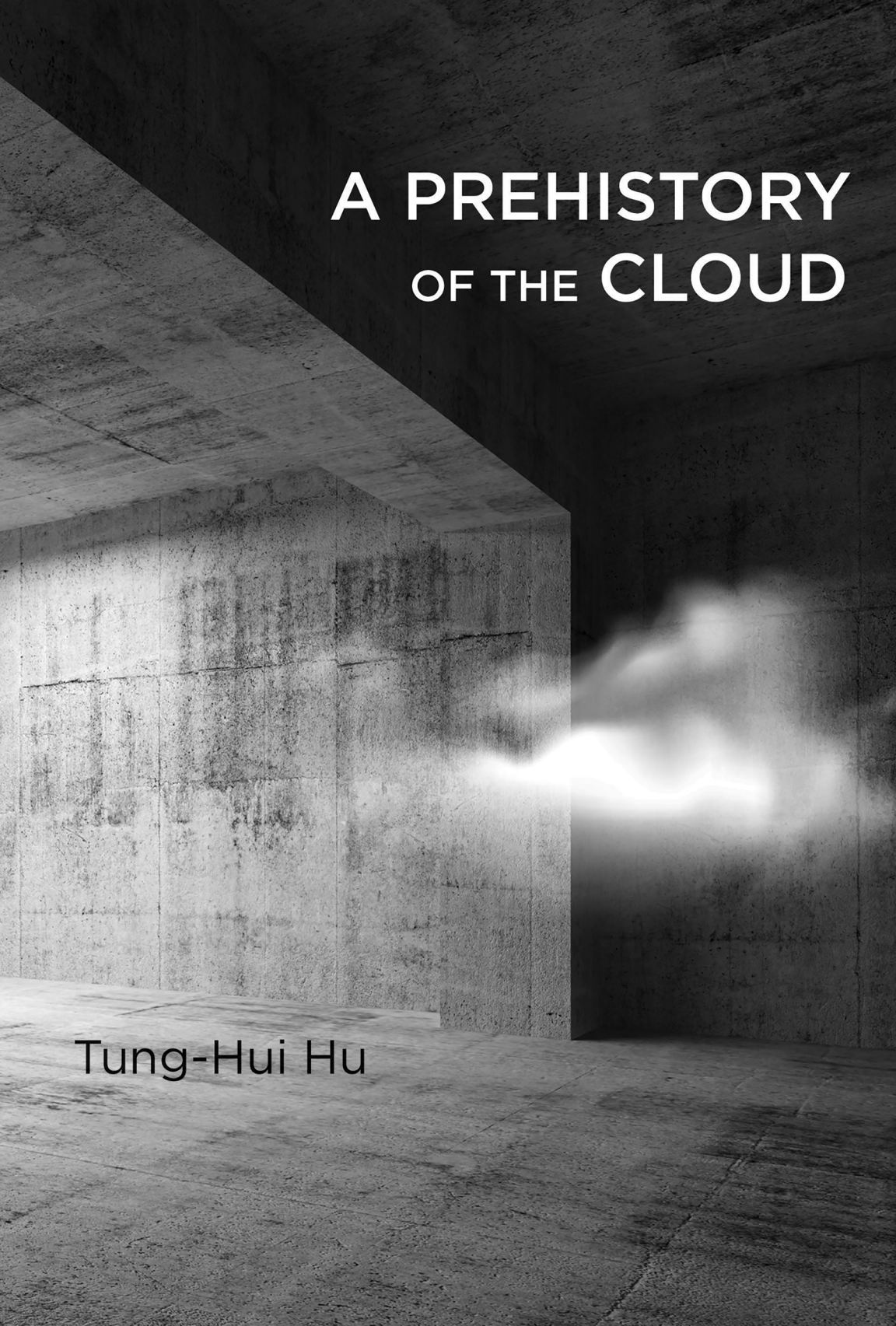
A PREHISTORY
OF THE CLOUD
Tung-Hui Hu

A PREHISTORY OF THE CLOUD

A PREHISTORY OF THE CLOUD

Tung-Hui Hu

The MIT Press
Cambridge, Massachusetts
London, England

This book was set in Gentium 10/14pt by Toppan Best-set Premedia Limited. Printed and bound in the United States of America.

Library of Congress Cataloging-in-Publication Data

Hu, Tung-Hui, 1978–
A prehistory of the cloud / Tung-Hui Hu.
pages cm
Includes bibliographical references and index.
ISBN 978-0-262-02951-3 (hardcover : alk. paper) 1. Computer networks—History—Popular works. 2. Internet—Social aspects—Popular works. I. Title.
TK5105.5.H79 2015
004.6—dc23

2015001899

10 9 8 7 6 5 4 3 2 1

CONTENTS

ACKNOWLEDGMENTS

Portions of this book were written while at the Michigan Society of Fellows and at the Stanford Center for Advanced Study in the Behavioral Sciences. Many units of the University of Michigan provided research funding and advice, including the Horace H. Rackham School of Graduate Studies, the Department of English, the University of Michigan Library, the Office of Research, and the College of Letters, Sciences, and the Arts. I thank these organizations for their support.

This book is for my correspondents: Megan Ankerson, Finn Brunton, John Cheney-Lippold, Victor Mendoza, and Lisa Nakamura. Thanks to Katy Peplin, whose work as a research assistant helped take this project in new directions. Ben Lempert's editorial advice has been indispensible and transformative. Karen Beckman, Linda Williams, Kaja Silverman, and Anne Wagner provided the intellectual scaffolding for this study—hopefully invisible to the reader, yet deeply felt nonetheless. Doug Sery, Susan Buckley, and Kathleen Caruso at the MIT Press brought this project to fruition. I'm grateful to the generous colleagues who read and commented on drafts of this book, including Sara Blair, Jonathan Freedman, Ilana Gershon, Roger Grant, Jeffrey Todd Knight, Petra Kuppers, Erica Levin, Kris Paulsen, Dan Rosenberg, Polly Rosenwaike, Ruby Tapia, Terri Tinkle, Damon Young, and Genevieve Yue; thank you. Last, for being there through the ends, and thus the beginnings: Elizabeth Bruch.

INTRODUCTION

Like the inaudible hum of the electrical grid at 60 hertz, the cloud is silent, in the background, and almost unnoticeable. As a piece of information flows through the cloud—provisionally defined, a system of networks that pools computing power[1]—it is designed to get to its destination with "five-nines" reliability, so that if one hard drive or piece of wire fails en route, another one takes its place, 99.999 percent of the time. Because of its reliability and ubiquity, the cloud is a particularly mute piece of infrastructure. It is just there, atmospheric and part of the environment.

Until something goes wrong, that is. Until a dictator throws the Internet "kill switch," or, more likely, a farmer's backhoe accidentally hits fiber-optic cable. Until state-sponsored hackers launch a wave of attacks, or, more likely, an unanticipated leap year throws off the servers, as it did on February 29, 2011. Until a small business in Virginia makes a mistake, and accidentally directs the entire Internet—yes, all of the Internet—to send its data via Virginia, and, almost unbelievably, it does. Until Pakistan Telecom inadvertently claims the data bound for YouTube. A multi-billion-dollar industry that claims 99.999 percent reliability breaks far more often than you'd think, because it sits on top of a few brittle fibers the width of a few hairs. The cloud is both an idea and a physical and material object, and the more one learns about it, the more one realizes just how fragile it is.

The gap between the physical reality of the cloud, and what we can see of it, between the idea of the cloud and the name that we give it—"cloud"—is a rich site for analysis. While consumers typically imagine "the cloud" as a new digital technology that arrived in 2010–2011, with the introduction of products such as iCloud or Amazon Cloud Player, perhaps the most surprising thing about the cloud is how old it is.[2] Seb Franklin has identified a 1922 design for predicting weather using a grid of "computers" (i.e., human

mathematicians) connected by telegraphs.[3] AT&T launched the "electronic 'skyway'"—a series of microwave relay stations—in 1951, in conjunction with the first cross-country television network. And engineers at least as early as 1970 used the symbol of a cloud to represent any unspecifiable or unpredictable network, whether telephone network or Internet.

Figure I.1 provides an early example. Drawn by Irwin Dorros, director of network planning for AT&T, this diagram utilizes a series of three clouds to describe the network behind AT&T's new Picturephone service. Previously, network maps had been drawn as block diagrams—a series of boxes indicating either the exact telephone circuit or at least the possibility of finding the exact circuit. But Picturephone, a primitive videoconferencing system, was one of the first applications that worked across a mixture of analog and digital networks. Because Picturephone would operate regardless of the type of physical circuit underneath, Dorros illustrated the boundaries of the networks as an amorphous form.[4]

What we learn from the diagram is simple: the cloud's genesis was as a symbol. The cloud icon on a map allowed an administrator to situate a network he or she had direct knowledge of—the computers in his or her office, for example—within the same epistemic space as something that constantly fluctuates and is impossible to know: the amorphous admixture of the telephone network, cable network, and the Internet. While the thing that moves through the sky is in fact a formation of water vapor, water crystal, and aerosols, we call it a cloud to give a constantly shifting thing a simpler and more abstract form. Something similar happens in the digital world. While the system of computer resources is comprised of millions of hard drives, servers, routers, fiber-optic cables, and networks, we call it "the cloud": a single, virtual, object. To do so not only make things easier on users and computer programs, but also allows the whole system to withstand the loss of an individual part. (Most of the time, anyway.)

As a result, the cloud is the premier example of what computer scientists term virtualization—a technique for turning real things into logical objects, whether a physical network turned into a cloud-shaped icon, or a warehouse full of data storage servers turned into a "cloud drive." But the gap between the real and the virtual betrays a number of less studied consequences, some of which are benign and some of which are not. One's data trail grows with each website one visits and each packet one sends through the cloud. The results are used by both marketing companies trying to target an online ad

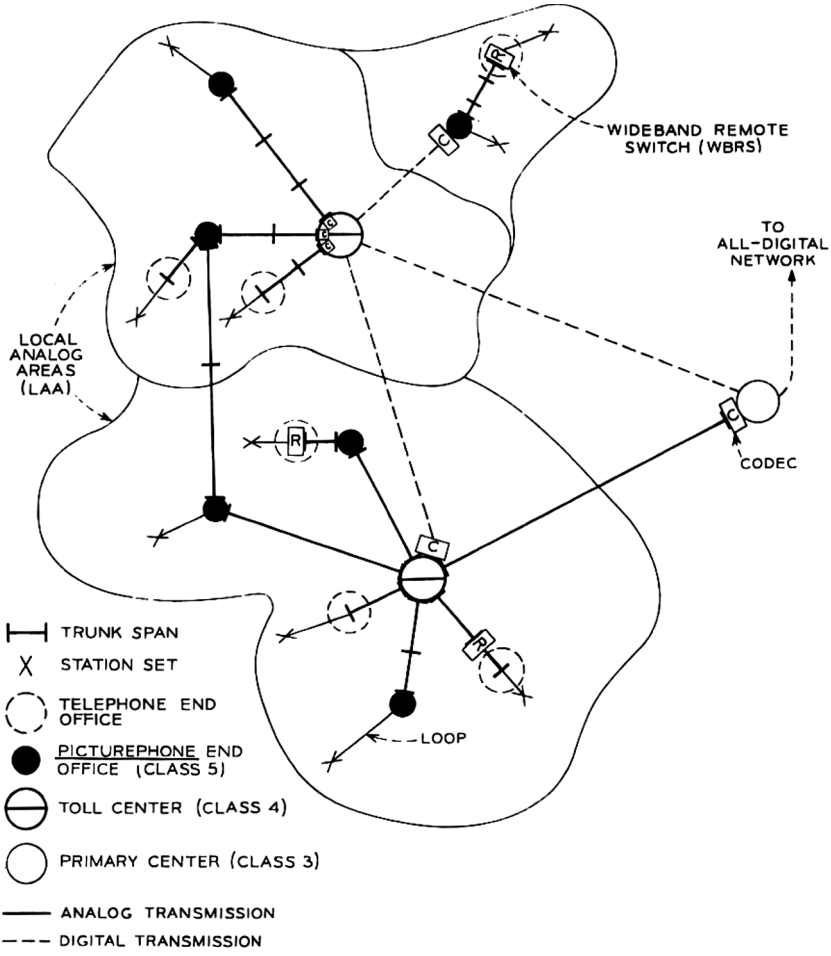

Figure 1.1

Illustrative local area configurations. *Source:* Irwin Dorros, "The Picturephone System: The Network," *Bell System Technical Journal* 50, no. 2 (February 1971): 232. © 1971 The Bell System Technical Journal. Reprinted with permission.

for, say, auto insurance, and government agencies trying to target terrorists for extrajudicial killings. We tend to perceive the two kinds of targeting as separate because online privacy appears to be a born-digital problem that has little to do with geopolitics. That gap, then, is crucial. The word "cloud" speaks to the way we imagine data in the virtual economy traveling instantaneously through the air or "skyway"—here in California one moment, there in Japan the next. Yet this idea of a virtual economy also masks the slow movement of electronics that power the cloud's data centers, and the workers who must unload this equipment at the docks.[5] It also covers up the Third World workers who invisibly moderate the websites and forums of Web 2.0, such as Facebook, to produce the clean, well-tended communities that Western consumers expect to find. By producing a seemingly instant, unmediated relationship between user and website, our imagination of a virtual "cloud" displaces the infrastructure of labor within digital networks.

This book is an attempt to examine what occurs in the gap between the real and the virtual. In this it offers two interrelated stories. On one hand, *A Prehistory of the Cloud* tells the story of how the cloud grew out of older networks, such as railroad tracks, sewer lines, and television circuits, and often continues to be layered on top of or over them. Today, of course, the cloud has become so naturalized in everyday life that we tend to look right through it, seeing it uncritically, if we see it at all.[6] To make this historical infrastructure more visible, this book turns back the clock to the clumsy moments when the cloud was more of an idea than a smoothly functioning technology. It examines a series of cultural records and events that shaped the cloud's "prehistory," including a group of microwave relay stations sabotaged near Wendover, Utah, in 1961 that sparked a furious debate about what a network actually *is*; a 1946 comic strip, *Bobby Gets Hep*, produced by AT&T that taught children etiquette for party lines and therefore helped construct our modern notion of privacy; and the US government's announcement of a National Data Center, a 1966 proposal deemed so dangerous to society that one scientist likened it to the development of a nuclear weapon.

Using these examples, the book tells a second story about the politics of digital culture. When commentators describe the nebulous Occupy Wall Street movements, the workings of global capitalism, the web-mediated resistance movements comprising the Arab Spring, and Al Qaeda and Associated Movements (AQAM) all as "cloudlike," or as "a network of networks," it

is clear that the cloud, as an idea, has exceeded its technological platform and become a potent metaphor for the way contemporary society organizes and understands itself.[7] Responding to this shift, communications and media scholars have attempted to theorize the new forms and structures of power that result from networked societies.

One traditional model of explaining political power is known as sovereignty. Consider a hypothetical kingdom, in which its sovereign can coerce his subjects into doing what he wants. Power here is top-down: centralized in the throne room, it radiates out to the borders of the king's territories. Further, sovereign power is framed in the negative: it can punish unruly subjects, prohibit certain practices, and, in the most extreme cases, confiscate a subject's life. While many modern democracies no longer have monarchs, they nevertheless retain some aspects of sovereign power. The United States, for example, has clearly defined borders; it centralizes power into clearly defined federal institutions and agencies, such as the White House and the FBI; and many of those agencies exist to prosecute or punish violations of the law. Yet the Internet puts pressure on this model of power. In one case, the US government attempted to limit the export of strong encryption software, only to be confounded by a proliferation of foreign websites—easily accessible by US users—offering that software for free download. Explaining this difficulty, legal scholar James Boyle writes that digitally dispersed, transnational networks always exceed a sovereign state's ability to "regulate outside its borders . . . We are sailing into the future on a sinking ship. This vessel, the accumulated canon of copyright and patent law, was developed to convey forms and methods of expression entirely different from the vaporous cargo it is now being asked to carry."[8]

Boyle and his contemporaries use sovereign power as an example of what digital networks make obsolete. Yet, counterintuitively, what this book argues is that "the cloud" also indexes a *reemergence* of sovereign power within the realm of data. Sovereign power may seem worlds away from the age of the Internet, particularly given its antiquated elements, such as the monarch's power to arbitrarily kill. Algorithms and users seem to be running the world online, rather than there being a central decision maker; further, a topography of power based on borders or territories, instead of networks, seems out of date.[9] Indeed, the incongruity has caused media scholars to develop two main alternate models of power, which I explain below; I then return to why the cloud may actually effect a return to sovereignty.

Initially, scholars of surveillance and media turned to Michel Foucault's model of *disciplinary power*, which replaces a single source of power, the sovereign, with a series of institutions, such as a factory, prison, school, hospital, or even the family, through which power can be exercised and subjects managed. Disciplinary power is far less coercive than sovereignty; it instead operates according to a set of norms and rules. A school, for example, educates its pupils and in so doing produces certain formations of knowledge and self-understandings of what constitutes "good behavior." The school organizes pupils by classroom, grade, and daily schedule; evaluates each pupil through testing; and, occasionally, attempts to reform a wayward student by issuing detention. Disciplinary power, then, works as a kind of surveillant gaze, under which subjects internalize behavioral standards, learn to order their bodies, or are supervised through other social mechanisms. In his perhaps most quoted study, Foucault mobilizes Jeremy Bentham's 1791 design of a prison called the Panopticon to analyze a condition in which, as Foucault writes, "a state of conscious and permanent visibility . . . assures the automatic functioning of power."[10]

While the Internet is certainly a space of radical visibility—each and every packet of data that passes through the US Internet may be inspected by the National Security Agency, one aspect of surveillance that has led to Panopticon-like comparisons—digital networks complicate many other aspects of this theory. In the cloud, for example, there is seemingly no set of behavioral norms, hierarchies, or enclosed spaces, and any institutions involved in managing users seem purely incidental; the closest, it would seem, are Internet protocols, rather than organizations. And as computer networks seem to have become decentralized and distributed, power, too, seems to have become distributed on a microscopic level. For these reasons, over the last ten years, scholars of new media have generally coalesced around a second model: the *control society*.[11] If Foucault originally described a shift from sovereign societies to disciplinary societies, Gilles Deleuze extended this shift into a third phase, in which subjects are governed by invisible rules and systems of regulation, such as our credit scores, web history, and computer protocols. As Deleuze puts it, prisons and other disciplinary institutions are subsumed by these mechanisms of control: "Everyone knows these institutions are finished, whatever the length of their expiration periods. It's only a matter of administering their last rites and of keeping people employed until the installation of new forces knocking at the door."[12]

As an example of Deleuze's idea of the control society, consider the credit card. There are often no preset spending limits associated with the card, and because a computer determines whether a particular transaction is fraudulent by comparing it to the charges the spender usually makes, a cardholder does not even have to worry if someone steals the card. Yet—and this is the key difference—the very freedoms credit cards offer also require users to order and self-regulate their own behavior. Even if the card is issued with no preset spending limits, a new cardholder still cannot typically buy a $100,000 car using that card. Regardless of whether the cardholder can afford it, a computer will likely decline the charge based on the lack of prior spending behavior; a cardholder, in turn, is aware of that potential for embarrassment, as well as the fact that overloading one's credit line will likely impact one's credit score and future credit potential. (The cardholder may wish to buy a car or a house in a few years, for instance, and hopes to get a loan.) Yet this situation may change from day to day; perhaps after the cardholder buys a series of $1,000 meals over a period of time, the computer will decide that he or she fits the profile of a "high spender" and allow the $100,000 charge in the future.

Somewhere, a computer is calculating the impact of each spending decision and adjusting to it in real time, and, in turn, the cardholders adjust, too. "You" are a set of spending patterns, and that projected profile both enables the bank to extend credit to you as well as puts the onus on you to take responsibility for those spending patterns. Convenient, if a little creepy. The core idea behind a control society, then, is thus a continuous set of cybernetic systems, financial incentives, and monitoring technologies molded to each individual subject, that follow him or her even when "outside" an institution as such; and, precisely because there are fewer explicit institutions, spaces, or rules to restrict the subject's behaviors, these systems are often experienced as freeing.

Can the cloud be explained by this model of control? Most scholars would unequivocally say yes; Deleuze's description of data aggregation, the amorphous and open environment of computer code, and even the gaseous qualities of corporations within a control society map directly onto attributes of the cloud. If there is any problem with his theory, it is that his argument seems a little *too* easy to apply to the cloud. When he writes about a nightmare scenario—that an "electronic card that raises a given barrier" is governed by "the computer that tracks each person's position"—a present-day reader

wonders what the fuss is about; much of what Deleuze envisioned, such as computer checkpoints and computer tracking, has come true already.[13] The widespread claim that we are in an era of biopolitics has largely been built on the strength of such evidence.

This book's goal is to think beyond this idea of the control society, to both acknowledge its influence and use the cloud to ask what this theory cannot account for. If we look at the cloud closely, we find the presence of phenomena that hint at other explanations. The all-but-forgotten infrastructures that undergird the cloud's physical origins, for example, often originated in a state's military apparatus; one of the earliest real-time computer networks was an early-warning system for incoming nuclear missiles in the 1950s. Today's cloud relies on a repurposed version of this infrastructure, among a host of other Cold War spaces. Internet providers reuse old weapons and command bunkers as data centers, while the largest data management company today, Iron Mountain, was founded as Iron Mountain Atomic Storage, Inc. Even as this militarized legacy begins to decay, its traces continue to haunt modern-day digital networks with their ghostly presence.

These traces are a clue that the supposedly anachronistic mode of sovereign power may be returning under different forms. Rather than consider sovereign power a historical exception or aberration within a wholesale shift to the systems of control, I suggest that it has mutated and been given new life inside the cloud.[14] As Foucault himself emphatically warns us: "We should not see these things as the replacement of a society of sovereignty by a society of discipline, and then of a society of discipline by a society, say, of government. In fact we have a triangle": a triangle where sovereign, disciplinary, and governmental power (or control) constitute the three sides.[15] What this book shows is that the cloud grafts control onto an older structure of sovereign power, much as fiber-optic networks are layered or grafted onto older networks. I term this new hybrid form the "sovereignty of data."

The cloud contains a subtle weapon, a way of wrapping sovereign power—torture, targeted killings, and the latest atrocities in the war on terror—in the image of data. By this I do not mean that sovereign power surfaces in new forms of "cyberwarfare," or (as others have argued) in the fact that war itself has become increasingly mediated by digital technologies.[16] Instead, the sovereignty of data comes out of the way we invest the cloud's technology with cultural fantasies about security and participation. These fantasies may be as

simple as the idea that the cloud will protect our data from unsafe, "unfree" hackers; that data needs to be secured from disaster; or even that the cloud is a unique medium for user interaction. These ideologies are disseminated through routine interactions with applications in the cloud, such as tagging a photograph on Facebook. Even measures meant for our safety—marking messages as spam, for instance—construct a set of cultural norms that we internalize as "responsible" online behavior.

As users are increasingly aware, values such as participation are sometimes co-opted by market mechanisms that John Horvath originally described as "freeware capitalism."[17] Corporations, for example, ask us to "interact" as a form of marketing feedback. Even more subtly, however, by interfacing with the structure of sovereign power, these ideologies position the cloud's users within the same political economy as the acts of state violence performed in their name. The wars over resources and territory and extralegal torture after 9/11 may appear to be worlds away from the political economy of data. But, I contend, they point to a resurgence of a violence that is enabled by the cloud.

Seen correctly, the cloud is a topography or architecture of our own desire. Much of the cloud's data consists of our own data, the photographs and content uploaded from our hard drives and mobile phones; in an era of user-generated content, the cloud is, most obviously, our cloud (this is the promise of the "I" in Apple's "iCloud," or to use an older reference, the "my" in "mySpace"). Yet these fantasies—that the cloud gives us a new form of ownership over our data, or a new form of individualized participation—are nevertheless structured by older, preexisting discourses. As chapters 1 and 3 argue, the cloud's relationship to security can be traced to Cold War ways of thinking about internal enemies as well as nineteenth-century notions of a "race war," while chapters 2 and 4 show that its participatory impulse comes not just through new interactive technologies but also through economic liberalism's mechanisms for constructing a modern subject that is left to itself—the sort of subject we call the "user." The intersection of security and participation in the cloud can help us understand any number of individual cases: why we constantly invoke the specter of foreignness (e.g., China, Iran, Nigeria) when discussing hacker/spammer threats to the "free" Internet; why Cold War rhetoric has increasingly informed digital threats, as in the *New York Times*' invention of the phrase "mutually assured cyberdestruction";[18] why calls for digital activism (or "hacktivism") are often co-opted in a

framework that already invites participation; why the so-called Internet kill switch reads (falsely) as a joke that involves no actual killing; and even why the NSA's facilities for decrypting intercepted calls are structurally similar to those used by digital archivists trying to preserve digital media from decay.

Taken together, my examples suggest that the sovereignty of data is ultimately what Achille Mbembe has called a "necropolitics," a politics of death.[19] It is the cloud's participatory ideology that motivates amateur data collectors to assist NATO in streamlining its F-16 bombing operations, for example: as I argue in chapter 4, war outsources its dirty work to volunteers by substituting a live, interactive representation of death for death itself. The perversity of the cloud is therefore not that it explicitly causes death. Rather, the cloud transmutes the mechanism of death and presents it to us as life.

How to View Emptiness

Of course, the idea that the cloud is inherently political may not be so new. Today one need not go far to find headlines like that on the February 2014 cover of *Popular Mechanics*: "Privacy Is Disappearing: How New Tech Tools Can Help You Fight Back." As ever more data moves into the cloud, the general public has increasingly become aware that the cloud is politically contested terrain; articles on data-veillance and cell phone tracking routinely run in the popular media. Yet typical responses to this debate invoke technological and legal solutions, such as do-not-track software or a new law; the *Popular Mechanics* article, for example, tells users to reclaim their privacy by installing encryption software and "practicing good browser hygiene."[20] The problem with this approach, however, is that it does little to address the wider political and social context from which these problems—and even the very idea of privacy—originate; nor does it take in account the logics behind technology itself that actually reproduce and redouble the problem of privacy. As I show in this book, for example, digital hygiene does not "fight" US government monitoring, as the article claims; indeed, digital hygiene is actually the goal of a Department of Homeland Security educational campaign that aims to have US users internalize correct (i.e., legal) online behaviors.

Scholars concerned about such issues have typically embraced the idea of materiality (or, more specifically, "platform studies") to recuperate the often invisible logics, algorithms, and apparatuses that structure digital culture. Focusing on digital culture's media-specific properties typically involves

examining the technological platforms within: Internet Protocol, lines of Java code, network cables, or conventions for the Unix operating system.[21] In doing so, such scholars claim that an awareness of a medium's materiality will lead to a more effective understanding of its ideological content. Yet the cloud, I am arguing, inevitably frustrates this approach, because by design, it is not based on any single medium or technology; it is medium-agnostic, rather than medium-specific. As an inter-network, any type of communications network or technological platform can conceivably be attached to it, even analog ones; in 2001, one Norwegian enthusiast even implemented Internet Protocol with a set of carrier pigeons. (Observers reported a disappointing 56 percent packet loss rate: rephrased in English, five out of the nine pigeons appeared to have wandered off, or have been eaten.)

Further, one of the curious dilemmas that the cloud represents is that not even the engineers who have built it typically know where the cloud is, and, as a consequence, what part of the apparatus to examine. A personal anecdote: in my stint as a network engineer in the late 1990s, I would routinely travel to a handsome, terra-cotta-roofed building a few blocks from downtown Palo Alto, California. Unbeknownst to its well-heeled passers-by, perhaps one-fifth of the world's Internet traffic once flowed through this building. Back then, Palo Alto was one of five major exchange points in which the major national "backbone" networks, such as AT&T or Sprint, would connect with each other. Because of security concerns, engineers were never quite sure who or what was in the neighboring rack of network and computer equipment; my coworkers and I just knew that our cables ran somewhere into a cage in the floor below. I had a pretty good hunch, though—gleaned through a combination of the rumor mill, glimpses of router names punched on Dymo tape, and the Quebecois-accented English that some other workers spoke. Yet while I knew how to route packets to Deutsche Telekom, Nippon Telegraph and Telephone, and Teleglobe Canada over my computer screen, the network's physical presence still felt remote to me. One morning at 4:00 a.m., I decided to become better acquainted with it.

So, impulsively, I took a fiber-optic cable and unplugged it. Then I held it up to my eye and looked in. On the other side of the fiber, I imagined, was Japan. The light was red, and it winked like a star on a smoggy night. Because fiber optics were new at the time, what I had only read about, but not yet experienced, is that there are two kinds of fiber-optic cable: single-mode, for long distances, and multi-mode, for short distances. A single-mode laser

would have lased a hole into my cornea and blinded me instantly. Multi-mode is often powered by LED light sources rather than true lasers. Single-mode is indicated by a yellow cable; multi-mode, orange. The cable I had grabbed was orange.

That I can still see today is a testament to both my dumb luck, and also, metaphorically, to the paradox that the cloud represents: that you can never see it by looking directly at it. Indeed, my naive desire to look into the cloud's fiber-optic network is a little like asking what a film is about, and looking into the most direct source of the image—the projector beam—to find out. You can get as close as you want to it, but the blinding light won't tell you much about the film, and it may even be dangerous for your eyes; it certainly involves turning your head away and not watching the film. The cloud is not unlike the changing shapes and virtual images cast by a projector. But to mistake the apparatus for the film makes us like those mythical "country rubes" of the 1910s who were said to have assaulted the projection booth, looking for the real movie star shown by the film.

Analyzing the cloud requires standing at a middle distance from it, mindful of but not wholly immersed in either its virtuality or its materiality. For this reason, this book does not adhere to the cloud's current technologies—for instance, by dissecting the lines of code in a network protocol implementation. Nor will this book begin with the story of an invention. There are no scenes of apartment windows in Cupertino or cubicles in Seattle lit late at night, where an Apple worker realized something about accessing e-mail applications over the web, or an Amazon engineer became aware that excess computing capacity could be resold to other companies. Because the "cloud" is, properly understood, a cultural phenomenon, I mobilize three categories of primary sources that address this larger sense of the cloud:

1. Representations and anticipations of the cloud in US popular media, legal and political records, corporate advertisements and ephemera, and the like. To be sure, the prehistory of the cloud is not only an American story; there is a need for parallel scholarly studies on, say, the French online service Minitel and specifically non-Western network cultures.[22] But the United States wields considerable veto power over supposedly international bodies for Internet standards as well as infrastructures such as domain name service; the Department of Justice has even used its jurisdiction over the Virginia-based registrar for the .com, .net, and .org domains to seize and prosecute non-US websites. And, more metaphorically, the book's focus on

the United States also responds to the cloud's own rhetorical framing as "the cloud." President George W. Bush was widely mocked for using the plural "Internets" when he referred to "rumors on the, uh, Internets" during a 2004 presidential debate. But in pluralizing the term, Bush was dead-on in a strict sense: there are multiple private Internets and clouds that parallel or shadow the public Internet, run by research universities, militaries, and even foreign countries that have built or are building "walled garden" Internets. Instead of recognizing this, however, we typically internalize the fiction that there is only one Internet, and one cloud.

The use of the cloud's singular form—"the cloud"—not only condenses a wide multiplicity of network forms and clouds into a single vision that encompasses all networks, but also reflects a universalist world view that tracked closely with American political ideals as they developed through the 1950s on: that the cloud would stand in for a "free" Internet and liberal civil society. For that reason, texts drawn from US culture offer a unique perspective for understanding this sensibility.

2. Examples drawn from the culture of computer science itself: the terms, metaphors, and diagrams that show how scientists and hackers understood their subjects—descriptions, to be clear, which often failed or succeeded purely by practice rather than technological superiority. What does it mean, for example, to name (and therefore to think of) a nonfunctional link to another website a "dead link" (rather than a "404 error"), or to mark each data packet with a "time to live" stamp? To think of multitasking as "intimacy," and debugging as a form of "peeping"?

In revisiting subjects whose stories have been partially told by computer historians, my goal is not to recycle existing narratives of invention, but to examine discourses that are typically hidden within these narratives. Part of this aim is to avoid the presentist bias that often confirms successful technologies at the expense of the myriad of alternate ways that scientists imagined the future. Interactive computing was, for example, not developed for interactivity at all, but rather for more efficient debugging. For a while, the word "computer" did not even designate a machine, but rather a laborer—generally a low-paid female worker. Nor was computer science thought of as an independent discipline worth serious academic study until the 1950s and 1960s, when the first computer science programs were founded at the University of Cambridge and Purdue University. Lacking their own discipline, early computer scientists were by necessity in dialogue with urban planners,

sociologists, businessmen, and even members of the counterculture; they were amateurs as well as professionals who were part of, but did not have the final word over, their cultural context.

3. Photographs, drawings, videos, and even games that offer insight into how visual culture functions in the cloud: what the cloud looks like on-screen; how we draw or map its shape; how the cloud grew out of TV/video networks. Crucial to this enterprise is the belief that visual culture does not merely reflect or represent beliefs; it also anticipates and shapes it. As Marshall McLuhan put it, artists serve as a "Distant Early Warning system" for societal change,[23] and the artistic avant-garde offer us a window into the bleeding edge of how new media might be used. The art objects I consider—by Ant Farm, Trevor Paglen, the Raindance Corporation, and others—bring into focus key moments of the cloud's development, and allow us to think through historical problems of power and visibility. Because visual culture tracks the minor mutations of power that shape the cloud, the question of power's visibility may be best interrogated by artists.

Collectively, these works of art also pose an important, if unanswerable, question: what tactics can we use to challenge a diffuse, invisible structure of power? Increasingly, artists and activists have used new media techniques to critique the myriad of problems raised in and by digital culture. As a form of electronic protest, for example, "hacktivist" groups have used distributed denial-of-service software to overwhelm target websites. Perhaps the best-known example occurred in 2010, when Visa and MasterCard refused to process donations for WikiLeaks, the site that positioned itself as a secure drop box for massive floods of leaked information; in response, pro-WikiLeaks sympathizers flooded, and shut down, websites such as Visa.com and Mastercard.com. In turn, the quantity of info on the WikiLeaks site, such as the 109,032 field reports of every death in the Iraq war, spurred another set of hacktivists to develop a parallel tactic: the construction of data-mining and data visualization tools for mapping and "seeing" the cloud of data (figure I.2).

Taken as a whole, these heterogeneous groups of "tactical media" artists have suggested that electronic problems should be opposed electronically.[24] Whether through activism, art, or simply the narratives written about it, the cloud has offered a platform for unconventional modes of critique and dissent, a medium for loosely organized, decentralized modes of protest. Yet as productive as these strategies may be, many of them assume that the electronic medium they work in is a neutral one; as we see in chapters 3 and 4,

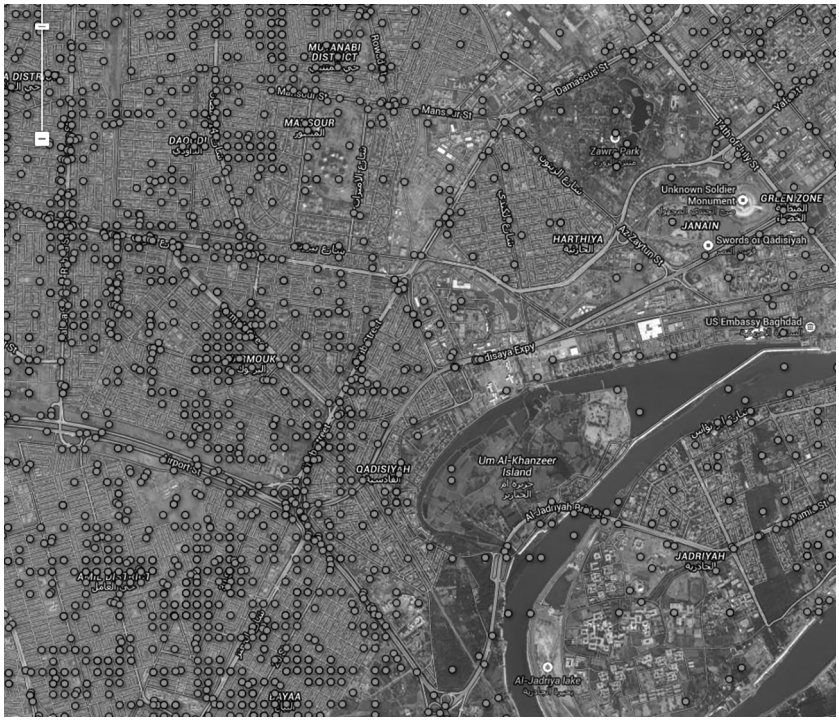

Figure 1.2

Simon Rogers, *Wikileaks Iraq War Logs: Every Death Mapped*, data interface, *The Guardian Datablog*, 2010–. Map data: Google Imagery; Cnes/Spot Image; DigitalGlobe; Landsat. Courtesy of Simon Rogers.

their protests often reproduce the system of values (of, say, "participation") embedded in the cloud.

This is a thorny problem, doubled by a historiographic one: the lines between newer and older forms of resisting power are typically drawn more sharply than usual, because the field of new media studies is typically built around finding and writing about the new. At the least, the term "new media" contains within it an implicit opposition to old media, just as digital media implicitly rules out or excludes the analog. (Even in the field of media archeology, a field oriented to studying dead media, the phrase "dead media"—and, as a result, media's "deadness"—is too often taken for granted.) In discussing these artists, it may be more productive to set aside the impulse toward defining what is new about their work. For the battles over digital media are often reflected in other, older medias, such as Portapak video, that

were once new. The call to reconfigure the structure of the television network in the 1970s using community access television (CATV), for example, is strongly reminiscent of the early debates over broadband Internet; both technologies briefly seemed to offer an alternative to the network's centralized structure before they were quickly commercialized and recentralized.[25]

Though such strategies may have failed in their utopian idealism, they offer a perspective on and a way of working through problems of contemporary media. To be clear, I am not suggesting that there is nothing new about new technology. Instead, I am offering an alternative to the kind of historiographical model reliant on a series of technologically induced epistemic shifts or ruptures that often pervades media studies.[26] The analog technologies within the cloud periodically return to view, even if in spectral form. As a result, analog sources will allow us to think through digital problems, and, in turn, challenge the implicit separation between analog and digital.

To challenge this separation is to realize that the cloud is a historical, fragile, and even mortal phenomenon with its own timespan. Over the last twenty years, the Internet has been variously described as a "series of tubes," an "information superhighway," an "ecosystem," a "commons," a "rhizome," a "simulacra," a "cloud" (note the title of this book), and even, as the director of the MIT Media Lab once put it, a "flock of ducks." Each term brings with it an implicit politics of space: if the Internet is imagined as a "public commons" being walled off by regulations such as the Digital Millennium Copyright Act, this serves as potent rallying point for those who would defend it from such incursions; but if the Internet is a "rhizome," then such incursions are already part of the network's anarchic structure: "The Net treats censorship as noise and is designed to work around it."[27] These metaphors have therefore served as flashpoints for political debate. As Tiziana Terranova has shown, prominent neoconservatives such as Alvin Toffler and Newt Gingrich used the image of a network as a self-regulating "ecosystem" to repudiate the Clintonian metaphor of an "information superhighway" that, presumably, needed government construction and maintenance.[28]

"The cloud" is only the latest in this series of metaphors. Because it represents a cultural fantasy, it is always more than its present-day technological manifestation (which has, at any rate, already changed since the moment I set these words to paper). If we come to see the cloud as a historical object, we might realize that the story of the cloud is largely unwritten on two fronts: the past and the future. As its title indicates, this book puts forth a prehistory

of the cloud. But it also attempts to open up a set of methodological tools to imagine the cloud in the future, meaning both the cloud's impending obsolescence as well as its barely foreseen consequences. For the legacy of the cloud has already begun to write itself into the real environment. As one of the largest consumers of coal energy, for example, the cloud's infrastructure was responsible for 2 percent of the world's greenhouse gas emissions in 2008, and data centers have grown exponentially since then. The long-term consequences of the cloud are worlds away from the seductive "now" produced by its real-time systems. It is our job to catch up with this legacy.

Mapping *Cloud*/Mapping the Cloud

To make a book about something as formless as the cloud is inherently a quixotic objective. Every book is a technology that imposes its own spatial terms on its subject: it's generally linear in form, contains a certain number of pages, and is operated by flipping (or swiping). Within that container, my own four-chapter structure lays out the following question: if the cloud is a cultural fantasy (chapter 1) of participation (chapter 2) and security (chapter 3), what happens when users participate in their own security (chapter 4)? My argument is constructed by examining the cloud's networks (chapter 1), virtualization (chapter 2), storage (chapter 3), and data-mining interfaces (chapter 4).

To understand what the chapter subjects in *A Prehistory of the Cloud* have to do with each other, it is first worth explaining one concept from computer science, which typically divides a technical apparatus into a series of so-called abstraction layers. These layers move progressively from the least abstract to most abstract. In the case of networks, for example, the physical link on the bottom—fiber-optic cable, Ethernet copper wire—forms the layer of least abstraction. Various protocols in between (Internet Protocol, then Transmission Control Protocol on top of IP) form the middle layers, with the application layer on the very top (the software built on networking protocols, such as streaming video) being the most abstract. This model also describes other technologies, such as operating systems or algorithms, usually through three to seven layers of abstraction.

The idea of layered abstraction is readily visible in our day-to-day lives: you can send an e-mail without worrying about if it travels over a wireless or wired connection, or store a file without knowing whether it is on a USB

Table I.1
The book understood as abstraction layers

4: Application	Data mining	Seeing the Cloud of Data
3: Data access	Data storage	Data Centers and Data Bunkers
2: Platform	Virtualization	Time-Sharing and Virtualization
1: Infrastructure	Network	The Shape of the Network

drive versus a magnetic drive; it is just "the network" or "the drive." The idea thus offers a spatial model of understanding and even standardizing computing: each layer depends on the more material layers "below" it to work, but does not need to know the exact implementation of those layers. Cloud computing is the epitome of this abstraction, a way of turning millions of computers and networks into a single, extremely abstract idea: "the cloud."

The chapter structure of *A Prehistory of the Cloud* evokes the spirit of its subject's abstraction layers (table I.1). This book begins with the earliest vision of the cloud as a "network of networks"; moves to the virtualization software that allows networked resources to be abstracted, and therefore shared; continues to data storage and security delivered through those virtual machines; and, last, examines the data-mining algorithms that "see" through, and rely on, cloud-delivered data. This layer of abstraction may be useful for readers more familiar with a traditional platform studies approach: for instance, someone who has read Matthew Kirschenbaum's work on hard drives and storage might refer directly to chapter 3, while someone interested in material infrastructures might find chapter 1 of interest.[29]

Of course, from a different perspective, my division of the cloud into four layers is arbitrary, and omits any number of other possible technological layers that could have been examined—for instance, the relational database, or web application architecture. Further, because the technology of the cloud is relatively young, the relation between layers is likely confusing: a consumer may think of "cloud" as the cloud drive on his phone (layer 3); a software developer may use "cloud" to mean "software as a service" (layer 2), while a network engineer may continue to use "cloud" to mean a "network of networks" (layer 1). Yet this confusion may also be an opportunity. One of the reasons that a network engineer thinks of a cloud in this way is because the cloud signified a network in the 1970s, while cloud storage did

not explicitly declare itself "the cloud" until the late 2000s. In other words, as each infrastructure becomes naturalized, we tend to refer to it with increasing amounts of abstraction, talking about its use (cloud storage) rather than the infrastructure itself (storage servers in data centers). Thus each level of abstraction is a sort of archeological deposit that records the idea of what we thought of "the cloud" at a certain moment in time—however problematic that "we" is. This chronology is neither linear nor exact, but instead testifies to the multiple discourses and prehistories that form the cloud today.

Begin, then, with the cloud's base layer: the network. How did the cloud come to be shaped the way it is? Chapter 1, "The Shape of the Network," answers this question by examining a highly charged moment in 1961, when the Bell System was targeted by a series of bomb attacks that tore through Utah and Nevada, at the same time that engineer Paul Baran began to develop his theories on distributed networks. Reviewing Senate hearings on the bombing, I conclude that the perfect network is an ideological fantasy, one that 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. From this, I turn to the architectural collective Ant Farm, which offered a very different vision of an information highway in 1970 and 1971—one reliant on trucks circulating on the interstate highway to carry packets of data—to suggest that in order to approach the perceptual effects of the cloud, one must first think of the network unobscured by the effects of technology.

In chapter 2, "Time-Sharing and Virtualization," I examine the prehistory of what we now call "cloud computing," the idea that computer power—along with the software programs and networks associated with them—could be "piped" into a user's home, like electricity or other utilities. This vision came out of the early 1960s, with the invention of a technology called time-sharing, which allowed the million-dollar cost of a computer to be shared and the computer multitasked. Though mostly forgotten, time-sharing not only invented the modern idea of a user—a personal subject that "owns" his or her data—but also positioned that user within a political economy that makes a user synonymous with his or her usage, and encourages users to take (even steal) computer resources for free. The freedom that results, however, is a deeply ambiguous one, for the same technologies that allow files and user accounts to be made private in the cloud—known as virtualization software—also represent a subtle form of control. This chapter uses the

metaphor of an ancient technology, the sewer system, to understand how the cloud keeps each household's private business private even as it extends the armature of the state or the corporation into individual homes.

Chapter 3, "Data Centers and Data Bunkers," traces the cloud of data back to the data centers that store them. These massive warehouses at the heart of the cloud cost up to $1 billion each to build and contain virtually every form of data imaginable, including airline tickets, personnel records, streaming video, pornography, and financial transactions. Interestingly, a number of data centers enclose data inside repurposed Cold War military bunkers. This suggests an unexpected consequence: the sovereign's rationale for a bunker or a keep, to defend an area of territory, has now become transported to the realm of data. Digital networks do not transcend territorial logic; even as data bunkers allow networks to be divided into logical zones of inside and outside, they raise the specter of attack from those that might be "outside" to network society, such as Chinese hackers or Iranian cyberwarfare specialists. By revisiting Paul Virilio's classic text *Bunker Archaeology*, I suggest that the specter of a disaster that the cloud continually raises also carries within it a temporality of our imagined death. This temporality animates a recent series of digital preservation projects, such as the "digital genome" time capsule, intended to survive the "death of the digital."

In chapter 4, "Seeing the Cloud of Data," I continue the discussion of data-centric tools by examining the ways that companies, users, and states navigate the piles of data by "targeting" information. As I show, targeted marketing campaigns online come out of the same ideological apparatus as military targeting, and I take up this militarized aspect to offer a more complete picture of data mining. Two oppositional groups provide case studies for this chapter. First, I examine a group of radio-frequency hackers who started data-mining the 2011 NATO intervention in Libya, in effect turning war into a problem of "big data." Next, I turn to artist/geographer Trevor Paglen, who has obsessively used data-gathering techniques to photograph what he calls "blank spots on the map"—reconnaissance satellites used to spy on us, and covert desert airstrips used to run the CIA's extraordinary rendition program, which secretly transferred foreign prisoners to torture sites outside of US soil. However these "hacktivists" may posit a mode of countersurveillance, their tactics mimic a militarized state's own operations; for this reason, these tactics may only end up reanimating the very structures of power that they purport to expose or overturn. This duplicative

structure is part of a logic I call the sovereignty of data, which co-opts the opposition's participation and gives practices such as torture and extraordinary rendition new life within the cloud.

Writing about violence within the cloud is difficult because the violence is largely displaced elsewhere. Rob Nixon, for example, has incisively pointed to the contrast between the supposedly real-time nature of the Gulf War and what he terms the "slow violence" of its aftermath.[30] The story of the Gulf War—so critics and writers tell us—is one of networks and screens, of virtually instantaneous strikes by computer, of what one journalist dubbed the "Hundred Hour War." Yet the story of the depleted uranium munitions released during combat (and their 4.5-billion-year lifespan) is not as easy to tell. Environmental problems, Nixon concludes, are difficult to narrate through conventional forms: "Stories—tightly framed in time, space, and point of view—are convenient places for concealing bodies."[31]

Nixon's insight is applicable beyond the realm of environmental activism (and the environmental footprint of the cloud); the cloud, too, enacts its own form of slow violence. The constantly changing platforms of digital technology seem to call out for, as Peter Lunenfeld puts it, "doing theory and criticism in real time"—namely, responding to each event of digital culture as quickly as possible.[32] Yet the cloud, this book argues, causes a double displacement: the displacement of place itself from sight, but also a temporal displacement. *A Prehistory of the Cloud* attempts to reframe this discussion. It places the digital cloud in dialogue with objects and spaces on the other side of the analog/digital divide. Both interacting with and stepping back from the current moment, it explores the limits and potentialities of a slower form of writing that takes seriously the temporal disjunctions and dislocations within the idea of the cloud. In doing so, I hope to shed light on the hybrid construction I have called the sovereignty of data, a construction that joins war and security, users and use value, participation and opposition. As I argue in this book, looking at the cloud's technology is not enough to tell the story. In truth, the technology has produced the means of its own interpretation, the lens ("cloud") through which power is read, the crude map by which we understand the world. That is the tail wagging the dog. Begin with space, power, and the combination we call history. Then the cloud will follow.

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

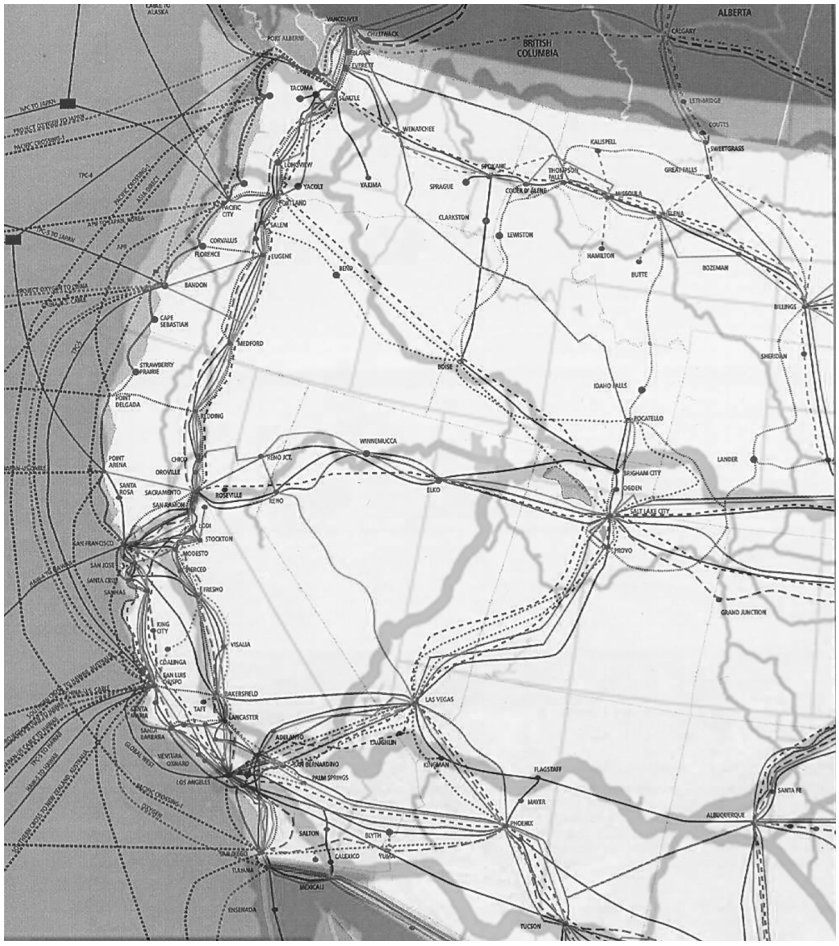

Figure 1.2

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

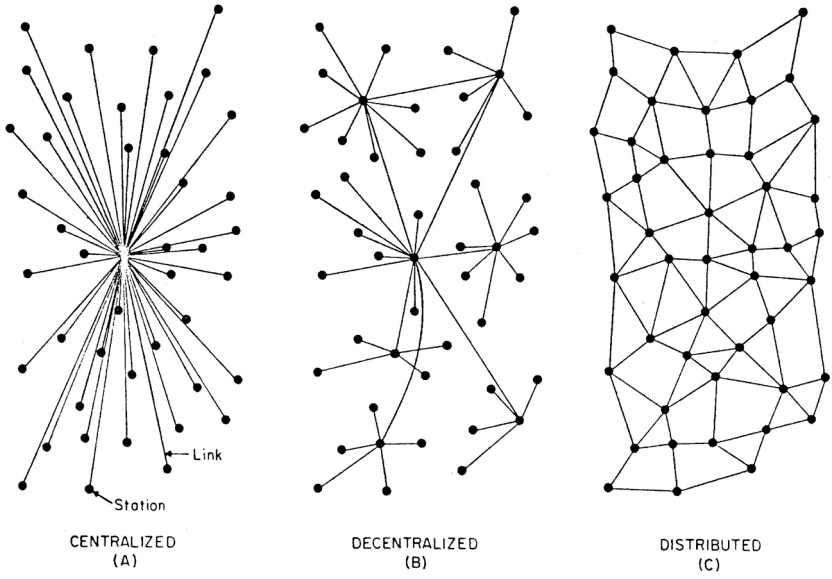

FIG. 1 — Centralized, Decentralized and Distributed Networks

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