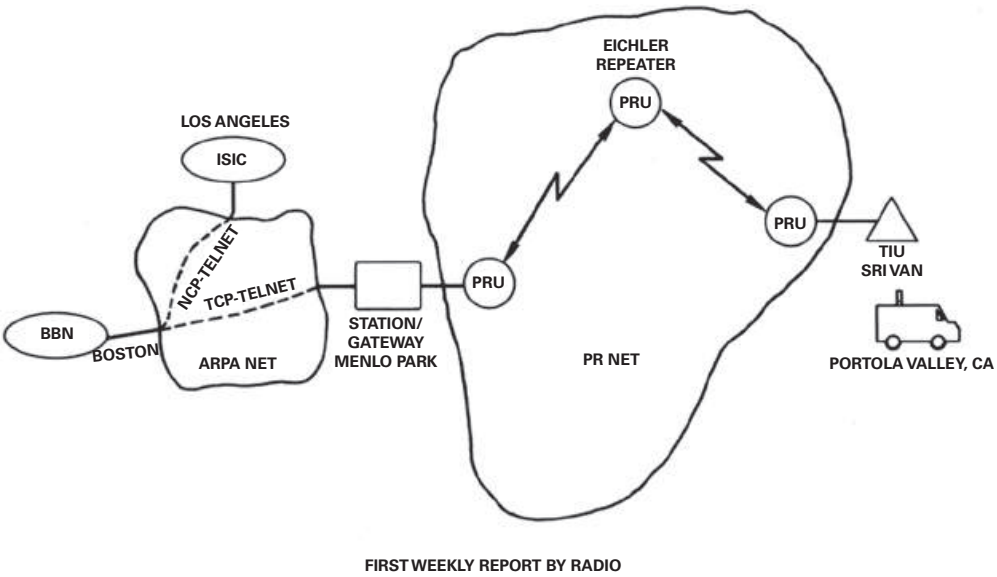

Figure 1.7

Diagram of first two-network Internet transmission, August 27, 1976. Originally published in "Progress Report on Packet Radio Experimental Network," September 1977. © SRI International, Inc. Used with permission.

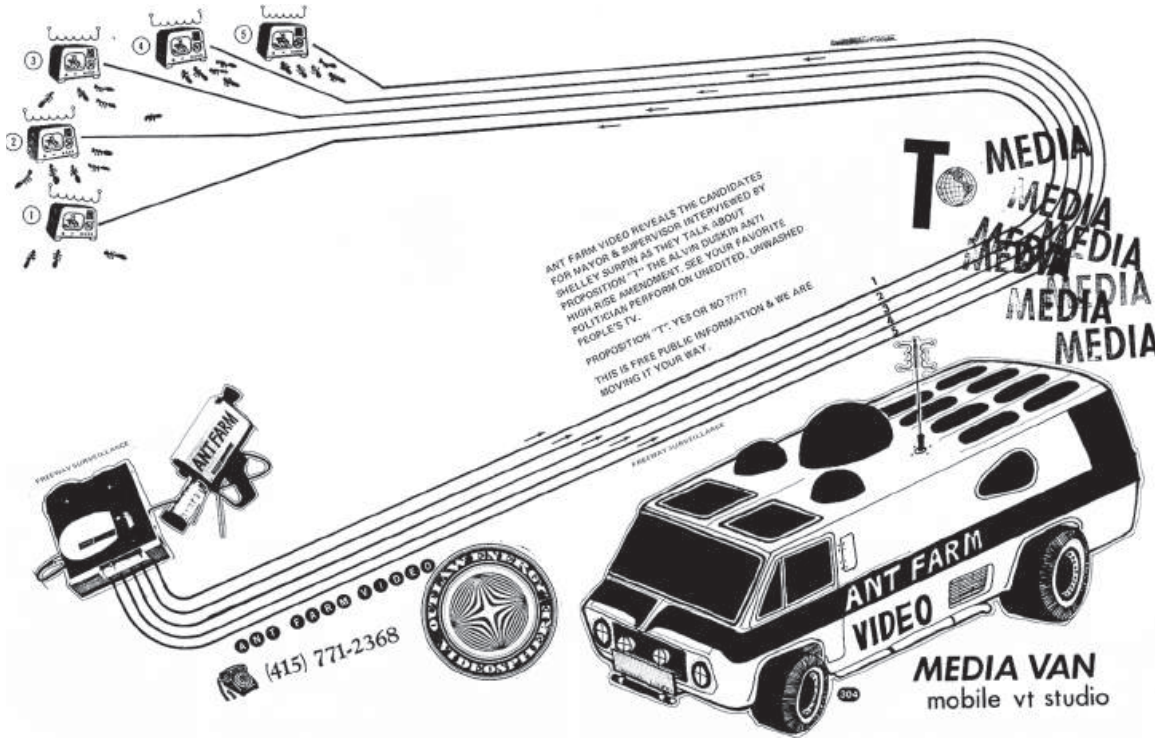

Figure 1.8

"Media Van: mobile vt studio," 1971, Ant Farm; ink, stamp marks in black ink, sticker, and collage elements on paper; 11 × 17 in.; University of California, Berkeley Art Museum and Pacific Film Archive. Photograph: Benjamin Blackwell. © Ant Farm. Used with permission.

bridged, and as a result, it is considered the first inter-network, or Internet, transmission.

In this inaugural test, the van is clearly visible on the right side of the network diagram, connected to two clouds labeled PR NET and ARPA NET. What is perhaps missing from the diagram is the texture of the setting, of the van's driver—protocol engineer Jim Mathis—trucking down Northern California's Bayshore Freeway, and the van's final stop, which was chosen because it was a "'hostile environment'—in keeping with relevance to military application": "This was the parking lot of Ross[o]tti's biker bar in Palo Alto, still well in reach of the repeater units at Mt. Umun[h]um and Mission Ridge—and with good supply of local bikers who gave the appearance of hostility after the requisite number of beers."[75]

There is an improvisatory aspect to SRI's van test. The inter-network they built was by definition an "amalgam of wire and radio networks"; it was a way of allowing a highly mobile, even ethereal network—packet radio—to tap into a preexisting, fixed network infrastructure.[76] The van also reveals a third infrastructure that is only implicit: the highways in what is now known as Silicon Valley where the researchers circulated to test their van, which also delighted the bikers and video freaks with whom they mingled. A few miles down the street from Rossotti's, you could buy a catalog containing Ant Farm's latest inflatable architecture projects or video schematics from the "Whole Earth Truck Store." The first node on the intermedia network was a truck stop, or, in the case of SRI, a biker bar.

The two media vans soon went into storage, SRI's to a forgotten back lot, Ant Farm's to a bunker in Marin County, California. But the inter-networking protocol tested in 1976, TCP, would cement the growth of what would be christened the "Internet" in 1983, and the networks' shapes would resemble the possibilities—the freedom of the road; a constantly moving, physically fragmented existence—once offered by the highway. No matter that American highway culture itself had gone into decline. The potentialities that the highway once represented—the idea of the highway without the highway itself, simultaneously decentralized and yet an infrastructure from the Cold War—remained.

The "information superhighway" articulated a new kind of lifestyle, where media processors could go mobile, feeding information (often in the form of video) back into the cloud. Yet the shift from the media of the van to digital media was not a particularly hard one to envision. In "Truckstop

Fantasy Number One," Ant Farm had even mused that "EVENTUALLY WE WILL ABANDON PHYSICAL MOVEMENT FOR TELEPATHIC/CYBERNETIC MOVEMENT (TELEVISION) AND OUR NETWORK WILL ADAPT TO THE CHANGE."[77] For Ant Farm, computer links were merely one of many forms of communication, and the specific medium (telepathy or television!) was somewhat beside the point. In the bottom of their network diagram for Truckstop Network, Ant Farm asks: "How many ways do you communicate/inter truckstop."[78] And then they list "linear" mediums, such as the mail, next to "electronic" mediums (radio and telegraph and computer) and land and aerial transportation mediums (cars, trucks, blimps). A single anomalous dotted line in a mesh network appears to indicate, of all things, a telegraph line.

The inspiration for Truckstop Network was as much the new technology of the Sony Portapak as the well-worn technology of the postal service. As Chip Lord recalls, "Before we went on the road, we were doing mail art and we tapped into this network of people doing mail art."[79] Kris Paulsen has additionally uncovered a buried history of guerilla television within its lo-fi distribution network: videographers swapped half-inch videotapes by advertisements and mail order.[80] The point is that the cloud is always an amalgam—a "network of networks"—that can only come into existence when it is not tied to a specific network or medium. This is why there are multiple clouds in the SRI diagram, and even some internal debate at SRI on how many networks—two or three—are needed before the project can officially be termed an "inter-network."

To think about the digital network, I am arguing, one must first think about the network in the absence of individual technologies. This is what I have tried to do with the example of the two media vans. In the late 1960s and early 1970s, the rhetoric behind the creation of new information structures was often overblown; the utopianism of their claims are so sweeping that they are sometimes hard to take seriously (Youngblood's videosphere that envisioned an "Intermedia network" that will unite all media). But we dismiss their rhetoric at our own risk. Strip away the technological layer—the artists' concern with television, for example—and we see something very similar to what we have now: the cloud as a place where all media seem to converge; the cloud as an enabler of supposedly distributed publics.[81] The universalist fantasy of the cloud remains as ubiquitous now as it was forty years ago.

There is a second reason why I have brought the vans into the story. If we only imagine the network as a product of the military, working with their contractors, to "invent" ARPA and the Internet, then the network that we take away is a deeply paranoid one—a vision of nuclear strikes and distributed tanks. There is a hole in that narrative. By their own admission, the engineers at SRI were trying to convince the military that their interests in packet radio could eventually have a military application. Inside the van were several other projects, including a computer program for encoding speech run by the "Network Speech Compression and Network Skiing Club," that reflected a more utopian heritage within SRI of using computers to augment human capabilities. Yet the story they told to the military is the one that is inevitably retold by computer historians.

Precisely because many of the claims in the late 1960s and early 1970s are strange—precisely because they are unexplainable—is grounds for why we should embrace them. SRI used a Mickey Mouse phone inside its van to test phone service over the packet network; this research in digital speech resulted in the decidedly unmilitary Speak & Spell toy for children. Meanwhile, Ant Farm sketched an ink diagram of Television America, its primetime audience reimagined as a slice of prime—prime meat, that is. In their specificity, in their improvisatory strangeness, they rub against the grain of universalism. A dancing chicken broadcast from the Media Van undercuts any sort of sweeping claims for a new Media America. By their very refusal to be assimilated into useful categories for Internet history, they stake out a space for the autonomy of their production. In contrast to understanding network culture as a paranoid world system, one that encompasses all networks, these weird and unexplainable moments offer the potential for an alternate, reparative reading.[82]

It is unknown whether the video freaks and the network engineers in Portola Valley rubbed shoulders over a beer at Rossotti's, though Ant Farm did visit the Xerox PARC archives in the early 1970s to research an upcoming exhibition. In either case, there was a rich relationship between the counterculture and computer scientists of the San Francisco Bay Area. Theodore Roszak and John Markoff have identified a shared interest in political dissent, communalist, and consciousness-expanding practices by members of the counterculture and computer researchers living in San Francisco and the Stanford area, respectively.[83] And as Fred Turner has shown, Stewart Brand served as a key hinge between the two worlds, acting as a cameraman during

Douglas Engelbart's 1968 demonstration of personal computing, and as a publisher of the seminal Whole Earth Catalog (an outgrowth of the Whole Earth Truck Store)—a kind of World Wide Web in print that indirectly led to the establishment of the Berkeley Homebrew Computer Club.[84]

These histories, however, typically trace inventors and researchers within or on the peripheries of computer science. As I have tried to show, network culture properly resides in a vibrant debate—one that preceded the 1960s, and continues to this day—about the proper configuration between media and power. Computer scientists were a part of this debate, but they were not the only ones to weigh in. Years before ARPAnet's existence, sociologists, urban planners, government bureaucrats, privacy advocates, epidemiologists, computer scientists, and, of course, the aforementioned artists, were keenly aware of the centralizing tendencies of networks. Would the computer network become a "natural monopoly," like all of its predecessor utilities, asked Baran in a 1966 Congressional hearing, and if so, how might concentrating data inside such computer monopolies affect privacy?

The next chapter tells the story leading up to that first federal hearing on computer privacy, and the effect it had on shaping what we now call cloud computing. Before I turn to that story, which begins just across the Stanford campus from the SRI engineers, it is worthwhile to remember that similar questions had already begun to percolate in the fierce debates over television. Only five years earlier, Newton Minow, the incoming FCC commissioner, warned about television's monopoly over its viewers in his famous "wasteland" speech by describing the flatness of television: "You will see a procession of game shows, formula comedies about totally unbelievable families, blood and thunder, mayhem, violence, sadism, murder, western bad men, western good men, private eyes, gangsters, more violence, and cartoons . . . And most of all, boredom."[85] This distaste builds to the commissioner's larger point: "I am deeply concerned with concentration of power in the hands of the networks." The network was then, as it is now, a potent manifestation of aesthetic questions. Aesthetic—which is to say, political.