The constitution of a *national security* state transformed the United States into a new kind of secret society after World War II, one in which state power rests to an unprecedented degree precisely on the ability of officials to manage the public-secret divide through the mobilization of threat. This *secrecy/threat matrix* marks all state secrets as equivalents of the atomic secret, making revelation a matter not just of politics but of the life or death of the nation-state. The Cold War arms race—founded on the minute-to-minute possibility of nuclear war—installed the secrecy/threat matrix as a conceptual infrastructure, enabling a new species of politics in the United States. Instead of enabling a system in which knowledge is power, the national security state’s system of compartmentalized secrecy produces a world in which knowledge is increasingly rendered suspect. This is a profound shift in how secrecy functions socially. In such a nation-state, secrecy becomes an increasingly pathological administrative form, one that prevents confidence in knowledge, and where no one—citizen, solder, or official—is untainted by secrecy’s distorting effects. As we shall see, the security state is increasingly structured not by the value of knowledge or by the power of withholding knowledge, but rather by the theatrical performance of secrecy as a means to power.
Instituting Secrecy

With the Atomic Energy Act of 1946 and the National Security Act of 1947, the United States effectively removed huge areas of governmental affairs from citizens’ purview. These acts formally installed a new security state within the United States, constituting a rather fundamental change in the nature of American democracy. The Atomic Energy Act created the first kind of information—nuclear weapons data—that did not need to be formally classified: it was “born” that way. The National Security Act then created a wide range of new governmental institutions—most prominently, the Central Intelligence Agency (CIA), the first of what would become seventeen intelligence agencies in the United States—that by charter would not be publicly accountable to citizens. Created in peacetime, the new laws and agencies marked the establishment of a permanent wartime economy as well as a fundamental commitment to state secrecy in the United States. Rationalized as an effort to protect military secrets about the atomic bomb in an uncertain world and to prevent a “nuclear Pearl Harbor” (see Dower 2010, 27), these acts inaugurated a split between national security and state security in the United States, with citizens implicitly recognized as a potential barrier to state security policies. After 1945 the U.S. security state apparatus increasingly used nuclear fear as an affective means of reconstituting the line between the foreign and the domestic, and to mobilize citizens as Cold Warriors.

Although the concept of a state secret was not invented during the Manhattan Project, the state structures that were established to build the atomic bomb have subsequently evolved into an unprecedented and massive infrastructure in the United States—so massive, in fact, that its sheer scale is difficult to assess (see Burr, Blanton, and Schwartz 1998; and also Masco 2002 and 2006). Today there may well be more knowledge that is classified than is not, more knowledge that is produced and locked up in the military-industrial state than is offered by all nonmilitary academic literatures. Peter Galison has calculated the scale of secret versus public knowledge in the United States and offers this assessment (2004, 231):

There are 500,000 college professors in the United States—including both two- and four-year institutions. Of course there are others—inventors, industrial scientists, computer programmers—responsible for generating and conveying knowledge, especially technical knowledge. But to fix ideas, four million people hold [security] clearances in the United States,
plus some vast reservoir who did in the past but no longer do. Bottom line? Whether one figures by acquisition rate, by holding size, or by contributors, the classified universe is, as best I can estimate, on the order of five to ten times larger than the open literature that finds its way into our libraries.

The classified archive is many times larger than the open library. Produced in the name of citizens who have no access to this knowledge except as employees of the security state, the classified universe is not simply a means of protecting the nation-state from the spread of dangerous military information; official secrecy is a social technology, a means of internally regulating and militarizing American society. The organizing principle for this system of secrecy is the atomic bomb, which is positioned within the universe of classification as the ideal type of state secret. Indeed, the system of secrecy that developed after World War II was premised on the idea that everything marked as classified had the potential to produce catastrophic results if made public. An important part of the cultural work accomplished by the state’s recitation of nuclear danger in the first decades of the Cold War was to establish this linkage between the classified and the apocalyptic—merging a bureaucratic system for managing the military-industrial economy with images of imminent destruction of the nation-state at the slightest slippage or revelation. By discursively positioning every classified file as potentially an “atomic secret,” the state transformed a provisional system of wartime secrecy into a fully nationalized system of perception management and control.

In essence, a new social contract was formed in the first decade of the Cold War, enabled and structured by the affective power of atomic weapons (Masco 2014). Simultaneously the ultimate weapon and the ultimate vulnerability, nuclear weapons presented a new set of contradictory resources and challenges to the state. For example, although declaring that the United States possesses “the greatest military potential of any single nation in the world,” National Security Council Directive 68 (NSC 1993, 50)—the top-secret policy document that articulated the Cold War policy of Soviet containment in 1950—is nonetheless ultimately a text about U.S. nuclear vulnerability. The directive depicts the Soviet Union as an existential enemy in anticipation of its future nuclear potential and argues not only for a fourfold military buildup but also for a mobilization of all institutions of American society to fight a long Cold War. This reengineering of American society for a new kind of warfare required a widespread recalibration of everyday life, including politi-
cal, economic, and military institutions as well as the urban landscape and ideas about the future (see Galison 2001; Masco 2008). The early Cold War military planners—Major General Walter E. Todd, commanding general of the Western Air Defense Force for the United Kingdom; Lieutenant General Willard S. Paul, an expert on economic mobilization in the U.S. Office of Defense Mobilization; and Val Peterson, head of the Federal Civil Defense Administration—all called in the same *Scientific Monthly* article (titled “National Defense against Atomic Attack”), for the construction of a “perfect air defense” involving the full accoutrements of now iconic “closed world” military technologies (see Edwards 1996), a dispersion of industrial sites away from urban centers, a relocation of housing stock to the periphery of cities, a constant war-gaming of potential Soviet attack scenarios along with domestic civil defense exercises, a massive program to stockpile critical materials to feed and care for the entire national population, new building standards for all construction designed to resist the effects of a nuclear blast’s effects, and a significant military expansion of the U.S. capability to fight a nuclear war. Todd, Paul, and Peterson concluded (1955, 246):

Mobilization is no longer to be undertaken upon declaration of war or after war starts. Either we stay ready at all times to absorb and survive the worst blow an enemy can strike, or we do not. If we do not, there probably will be no chance to mobilize afterward. If we do, there is a good chance that the blow will never be attempted, for we will have substituted many targets for a few. The enemy will no longer be able to destroy effectively the capacity to operate and, thus, to break the national spirit by a massive attack on major metropolitan areas.

*We stay ready at all times.* The immediate goal of the countercommunist state was to reengineer American society around and through the atomic bomb. Not only was nuclear fear integrated into military planning, but it also transformed the very nature of the nation-state. Indeed, all the projects proposed by Todd, Paul, and Peterson were actually pursued, fusing the Cold War military project with a new kind of domestic military economic strategy. But what was the actual nature of the nuclear threat? In 1950, the Soviet Union had no more than 5 nuclear devices, while the United States had more than 350; by 1961, these arsenals had grown substantially: the Soviet Union had amassed more than 2,400 weapons, while the United States had more than 24,000 warheads and bombs (Norris and Kristensen 2006). Few Americans at the time, or today, understand that the United States maintained at least a ten-to-one
nuclear advantage throughout the first decades of the Cold War, the period of the most intense nuclear paranoia in the United States. So how do we reconcile the clear nuclear advantage the United States maintained through the early decades of the Cold War with the domestic nuclear discourse of absolute vulnerability and imminent surprise nuclear attack?

Nuclear fear was the central concept within a larger project of emotional management campaign project designed and conducted by both the Truman and Eisenhower administrations to mobilize citizens for a new kind of war (see Oakes 1994). By concentrating public attention on specific images of nuclear threat and by classifying all other aspects of the nuclear economy, the early Cold War state sought to calibrate the image of crisis to enable the Cold War project. The primary goal of what was publicly called “civil defense” in the first decades of the nuclear age was not to protect citizens from the exploding bomb but rather to psychologically reprogram them as Cold Warrior. The calculated campaign of images—produced by the nuclear test program and delivered under the rubric of domestic civil defense—was an effort to access the emotions of U.S. citizens and thereby transform an emerging nuclear threat into a means of consolidating the power and importance of the security state. As a top-secret report to President Dwight Eisenhower put it in 1956 (Panel on the Human Effects 1956, 5), “Just as the Industrial Revolution of the early nineteenth century, with its far-reaching effects on war and peace, required vast social and psychological adjustments, so the present period faces extremely complex social and psychological changes.” Vast social and psychological adjustments are needed.

Calling for a new state project to install “psychological defenses” in citizens, and challenging each individual to engage in an “emotional adaptation” to the thought and reality of nuclear warfare, the report concludes (Panel on the Human Effects 1956, 11; see also Vandercook 1986): “The keystone of the program is knowledge—not merely information made available but information, both frightening and hopeful, so successfully conveyed as to become useful knowledge translated into plans, procedures, and the capability for constructive action. . . . In order to prepare the people, we believe that it will be necessary to involve them, and to involve them at deeper levels than mere factual information.” *A deeper level than facts.* Involving citizens meant teaching them about the effects of nuclear explosions—providing specific images of the bomb and censoring all others—while publicizing the emerging Soviet nuclear threat. Civil Defense was an explicit program to teach citizens to fear the bomb, fuse that fear with anticommunism, and modulate its
intensity so that a potentially terrified public did not become unwilling to support the larger Cold War program. The ultimate goal of civil defense was the creation of a citizen who was permanently mobilized as a Cold Warrior, restructured internally for constant readiness and psychologically hardened by nuclear fear. One of the most powerful attributes of the atomic bomb, in other words, is that it offered new access to the emotional life of the nation, producing a new kind of public constituted and militarized through a highly tailored vision of totalizing threat.

But if publicizing a specific concept and image of nuclear danger was the key to mobilizing citizens—to establishing an everyday life infused with the minute-to-minute possibility of nuclear war—the corollary project was an expanding use of state secrecy to manage the production of threat and control its public image. In the early Cold War period, the atomic bomb was the ultimate key to achieving global “superpower” status, as well as to installing a concept of danger that was the exclusive domain of the security state. For the nuclear state, this secrecy/threat matrix became a concentrated means of managing domestic populations as well as pursuing the broader geopolitics of communist containment. Secrecy was not just about protecting technological secrets in a global competition with the Soviet Union; it was also a means of converting American society into a countercommunist state at the level of institutions, economies, politics, and emotions. The War on Terror is a contemporary effort to reproduce the success of this early Cold War project in population management, affective governance, and military-industrial expansion, while at the same time expanding existential danger itself through the phantasmatic figure of the “terrorist with a WMD” (Masco 2014). The Obama administration ultimately committed also to a “modernization” of the U.S. nuclear complex, planning a set of new warheads, bombers, and missiles to be developed through mid-century at a foreseeable cost of at least one trillion dollars, thus extending the U.S. commitment to military nuclear power through the twenty-first century (Wolfsthal, Lewis, and Quint 2014).

The Counterterror State

Since 2001, secrecy has become a core tool in transforming the United States from a countercommunist to a counterterrorist state, and its official use is an ever-expanding practice. In a variety of Executive Orders and formal direc-
tives in the aftermath of the 2001 terrorist attacks, the Bush administration required each federal agency of government to increase its control of information.² According to government audits, there were nine million formal classification decisions in 2001 but over sixteen million by 2004, a trajectory that continues well into the Obama administration. Moreover, the rate at which records that are over twenty-five years old were declassified fell by over 75 percent in the same period. Thus, the official past as well as the official present have become newly politicized as well as highly censored domains.³ The cost of simply managing secret information in the United States grew to be over $7.2 billion a year, involving in one year alone over four thousand classification authorities and over 351,150 new classifications decisions.⁴ However, these figures only deal only with explicit classification or declassification decisions, the making of which is a formal regulatory process. An expansive “Sensitive but Unclassified (sBU)” category of information is a potentially larger and more influential category of knowledge. Information that is SBU is not officially classified; it is information simply removed from public circulation and treated as if it were classified.

Officially justified as a means of protecting information about “critical infrastructures” following the terrorist attacks on New York and Washington in 2001, the SBU designation and its expanding use have radically changed the way information is handled within federal agencies. The Homeland Security Act of 2002 charged federal employees to “identify and safeguard homeland security information that is sensitive but unclassified.”⁵ However, the act defined none of its terms, leaving it up to each federal agency to draw the lines between public access and critical infrastructure protections. Concurrently, the Department of Justice advised all government agencies to limit the scope of Freedom of Information Acts (FOIA) requests wherever possible—forcing litigation and thus contradicting the law’s intent—and while also pursuing an unprecedented application of the Espionage Act of 1917 to targeting whistleblowers within the government. These processes only accelerated during the Obama administration, including prosecutions of reporters writing about counterterror policies (Elsea 2013). In support of these new restrictions, the counterterror state has also embraced advocated a “mosaic theory” of information threat. This theory assumes that disparate items of information (particularly those that appear innocuous and of no obvious use to an adversary) can nonetheless be assembled to create a whole that is more powerful than the sum of its parts. According to this theory, any piece of information is potentially a national security threat, as it is the creative linking together bits
of knowledge that are imagined to be dangerous. The extensive surveillance programs run by the National Security Agency after 2001—involving digital surveillance, archiving telecommunications across platforms, and data mining on a newly comprehensive global scale—also rely on this concept. David Pozen has consequently argued that an aggressive use of the mosaic theory of information synergy produces claims that are “unfalsifiable,” leading inevitably to overclassification and threat proliferation (2005, 679).

The result of these new laws, practices, and interpretive strategies is obvious: information that flowed relatively freely a few years ago—for example, environmental impact studies of government projects—now fall into this SBU category and are often not available to citizens. A generalized state security concept trumps all other concerns (in this case, environmental protection) via the SBU approach. The images of prisoner abuse from Abu Ghraib prison fell within the SBU category and were released only after being leaked to 60 Minutes, the New Yorker, and Salon.com and via litigation by the American Civil Liberties Union. But less provocative information about government contracts, policy debates and initiatives, and anything that might have patentable potential—also falls within the SBU category. Thus, the overall strategy of the counterterrorist state has been to replace a presumption of transparency in nonmilitary matters with wide-ranging restrictions that emphasize noncirculation rather than, or in addition to, formal classification (see Roberts 2006, 36–41). It is via the SBU category that much of American society is being implicitly militarized—as keeping basic governmental information from citizens is increasingly normalized, equated with antiterrorism, and accepted as an administrative practice.

The most important aspect of the SBU category of information is that it has never been defined by federal law; it is a strategically vague concept that is used differently by each federal agency. The U.S. Government Accountability Office (2006) found fifty-six different definitions of SBU in use and could document few provisions to identify which (and how many) officials within an agency are authorized to designate information as SBU. The SBU designation is thus a largely unregulated category of information within the federal government. The first articulation of SBU as a category came from John Poindexter, while working as Ronald Reagan’s national security advisor, before he gained notoriety for his role in the Iran-Contra scandal. At the start of the War on Terror, he also served as head of the Defense Advanced Research Projects Agency until public revelation of his proposed Total Information Awareness data-mining project (devoted to capturing all digital com-
munication) forced him to step down in 2002. In 1986, Poindexter defined SBU information this way (quoted in Knezo 2003, 20):

Sensitive, but unclassified information is information the disclosure, loss, misuse, alteration or destruction of which of which could adversely affect national security or other Federal Government interests. National Security interests are those unclassified matters that relate to the national defense or the foreign relations of the U.S. government. Other government interests are those related, but not limited to the wide range of government or government-derived economic, human, financial, industrial, agricultural, technological and law enforcement information, as well as privacy or confidentiality of personal or commercial proprietary information provided to the U.S. government by its citizens.

National security or “other” interests. The “related but not limited to” concept here expands the SBU category to include most of governmental work: today, perhaps as much as 75 percent of nonclassified government information could be designated as SBU. When fully deployed, the SBU category effectively expands national security to include any kind of information whose release might be inconvenient to the execution of state policy. When combined with the mosaic theory of information risk, there is literally no aspect of governmental work that could not be conceptualized as an essential part of U.S. national security and thus seen as a threat if made public. Increasingly, anticipatory defense trumps democratic process across governmental activities.

Indeed, the SBU category was aggressively mobilized by federal agencies as an antiterrorism provision in October 2001, as a means of protecting critical infrastructures (also a strategically vague term) from terrorist attack (Knezo 2003, 25). From the perspective of the counterterror state, the value of SBU as a category is not only its ambiguity—as literally anything in the government can be separated from the public sphere, according to its logics—but also because there is no formal review process that citizens can use to challenge the designation of information as SBU. There is no federal agency charged with regulating the use of SBU or hearing appeals. It is therefore up to each federal agency, branch, office, and official to decide where to draw the line between public accountability and security, which allows near-infinite flexibility in standards and logics. If having basic information about governmental practices can be constituted as a threat, then SBU functions to blur the distinction between the citizen and the enemy. It also allows any kind of federal informa-
tion to be marked for noncirculation, creating an expansive new category of withheld information located between the explicitly classified and the public.

Following the declassification campaigns of the immediate post–Cold War era, and the enormous democratization of access to information access enabled by the Internet in the 1990s, the early twenty-first century has thus witnessed a fundamental shift in the idea and mechanisms of openness and transparency in the United States. Indeed, a central part of the conversion of the United States from a countercommunist to a counterterror state has been an information strategy of increased classification and noncirculation, and also of censoring of the existing public record. The U.S. National Archives have become an explicit front line in the counterterror project, as historical records relating to presidential authority, war authorizations, intelligence on WMD issues, and other military matters going back to the start of the Cold War have been removed, and designated as either designated as SBU or reclassified (ISO 2006). At least one million pages of previously declassified materials have been pulled from the National Archives since October 2001 (see Bass and Herschaft 2007). Thus, the historical formation, as well as the current projects, of the security state have been subject to expanding forms of censorship. Official fear of the terrorist, and of the WMD, has enabled a formal reconstitution of the security state as secret entity generating a wide range of covert actions within the United States and around the world. Secrecy in all its forms is a political tool, with the art of redaction an additional method for withholding information while complying with federal law (see figure 8.1).

Agreeing with every major official study of state secrecy in the past thirty years, William Arkin (2005, 12) argues that this level of secrecy is not only excessive but also profoundly damaging to a democracy, because it confuses the domestic politics of secrecy with efforts to protect military operations. Arkin notes, for example, that U.S. military activities operations that are easily recognized as such in the Middle East (from special operations to drone strikes) are nonetheless classified by the United States government, a state of affairs that serves only to keep U.S. citizens—not foreign nationals, military leaders, or adversaries—in the dark (see also Sagan and Suri 2003, 150). Chalmers Johnson (2000), takes this insight a step further, by pointing out that the CIA term “blowback” addresses not only the retaliatory consequences produced by U.S. covert actions at home and abroad, but also the damaging crucial domestic effects of secrecy. Since U.S. covert operation actions are by definition unknown to U.S. citizens, then actions taken around the world in response to them are literally unintelligible to U.S. citizens. Secrecy works here in a dou-
bled fashion to enable state actions that might not be supported if they were subjected to public debate while at the same time denying citizens a means of understanding the long-term political effects of U.S. global activities. In a counterterror state, blowback has several additional perverse effects: since U.S. citizens have no insight into U.S. covert actions around the world, retaliatory acts appear to the American public as without context and thus irrational. And given that the premise of the War on Terror is that a “terrorist” is an irrational and inherently violent being who is dedicated to destroying the United States, blowback empowers yet another level of American misrecognition and fantasy: namely, that the United States is only a global military actor when provoked by irrationally violent attacks. As Joseba Zulaika (2009) has shown in great detail, terror produces terror, becoming a self-propagating circuit of fantasy, preemptive violence, and retaliation.

A similar observation was made by Daniel Moynihan (1998) in his post–Cold War review of official secrecy: he noted that the Cold War decision to keep the Venona intercepts of encrypted Soviet diplomatic communications classified to protect sources and methods in the 1950s actually worked primarily to keep U.S. citizens in the dark about the true scale of Soviet espionage in the United States, since the Soviets soon knew their code had been broken. Moynihan suggests that releasing the files before 1995 might have prevented or reduced the profound political divide in American society over the nature of Soviet infiltration—as the Venona intercepts documented that there were, in fact, Soviet spies in the United States but nowhere near the numbers imagined by Senator Joseph McCarthy (see also Shils 1996, 13). Thus, secrecy produces political fetishes that can fundamentally distort a democratic public sphere. For example, the CIA’s increasing use of drones for targeted killings in Pakistan and Afghanistan has been the subject of widespread reporting (by nongovernmental agencies and mass media) and even confirmed by both President Obama and Secretary of Defense Leon Panetta, yet the CIA asserts in FOIA litigation that “the use (or non-use) of drones” is a “classified fact” and therefore not subject to any declassification claim.8

Jodi Dean (2002) argues that it is public recognition of state secrecy that enables a democracy to manage the split between what political life is supposed to be and what it is believed to be, between its ideal type and its lived experience. She argues that recognition of state secrecy—and the accompanying conspiratorial subtext to everyday life that it engenders—functions today to block political participation and curtail the possibility of truly demo-
ocratic endeavors. Specifically, collective assumptions about the secret state (its capacities, interests, omnipotence) installs an ever-ready alibi for failed or stalled politics within the public sphere, allowing the fantasy of democracy to coexist within its distorted reality. In Dean’s view, citizens now work more passionately to locate and reveal the secret than to enact structural change through direct political action. The democratic state form, which formally claims to be both transparent and accountable, has been reduced, via the logic of the secret, to a fight over the terms of the visible and nonvisible rather than social progress. For Dean, engaging the secret therefore becomes an act of misrecognition for citizens, who assume that revealing the hidden is the means of organizing democratic politics rather than mobilizing for collective action and is the way to organize democratic politics. She suggests that the evocation of the secret and the call to reveal it have therefore become surrogates for real politics in the United States— together constituting a fetish form that prevents the kind of collective mobilizations that enabled the social justice movements of past eras. Dean suggests, in short, that a belief in the secret constitutes the possibility of a democratic public—for if only citizens knew the state’s secrets, they could correct the obvious failings of the current political system and create a more perfect society—but it also installs a public for which agency is therefore also endlessly deferred in the act of chasing greater transparency. But if an informed, democratically energized citizenry is the first victim of the elaborate system of secrecy in the United States, policy makers also suffer.

There is a remarkable moment in Daniel Ellsberg’s autobiography in which he describes a conversation with Henry Kissinger, who was then on the verge of becoming Secretary of State. Ellsberg, the RAND analyst who eventually leaked the top-secret U.S. history of the Vietnam War known as the Pentagon Papers to the *New York Times* and the *Washington Post* (see Prados and Porter 2004), attempts to prepare Kissinger for the psychological effects of having access to above top-secret information. He informs Kissinger that, over the coming years, he will feel, in the following order: exhilarated (at the access), foolish (for what he once thought he knew), contempt (for those who do not have access), and increasing skepticism (about the quality of classified information). In the end, Ellsberg tells Kissinger (Ellsberg 2003, 237–38):

> It will become hard for you to learn from anybody who doesn’t have these clearances. Because you’ll be thinking as you listen to them “What would this man be telling me if he knew what I know? Would he be giving me the
same advice, or would it totally change his predictions and recommendations?” And that mental exercise is so torturous that after a while you give it up and just stop listening. I’ve seen this with my superiors, my colleagues . . . and with myself. . . . You will deal with a person who doesn’t have those clearances only from the point of view of what you want him to believe and what impression you want him to go away with, since you’ll have to lie carefully to him about what you know. In effect, you will have to manipulate him. You’ll give up trying to assess what he has to say. The danger is, you’ll become something like a moron. You’ll become incapable of learning from most people in the world, no matter how much experience they may have in their particular areas that may be much greater than yours.

You become something like a moron. Ellsberg reveals here a rarely commented on aspect of compartmentalized secrecy: it relies not only on withholding information but also on lying. Individuals must lie in order to protect their own classification level in everyday interactions throughout the system, and thus, they distort their social relations to protect the system of secrecy. Knowledge itself thus becomes doubly corrupted: first, because of the effect of compartmentalization on perceptions of expert knowledge as described by Ellsberg, and second, because perception control becomes as important as information management. Deception via classification becomes the internal structure of the security state, which over time works not to underscore the value of information—often the assumed goal effect of a system of compartmentalized classification—but rather to corrode the very terms of knowledge and expertise, making individual motivations and judgments also suspect.

The role of deception is crucial in the transformation of a democratic state into a security state, as the public good becomes absorbed into that of a security apparatus that by definition seeks to extend its power and reproducibility. This logic is made visible by even a cursory look into the state secrets privilege in the United States—the tool whereby the security state blocks a legal proceeding to protect “national security interests.”

The states secret privilege was formally established in 1953 in the Supreme Court case United States v. Reynolds. After an Air Force B-29 aircraft crashed near Marion, Georgia, in 1948, family members of the dead and injured sued the government for negligence, and sought declassification of the accident report to support their claim. The families won in lower courts, but lost on federal appeal in the Supreme Court. The air force argued that the B-29 mission involved research on “secret electronic equipment” and that to release
any information about the crash would damage national security. This case set the precedent for a “state secrets” privilege in the United States, which has become a now standard federal tool for nullifying legal challenges on national security grounds. The family members, however, continued to push for release of the accident report via the Freedom of Information Act, receiving several copies during the 1990s that were heavily redacted. Then, in 2000, they found an uncensored copy of the once-classified, and by then highly litigated, accident report on the Internet. It had been inadvertently released by the air force as part of a larger declassification of fifty-year-old records. The report made no mention of the “secret electronic equipment” that was the basis for the initial Supreme Court state secrets ruling, but it did document negligence in the maintenance of the aircraft and the training of the crew. Thus, the air force appears to have classified the report in 1948 not for national security reasons but rather to avoid liability for the accident. The families sued again to have the 1953 ruling overturned as fraud, and the Justice Department successfully deployed the mosaic theory of secrecy to stop the legal proceedings: in essence, federal lawyers argued that it is impossible to understand today what seemingly innocuous bits of information might collectively have had national security implications in 1948, regardless of the initial Air Force arguments (Fisher 2006, 203). It is crucial to recognize here that the foundational legal case for the state secrets privilege in the United States is grounded in deception rather than a principled theory of national security—illustrating how secrecy functions not only to protect information but to create new realities and new forms of bureaucratic agency and protection. Since 2001, the state secrets privilege has been evoked to nullify judicial hearings in an exceptional number of high-profile cases, including the extraordinary rendition of a German citizen by the CIA, retaliatory suits against whistle-blowers within the Federal Bureau of Investigation (FBI) and the air force, domestic data-mining operations in the United States, multiple cases involving the surveillance of U.S. citizens without a legal warrant, and accusations of targeted killing of foreign nationals and Americans abroad (Chesney 2007; Garvey and Liu 2011). The states secrets privilege is a central tool of the counter-terrorist state in managing threat perception as well as legal standing. It reveals the extraordinary power of the secrecy/threat matrix, which promises catastrophic consequences for a revelation of the secret while simultaneously classifying the considerations, evidence, and precedents supporting such an assessment.
The Affects of Secrecy

The modern state form is, in many respects, founded on the assumption of secrecy. Michel Foucault (1995; 2003) has shown that the modern state maintains the right not only to keep secrets but also to subject its citizens to increasingly minute forms of surveillance. The eighteenth-century logic of the panopticon is of a sovereign who sees without being seen, a formulation built literally into the architectural infrastructure of the prison and ultimately the mind of the prisoner. A similar logic is today replicated across U.S. digital surveillance activities on an unprecedented scale—creating a counterterror state that attempts to be completely hidden while rendering citizens completely transparent. Similarly, the modern project of population management involves a fine mesh of institutions devoted to measuring individuals and creating statistical portraits of citizens across a wide range of subjects, from health, to education, to the economy. Foucault charts a steady progression in the forms of knowledge, as well as the psychosocial intimacy of these state projects, from the overthrow of monarchal authority to the early twentieth-century nation-state, as the tools of surveillance and technologies of population management steadily increase in both power and resolution. Thus, there has always been a profound separation between citizens and the state, and the practice of democratic politics has always been highly mediated by practices of secrecy. Yet, the kind of state produced in the aftermath of World War II in the United States—a nuclear-armed, global superpower—takes a core principle of the nation-state form, the use of secrecy in the name of collective security, and expands it into a totalizing structure that links all aspects of the state in a radical global counterformation. In this post–World War II system, secrecy becomes not just a technology of state power, a means of orchestrating policy and protecting state interests through the withholding of information, but also the basis for an entirely new kind of power: the ability to create new realities.

Specifically, in the nuclear age the idea of the secret knowledge becomes deployable on its own. Evoking the secret thus also becomes a means of claiming greater knowledge, expertise, and understanding than, in fact, is possible. How else do we explain the fantastic collective failure of the U.S. intelligence agencies to be attuned to the internal collapse of the Soviet Union in the late 1980s, even after generating nearly constant threat assessments of Soviet activities for four decades? How do we explain the constant tension within U.S. security culture over dissent in the United States and the fre-
quent placing of nonviolent social activists into the category of the enemy? Secrecy has been enormously productive in terms of building and protecting a military-industrial economy, but it has also created new perceptions of state power that affect government officials as well as citizens. The linkage between the secret and the apocalyptic in the nuclear security state has transformed the citizen-state relationship both conceptually and in practice. The secrecy/threat matrix is, in this regard, ultimately a project of perception management, one that functions to create, protect, and project the idea of a “superpowered state.” Thus, the atomic bomb inaugurates a new kind of social contract in the United States, one that separates national security as a public discourse from state security as an institutional practice. It ultimately grounds the power of the state in the perceived ability to destroy or be destroyed, rather than in the strength of its democratic institutions (see, for example, Armstrong 2002).

The WMD as a technological form has always promised apocalyptic consequences if used in combat, but the idea of the “WMD,” its phantasmatic figuration, has been equally powerful in U.S. security culture. By defending all state secrets as the equivalent of the atomic secret, the U.S. security state has increasingly consolidated and defined its power via threat designation and inflation. The counterterror state’s efforts to expand official secrecy alongside its amplification of the WMD as the single greatest threat to the United States (see U.S. White House 2002) reveals one long-term effect of the Cold War secrecy/threat matrix: an official desire to close off citizens’ access to the state altogether, in the name of protecting the public. Official secrecy can now effectively restrict even the most banal forms of government information under the SBU category and mosaic theory concepts. These practices overturn the market logics of the information age, in which information made free was seen as a social good. The consequences of this information strategy are widespread in the United States, not only for systems of accountability but also for the sciences—in which self-censorship is increasingly sought for those working in fields of study that might have infrastructural, or military, or patent applications. Thus, the broader effect of these policies is to define the public sphere not as an inherent aspect of democratic order but as a fundamental risk to that very order, identifying rights that citizens should willingly surrender for their personal safety. The extensive data collection of the National Security Agency after 2001, for example, has rendered every detail of American citizens’ digital lives a potential security concern in the name of counterterror. Indeed, what does it mean when the free flow of information...
is the exception rather than the rule in a global superpower that is also a self-proclaimed democracy?

Finally, and importantly, the secret society that is the state is ultimately headless, an effect of both the systematic distortion in the believability of knowledge as it moves up the levels of a compartmentalized infrastructure and the demands on individuals to protect perceptions. Thus the secret is transformed over time in such a system: indeed, the “idea” of secret knowledge itself becomes deployable, corrupting public understandings of what is possible and what is not, and giving those with executive authority the ability to seem more knowing then they actually are. Instead of limiting agency via protected knowledge, the secrecy/threat matrix empowers a new kind of agency, unrestrained by facts. In the lead-up to the invasion of Iraq in March 2003, the Bush administration systematically deployed the idea that there were WMDs in Iraq as well as an imminent threat to the United States, to enable war. Vice President Dick Cheney, for example, stated in a speech to the Veterans of Foreign Wars National Convention on August 26, 2002, that there was absolute certainty about the Iraqi threat (Cheney 2002): “Simply stated, there is no doubt that Saddam Hussein now has weapons of mass destruction. There is no doubt he is amassing them to use against our friends, against our allies, and against us. And there is no doubt that his aggressive regional ambitions will lead him into future confrontations with his neighbors—confrontations that will involve both the weapons he has today, and the ones he will continue to develop with his oil wealth.” There is no doubt. Here is the secrecy/threat matrix in action, for Cheney implies that the intelligence community has documented with perfect clarity not only the technical terms of the Iraqi biological, chemical, and nuclear programs but also the intent of the regime to use them “against our friends, against our allies, and against us.” This is not a deployment of actual knowledge, as the lack of any evidence of weapons of mass destruction in Iraqi after the invasion demonstrates, but it is a political deployment of a claim to secret knowledge.10

Secretary of State Colin Powell, in his historic presentation to the United Nations in February 2003, was even more exacting in his deployment of the secrecy/threat matrix.11 He portrayed an Iraqi biological weapons program that was so advanced, it was already capable of threatening the continental United States. Claiming to have sources within the Iraqi government, he presented cartoon diagrams of mobile weapons labs (see figure 8.2) and satellite imagery of “WMD” production facilities (see figure 8.3). Powell stated conclusively (2003):
8.2 Iraqi mobile bioweapons laboratories, from Secretary of State Colin Powell’s presentation to the United Nations, February 2003 (Powell 2003).

8.3 Iraqi WMD sites, from Secretary of State Colin Powell’s presentation to the United Nations, February 2003 (Powell 2003).
We know that Iraq has at least seven of these mobile, biological agent factories. The truck-mounted ones have at least two or three trucks each. That means that the mobile production facilities are very few—perhaps 18 trucks that we know of. There may be more. But perhaps 18 that we know of. Just imagine trying to find 18 trucks among the thousands and thousands of trucks that travel the roads of Iraq every single day.”

*We know.* This depiction of mobile “biological agent factories” effectively transforms every truck in Iraq into a potential WMD laboratory, illustrating the phantasmatic power of the concept of the WMD when used by officials deploying secret knowledge.

But the nature of the threat becomes increasingly specific in Powell’s presentation, its very recitation of detail suggesting that even more exacting knowledge existed in the classified domain:

We know from Iraq’s past admissions that it has successfully weaponized not only anthrax, but also other biological agents, including botulinum toxin, aflatoxin, and ricin. But Iraq’s research efforts did not stop there. Saddam Hussein has investigated dozens of biological agents causing diseases such as gas-gangrene, plague, typhus, tetanus, cholera, camelpox, and hemorrhagic fever. And he also has the wherewithal to develop smallpox.

*We know.* Powell claims that Iraq has the capability not only to weaponize biological weapons but also to deliver them via state-of-the-art technologies—including unmanned aerial vehicles or drones:

The Iraqi regime has also developed ways to disperse lethal biological agents widely, indiscriminately into the water supply, into the air. For example, Iraq had a program to modify aerial fuel tanks for Mirage jets. This video of an Iraqi test flight obtained by UNSCOM [a United Nations Special Commission] some years ago shows an Iraqi F-1 Mirage jet aircraft. Note the spray coming from beneath the Mirage. That is 2,000 liters of simulated anthrax that a jet is spraying. In 1995, an Iraqi military officer, Mujahid Salleh Abdul Latif, told inspectors that Iraq intended the spray tanks to be mounted onto a MiG-21 that had been converted into an unmanned aerial vehicle, or UAV. UAVs outfitted with spray tanks constitute an ideal method for launching a terrorist attack using biological weapons.

*That is simulated anthrax.* Iraqi jets as well as drones are presented here as a means of threatening not only Middle Eastern states but also the home ter-
ritories of the United States and United Kingdom, a fantastic claim given the distances involved. After this expansive portrait of Iraqi military capabilities, Powell concludes that the weapons inspectors have failed to find the “wmds” and that the threat from these weapons is immediate: “There can be no doubt that Saddam Hussein has biological weapons and the capability to rapidly produce more, many more. And he has the ability to dispense these lethal poisons and diseases in ways that can cause massive death and destruction.” There can be no doubt. Powell’s cartoons and fuzzy pictures of industrial sites appear today, years after the invasion, not simply as a fabrication of knowledge but rather as a tactical deployment of the idea of secret information, for his presentation was loaded with the promise that more detailed and exacting information existed, but that it could not be made public without putting U.S. interests at risk. Indeed, Powell began his presentation to the United Nations Security Council Assembly by stating: “I cannot tell you everything that we know, but what I can share with you, when combined with what all of us have learned over the years, is deeply troubling.”

This deployment of “secret” knowledge relied on the mechanisms and techniques of government that were initially established after World War II to protect information about the atomic bomb—which linked existential threat and covert knowledge production in a new way. The campaign to invade Iraq also drew on culturally established forms of nuclear fear developed in the United States during the Cold War and cultivated for generations. We see here one result of a multigenerational system of state secrecy: a fundamental corruption in the terms of knowledge, where the idea of knowledge (imagined, projected, fantasized) replaces actual content as a means of engaging the world. The “will to believe” (in Iraqi wmds and links between Saddam Hussein and al Qaeda) by the Bush administration remains a staggering achievement of the counterterror state, but it was only enabled as official policy by the structural effects of compartmentalized secrecy, which worked to limit debate, discount all alternative sources of information, and discredit and politicize any course of action short of war. It was not a lack of good intelligence that led to the invasion of Iraq in 2003; rather, it was the long-term corrosive effects of a compartmentalized and politicized worldview on the very possibility of governance. The secrecy/threat matrix is a core tool in the War on Terror, but it has also been revealed to be a highly overdetermined form, one that functions to fundamentally distort both expertise and knowledge. And in a counterterror state where knowledge itself is rendered either suspect or irrelevant, only fear, desire, and ideology remain as the basis for
action in a world constituted as full of emergent and proliferating existential dangers.

Notes

This chapter is excerpted and revised from an article first published in *Public Culture* (22:3) and later appearing in expanded form in *The Theater of Operations: National Security Affect from the Cold War to the War on Terror* (2014).

1 Indeed, the cultural, institutional, and environmental effects of the bomb have been installed very deeply in American society precisely because they are to a large degree constitutive of it after 1945 (Masco 2006; Masco 2014). See also Schwartz (1998), Wills (2010), and Priest and Arkin (2011).

2 President Bush signed Executive Order 13292 in 2003—which permitted classification of “scientific, technological, or economic matter related to the national security, which includes defense against transnational terrorism” (Bush 2003). For reviews of secrecy policy in the Bush administration, see Knezo 2003 and the detailed report prepared by Representative Henry Waxman (U.S. House 2004).

3 See OpenTheGovernment.org (2005a; 2005b) for a detailed assessment of the first George W. Bush administration’s record on secrecy.


7 For a detailed discussion and analysis of the reclassification program in the National Archives and Records Administration, see Aid (2006).


10 Cheney has long argued that a president should not be fully informed about covert actions, to enable plausible deniability in public statements. As vice president, he found various ways of restricting briefing information (including reducing the daily national intelligence estimate to a single page) for President Bush (Suskind 2006, 173–75; see also Gellman 2008).

11 For a transcript of his presentation to the United Nations, as well as images from his slide presentation, see Colin Powell (2003). For a detailed assessment of the biological weapons claims in Powell’s presentation, see Kathleen Vogal (2008).
The categories “for official use only” and “sensitive but unclassified” have recently been replaced by the term “controlled unclassified information,” an official effort to reduce the number of information management markings in the federal government that does not change the core logic of the SBU designation (Obama 2010).

References


