Peter Galison

Secrecy in Three Acts

THE ESPIONAGE ACT: SPYING-SABOTAGING-UTTERING

AT 1:18 PM ON APRIL 6, 1917, THE CONGRESS OF THE UNITED States launched the country into the great European conflict that had been raging for almost three years: "The state of war between the United States and the Imperial German Government, which has been thrust upon the United States, is hereby formally declared" (National Center). In June, Congress passed the Espionage Act, the first act of the three secrecy-defining statutes that have shaped so much of the last hundred years of modern American secrecy doctrine.[1] Along with the two other statutes that followed in later decades—the Atomic Energy Acts of 1946 and 1954, and the Patriot Act of 2001—these three acts picked out inflection points in the great ratcheting process that has expanded secrecy from the protection of troop positions and recruitment stations through an entire field of the physical sciences to almost the whole of government and civil society. Along with a surround of orders, directives, laws, and policies, these three acts ground the modern world of national security secrecy.

Necessarily schematic, my aim here is to follow the long-term history of secrets over the last 100 years, using the debates and cases that encircled them to understand better the governing principles of what information had to be hidden. What dangers did each period identify among that which should be secret? What were the properties and

I would like to thank Jeanne Haffner for her exceptionally helpful research assistance and thoughtful comments; Robb Moss whose collaboration on our film, *Secrecy*, lies behind many of the concerns explored here; and Alex Wellerstein for many fascinating discussions surrounding his original research into nuclear secrecy.

assumed power of these secrets? What could, in the end, properly be declared secret? In short, I am interested in using the acts to fix what it is that secrets were: a historically changing *ontology of secrets* from World War I through the Long War (World War II through the Cold War), and finally into the Terror Wars, our age's unbounded conflict.

The first of our three breakpoints, the 1917 Espionage Act, forbade just the kind of thing you might expect: it laid out stern punishment for anyone convicted of stealing secrets about the national defense in order to harm the United States. Here are proscribed in sections 1 and 2 just the kind of cloak and dagger activities that its title suggested: entering or flying over forbidden sites to obtain information about ships, aircraft, dockyards, torpedo stations, defense works, canals, factories, camps, communications centers, or troop movements. Punishable too would be copying, taking or making sketches, photographs, documents, blueprints, code books or models of defense materials for the purpose of causing injury to the United States. For mere destruction or misuse, the perpetrator could be imprisoned for two years and fined $10,000. As the misdirection of, say, a secret photograph moved toward a foreign recipient, the consequences became graver. Worst of all would be deliberately handing such items in wartime to enemy agents—a crime punishable by death (Espionage Act of 1917; Sedition Act of 1918).

To keep the secrets of the Army and Navy safe from snoops, Congress vested in the president the power to designate any site a *prohibited place.* Other titles within the Espionage Act addressed the danger of sabotage—setting fire, for example, to a munitions factory, or planting bombs on ships. Where an enemy was illicitly observing, destruction could not be far behind. More surprising and fateful for ordinary citizens was that the Espionage Act went on, in section 3, to address *utterances*—the kind of speech or written act that might obstruct recruitment, hamper the success of military force, or, in time of war, precipitate insubordination, mutiny, disloyalty, or dereliction of duty. The move to censor met resistance. President Woodrow Wilson himself objected in a letter to Arthur Brisbane, the New York newspaper editor on April 25, 1917 that

> I sincerely appreciate the frankness of your interesting letter of April twentieth with reference to the so-called Espionage Bill now awaiting action of the Congress. I approve of this legislation but I need not assure you and those interested in it that, whatever action the Congress may decide upon, so far as I am personally concerned, I shall not expect or permit any part of this law to apply to me or any of my official acts, or in any way to be used as a shield against criticism. I can imagine no greater disservice to the country than to establish a system of censorship that would deny to the people of a free republic like our own their indisputable right to criticise their own public officials. While exercising the great powers of the office I hold, I would regret in a crisis like the one through which we are now passing to lose the benefit of patriotic and intelligent criticism.
>
> In these trying times one can feel certain only of his motives, which he must strive to purge of selfishness of every kind, and await with patience for the judgment of a calmer day to vindicate the wisdom of the course he has tried conscientiously to follow (Woodrow Wilson 1917).

What kind of utterances were actually prosecuted? Ves Hall was a rancher from Rosebud Country, Montana. In January 1918, the prosecutor, Assistant District Attorney Homer G. Murphy hauled him before federal district Judge George M. Bourquin, charging him with violating the Espionage Act: interfering with military operations, blocking recruitment, aiding the enemy. From the court proceedings: "At diverse times in the presence of sundry persons, some of whom had registered for the draft, [Hall] declared that he would flee to avoid going to war, that Germany would whip the United States, and he hoped so, that the President was a Wall Street tool, using the United States forces in the war because he was a British tool, that Wilson was the crookedest [censored]-ever President; that he was the richest man in the United

States." Murphy went after the rancher tooth and nail (Nelles 1918: 6; Gutfield 1968: 168).

In his prosecution, Murphy had the full backing of the press, which was owned by the big mining companies. Federal District Court Judge George M. Bourquin shrugged off the pressure from both the extraction industry and from the Justice Department itself—refusing to be shoved into convicting war-resisting "slackers." In the Hall case, Bourquin found that the loud-mouthed fellow had, in fact, said the things of which he was accused, but had done so in a village with a population of 60, 60 miles from the railway and thousands of miles from the frontlines of the armies and navies he was supposed to have wounded with words: "The declarations were oral, some in badinage with the landlady in a hotel kitchen, some at a picnic, some on the street, some in hot and furious saloon argument" (Nelles 1918: 6). Thanks to the nonpresence in Montana of a great naval fleet or army, the judge judged that Hall did not seem to have had an intent to interfere with their operations. In Bourquin's view, someone who shot another with a .22 pistol from three miles away could hardly be convicted of attempted murder—so it was with Hall; his verbal assault was so distant from its target that there simply was no plausible case to be made for interference with military operations or recruitment (Gutfield 1968: 168-169).

More likely than Hall suddenly sinking the U.S. Navy, Bourquin added, would be Hall getting a "broken head" in a barroom brawl: "The Espionage Act is not intended to suppress criticism or denunciation, truth or slander, oratory or gossip, argument or loose talk," but only actual obstruction or injury to the military. The idea, he concluded, that slanderous or disloyal talk could get the utterer prosecuted by the United States "is a mistake." The court acquitted Hall, though not without a roar of disapproval from the nationalist press and the impeachment of one of Hall's character witnesses, Judge Charles L. Crum (Nelles 1918: 6-8; Gutfield 1968: 163).

Prosecutors were more successful in their October 1917 indictment of 27 Socialist farmers in Hutchinson County, South Dakota, with Emanuel Baltzer as the lead defendant. The accused sent a petition to

the sheriff, treasurer, and auditor of Hutchinson County and to the governor of the state, arguing that the people were against the draft, that the county quota was unfairly fixed, and a referendum on the war and draft was needed. Ignoring this petition, so said the farmers, would "spell sure defeat for you and your party." The charge here was that the accused had deliberately interfered with an official's discharge of his duties to run the draft. Judge F. A. Youmans instructed the jury to assess whether the defendants were in conspiracy and whether their actions willfully obstructed the draft. The jury convicted, but the district court's decision was reversed by a higher court on December 16, 1918 (Nelles 1918: 17-18).[1]

On August 29, 1917, in the Southern District of Georgia, the postmaster sought to block mailing privileges for "The Jeffersonian" under the Espionage Act. A bill came before the court to remove the block. The court read from the Espionage Act and admired the "light . . . of a valid and vital law" that shone upon the dark, nefarious pages of "The Jeffersonian." In contrast to the subversion of those pages, the prosecutor urged the court to think of the "thousands of the elite of the American army [who] were on the soil of France." Then came a patriotic hymn: "At any moment the crash of their rifle fire and the thunders of their artillery in the vindication and defense of human liberty might be heard. American men-of-war manned by Americans were swiftly cleaving the waters forbidden by the enemy to our commerce, questing every billow for his lurking and deadly craft." Every strong-hearted American was rising to the occasion: "[G]allant youth of every American State were rallying to the Flag . . . over-subscription of the Liberty Bonds . . . self-sacrificial spirit of women . . . our country's daughters were no whit behind her sons" (Nelles 1918: 31). In contrast to these patriots, the prosecutor introduced some offending passages from "The Jeffersonian":

- "Men conscripted to go to Europe are virtually condemned to death and everybody knows it."
- "Are we, like the sow returning to her wallow and the dog to his

vomit, to go back to the medievalism of personal rule, a Pope's word ruling the church and a king's word ruling the state? Why not call Woodrow Wilson by the name of King, or Kaiser, or Czar. . . ."

- "What about a car load of German soap made out of our boys? What about manuring German fields with our bravest youths, and fattening German hogs on the choicest selection from American manhood? I raised my boy to be a soldier says the song, but did mother raise him to be a pig feed?"

Should the postmaster have let such propaganda wend its way through the mails, then, so said the prosecutor, he would have contributed to the bloody defeat of a demoralized American army. The world would have beheld the degradation of America, its "disintegration under fire" not unlike the ignominous defeat of the Russian army, brought about "by methods much the same . . . the destruction of [America's] institutions and the perishing of popular Government on earth." The judge agreed; the mail ban imposed on "The Jeffersonian" would be maintained (Nelles 1918: 32-33).

Cases like those of Hall, Baltzer, and "The Jeffersonian" all involved putatively false, willful, and potent disloyal statements. But even that wide radius was not enough: censorship could reign even when the *truth* of the utterance was indisputable, that is where there was clearly no violation of Section 3 (the willful making of false statements). That much is clear from the November 1917 case of Robert Goldstein, a 34-year-old Jewish costume store owner who, in 1917, produced a film, *The Spirit of '76*. Judge Benjamin Franklin Bledsoe, from southern California, conceded that the film made excellent use of such prominent and laudable phases of the war as Paul Revere's ride or the signing of the Declaration of Independence. But *Spirit* showed some things that wouldn't do at all: the Wyoming Valley Massacre (1778, in Wyoming Pennsylvania), for example. Worse, it depicted a British soldier "impaling on a bayonet a baby lying in its cradle and then whirling it around his head so impaled." Loyalists shot harmless young women, and, in preparation for "unspeakable" aims, the redcoats could

be seen on screen "dragging off, sometimes by the hair of the head, . . . young American girls" (Slide: 1993: 207-208).

Now, Bledsoe reckoned, the United States was in the midst of "the greatest emergency we have ever . . . confronted," which was no time for anything that might limit efficiency of the cause. Depicting the perfidy of the British was precisely that. "History is history, and fact is fact. There is no doubt about that. . . . It is a fact that we were at war with Great Britain during the Revolutionary times, and whatever occurred there is written upon the pages of history and will have to stand, whomsoever may be injured or hurt by the recital or recollection of it." But facts, Bledsoe insisted, have their time and place. Sowing dissension, creating animosity or lack of confidence between allies—this was a real danger "because so to do weakens our efforts, weakens the chance of our success, impairs our solidarity, and renders less useful the lives we are giving, to the end that this war may soon be over and peace may soon become a thing substantial and permanent with us." The result: *Spirit* seized, Goldstein jailed. He struggled for rehabilitation, and indeed President Wilson eventually pardoned him after the war. Still, he spent the rest of his life struggling for rehabilitation. In the 1930s, Goldstein went scrounging for movie funding in Germany, and very probably died in the Holocaust, for want of the nine dollars he needed to renew his American passport (Slide 1993: 209-210; Noah 2000).

All these cases (Hall, Baltzer, "The Jeffersonian," Goldstein) took place between August 1917 and January 1918. The war continued, bloodily, and chauvinism extended its reach. On April 15, 1918, U.S. Attorney General Thomas Watt Gregory read an address to the American Bar Association, and a few weeks later it was read into the *Congressional Record.* Lynching, the attorney general said, was the most cowardly of crimes, and a purported German sympathizer lynched in Illinois was guilty of nothing, his death the product of a mob frustrated by its sense that the government was not doing anything. The attorney general pressed the Bar Association on the point: "to give you an idea of the ineffectiveness of the [Espionage Act], I refer to celebrated case recently

decided by a district judge [Bourquin] of the United States, which will give you an idea of how impossible it is to enforce it in some jurisdictions." That case—Ves Hall's—was an affront to the attorney general, a clear sign that disloyalty could go unpunished. Even a German, chemist Walter T. Scheele, who had plotted to sink vessels on the high seas with incendiaries, got away with a mere $2,000 fine. "Hanging would have been too good for that crime, because women and children with no protection were on those vessels." With 1,500,000 male aliens enemies over 14 years of age, the attorney general suggested that each such man or young man belonged to a family of at least three, and so concluded that there would be 4.5 million "enemy aliens within our borders. This will give you an idea of the size of the problem." Somewhere between reporting and agitating, he intoned, "from every side section of the country comes up the cry that the disloyal and seditious should be tried by military courts-martial and promptly shot." That, the attorney general said, might be going a tad too far. Civilian courts could do the job if lawyers rose to this national emergency (All quotations in this paragraph from *Congressional Record* 1918: 6233-6234).

Reaction to the Ves Hall acquittal was a key event in the formulation and passage of the May 1918 amendment to Section 3 of the Espionage Act. This expansion became known as the Sedition Act, and held sway until its repeal in 1920. *Dangerous language* loomed even more powerfully as a major problem—language spoken, printed, written, or published. Examples of the revised section Espionage Act included these:

- Whoever, when the United States is at war, "shall willfully make or convey false reports or false statements with intent to interfere" with the military;
- Whoever shall "make or convey false reports or false statements . . . with intent to obstruct the sale by the United States of bonds";
- Whoever . . . shall willfully utter, print, write, or publish any disloyal profane, scurrilous, or abusive language" about the form of U.S. government;
- Whoever shall utter, print, write or publish "any language intended

to bring the form of the government of the United States, or the Constitution of the United States, or the military or naval forces of the United States, or the flag of the United States . . . into contempt, scorn, contumely, or disrepute";

- Any official or employee of the U.S. government who "utters any unpatriotic or disloyal language, or who, in an abusive and violent manner criticizes the Army or Navy or the flag of the United States" (Nelles 1918: 1-2).

Arise the civilian courts did. Walter Nelles, the Yale law professor and pacifist who assembled précis of the various Espionage Act cases, reported that there had been 877 convictions under the act between June 30, 1917 and June 30, 1919. No doubt great harm had come to them and the many other cases prosecuted but not convicted. But Nelles worried in *The Nation* of December 1920 that the real damage went farther: the act had "cowed minds." Though by the end of 1920, the legislation had fallen dormant, Nelles found that minds had been all too well mobilized, "incapacitated for independent thinking." And a legacy of "vague and disingenuous statutes" allowed people to be prosecuted not for *real* injury to the Army, Navy, or recruitment offices, but instead for having spoken their minds. Many of the jailed had said no more than President Wilson himself in St. Louis on September 5, 1919: "Why, my fellow-citizens, is there any man here, or woman, who does not know that the seed of war in the modern world is industrial and commercial rivalry? This war was a commercial and industrial war. It was not a political war" (Nelles 1920: 684). Nelles blasted the Supreme Court for having backed Espionage Act prosecutions, even when there was neither "visible and tangible harm" nor proof of "causal responsibility." This, Nelles warned, amounted to the imposition in America of the old English infractions of seditious libel and constructive treason. Prosecution for "reason to believe" was, he concluded, a fundamental threat to the First Amendment.

At first blush, the Espionage Act offers a puzzle: How did classical espionage (photographing a "prohibited area," or sequestering a

code book) find an easy grouping with the denunciation of President Wilson as a British tool or the cry that young Americans would end up fertilizing a French battlefield? But espionage joined sabotage in the dark crimes of enemy agents; and sabotage carried over in practice to include utterances that, the state contended, causally and proximately blocked the capacity of the armed forces to recruit or fight.

Agitated times: Franz Bopp the German consul in San Francisco, sat accused of conspiring to blow up American munition ships. On the day filmmaker Robert Goldstein's trial began, the *Los Angeles Times* put a picture on its front page depicting the canvas sign advertising *The Spirit of '76*, damaged by winds to read *Spi '76*. Superimposed on it were images of Goldstein and Bopp with the headline "Dynamiter of Munition Ships Goldstein 'Angel'?" Forbidden knowledge, the unutterable, extended its domain. In the writing and application of the Espionage Act, words became acts, judged as if they were bombs.[2] Aim near with a weapon and intent, you could be convicted for attempted murder; aim far and wide, and you might go free.

Espionage in the midst of World War I may at first seem to be trench-coat spies with secret cameras and furtive saboteurs with hissing firebombs. But it soon became much more than that: a great dragnet for purportedly dangerous words, a campaign that prosecuted thousands of cases and drove the first, not the last, of a large-scale political repression behind a façade of counterespionage. Though the excesses of the expanded Section 3 were repealed in 1920, the larger structure of the Espionage Act remained, amended numerous times to take account of new technologies and new threats—and remains in force into the twenty-first century.

THE ATOMIC ENERGY ACT (1946, REVISED 1954)

Battles in World War I turned on many factors: troop numbers, endurance, weather, machine guns, and, though in fewer instances than is often thought, poison gas. But taken in its totality, World War I was not, in the main, a technological war, at least not in comparison with its sequel, which began in 1939. Measured by budget, personnel, or weap-

ons, the Second World War, far more than the First, was a battle of technology and science. Radar took a key role, both in directing bombers to their targets and in defending those targets from attack. But though the "battle of the beams." as it was called, raged furiously, secrecy was a short-lived affair. British and German scientists were constantly detecting and countering the other side; a radar set at the cutting edge of 1943 was thoroughly obsolete and not worth protecting in 1944.

Though the Manhattan Project itself operated during World War II under the legal cloak of the Espionage Act, within weeks after Hiroshima and Nagasaki debate began about what kind of secrecy would reign over all things atomic. More than any other technology, a new scope, scale and even ontology of secrecy entered, orbiting, as it were, around the nucleus. Many scientists demanded openness about the new world of heavy nuclei and their properties. Enrico Fermi commented, "Unless research is free and outside of control, the United States will lose its superiority in scientific pursuit" (Hewlitt 1981: 20).[3]

For politicians, especially the conservative politicians who dominated congressional discussion, the fear above all else was that the technology of nuclear weapons would be passed to potential enemies. In the "Dissemination of Information" section of the 1946 Atomic Energy Act, the bill tried to split these two realms. Senator Brien McMahon, who took the atomic bomb to be "the greatest thing since Jesus Christ," was keen for restriction, and his original bill insisted that fissionable material along with all facilities and fissionable materials would belong to the Atomic Energy Commission (AEC), compensating, if necessary, the inventor. Section 9 (Dissemination of Information) of the original bill guaranteed that basic scientific information about atomic energy would be distributed in libraries and publications with "related technical information" that were determined not to harm national security. But even information not so determined was not, for that, automatically in violation of the Espionage Act.

As the bill moved through hearings, it became increasingly restricted. "Control of Information" (Section 10) displaced the older ambition for "dissemination." And though the bill did not use the later

term "born secret," the act as passed promoted the category, "restricted data" to include any information about the manufacture or use of fissionable material, nuclear weapons, or nuclear power—unless that information was *de*-classified by the AEC. Scientists protested in vain. The commission backed up a powerfully inclusive notion of secrecy with severe punishment for violation. Distributing information to any foreign nation with intent to injure the United States may be "punished by death or life imprisonment" (Hewlitt 1981: 20-21).

More specifically, what misuse of restricted data would precipitate punishment ? Anyone who communicates, transmits, or discloses restricted data with intent to injure the United States or secure advantage to a foreign nation could be punished by death or life imprisonment. Anyone who moves the restricted data with "reason to believe" that their communication, transmission, or disclosure will injure the United States or secure advantage to a foreign nation could face up to 20 years in jail and/or up to a $20,000 fine. Indeed, death or life imprisonment could be punishment for conspiring to acquire restricted data with intent to injure the United States—as could any attempt to alter, mutilate, or destroy documents or materiel used in the production of fissionable material (Atomic Energy Act 1975; Newman 1946-1947: 781-782).

By lumping together knowledge from theoretical nuclear physics with the fabrication of isotope separation devices, the Atomic Energy Act of 1946 eroded the distinction between pure and applied science. Through patent law it also began to eat away at the distinction between official secrets and private secrets (Newman 1946-1947: 781-782). Though perhaps surprising in retrospect, the atomic bomb project was debating the role of patents from the beginning. The Office of Scientific Research and Development had two contracts. One was short—it did not need much elaboration since it turned over to the government all power to dispose of rights in discoveries and inventions. When this full surrender form met resistance among key industrial entities, the government wrote up a long form that left the contractor with the title, but ceded to the government rights for use in national defense. As the

Manhattan Project rose in scale, the big contractors—Standard Oil and then Columbia University, the Kellogg Company, DuPont, and others—agreed to the shorter, more direct form of government control.

But this full concession was temporary. When the shooting stopped, suddenly patents, ownership, and the prospects of a vast new industry brought intellectual property front and center. On February 11, 1946, hearings took place before the Senate Special Committee on Atomic Energy. Captain Robert A. Lavender (chief patent adviser to the Office of Scientific Research and Development, or OSRD) responded to questions:

> The Chairman: If an individual or a company works in the atomic energy field at his own expense, there would be no way that you could get hold of [the patent]?
> Captain Lavender: There is one part of the Espionage Act, which requires that information involving national defense come as a result of some relation with the Government. The Government could go to the inventor and place him under the Espionage Act, and he would not be permitted to disclose his invention.

In practice, the commissioner of patents would report the patent to the Atomic Energy Commission, and the AEC would have authority to purchase it or otherwise gain control. Lavender: "this is in effect the seizing of the invention and restricting the inventor under police power" (Senate Hearings on Atomic Energy 1946: 11; "Atomic Bomb Patents" 1946: 30-31). Just this seizure and police power restriction put many on alert. Suppose you were cautious enough not to publish, in order to avoid transmitting the atomic energy invention to foreign nations to their advantage, or worse, to the injury of the United States. You still would not only need to guard your own morals, your own intent, but also monitor those within the United States to whom you conveyed your ideas. For just this reason, the Atomic Energy Act of 1946 met with shock among many in the legal community. James R.

Newman, who had been counsel to the Senate Special Committee on Atomic Energy, warned in the *Yale Law Review* that "one must also judge the loyalty, patriotism and discretion of those with whom one communicates and run the risk of imprisonment if this judgment should prove erroneous" (Newman 1946-47: 787). Newman continued: "the unprecedented provisions which prescribe the death penalty in peacetime for such an offense as 'mutilating' a 'sketch' relating to research on atomic energy partially financed by federal funds can be ascribed only to superstitious dread. Terror of the atomic bomb is natural and understandable—perhaps even healthy; but terror at the loss of the 'secret' is a tribal fear which, once gaining ascendancy in our minds, must inevitably weaken rather than strengthen our defensive power as a nation" (782-783).

Bit by bit, over the course of 1946, 1947, and 1948, the wheels of declassification turned. Certain categories of Manhattan Project secrets cracked open to allow the outside world to catch a glimpse of the myriad advances that had been gained in nuclear instrumentation, mathematical techniques, particle accelerators, chemical processes, medical and health studies, and "properties of elements below 90." So the properties of the basic elements of the universe were for all to see—at least those that ran from hydrogen, helium and up through francium (87), radium (88), and actinium (89). But the commission left a *ne plus ultra* on the periodic table just to the right of actinium: beyond it lay the forbidden zone of thorium (90), protactinium (91), uranium (92), neptunium (93), and plutonium (94). But the draconian web of secrecy that had covered the Manhattan Project—backed in many ways by the 1946 Act—began to fray in the immediate postwar years as scientists, industry, and foreign powers began to dig into the atom. Hearings in the 1950s led to a significant revision to the act in 1954.

The problem in formulating the 1954 act was the same one Congress had been grappling with for years. The government was caught between a rock and a hard place: on one side it wanted to encourage scientists and industry to advance the technology and science of all things nuclear. To encourage work on nuclear power, the 1954 act

allowed private companies access to relevant restricted data if they followed AEC security and secrecy stipulations. The new act partially opened exchange with foreign countries, and it liberalized a few of the patent provisions. By the 1960s, pressures of another sort emerged as foreign companies began developing uranium centrifuge technology. Open communication could, the AEC hoped, maintain a modicum of control (Hewlitt 1981: 21-22).[4] On the other side, the early 1950s were McCarthy days and the terrible fear of disloyal scientists and an uncontrolled industry. The problem of the widening gyre of secrecy caught the attention of some in Congress. In one hearing about amending the Atomic Energy Act of 1946, Representative Carl T. Durham put it starkly:

> Rep. Durham: Do you think it would be possible, or would it be reasonable, for a physicist who has of course full knowledge of practically all of these developments, who has never had contact with the AEC, who has never seen a classified document, to write an article in a newspaper which could be construed as being classified material? It looks to me like it is possible."
>
> Oscar Ruebhausen [Chairman of the Special Committee of the New York City Bar Association]: "I am very troubled by it, too, sir. . . . It is the complete absence of any exception for the wholly innocent communication which bothers me. Maybe we have no other alternative than to penalize the innocent with the guilty. But before we do it, it is a very drastic step, and I know the committee will search for ways to soften it" (Cheh 1979–1980: 186).

By collapsing scientific ideas, technological principles, and device design into the conglomerate category of "restricted data," Congress made almost any kind of disclosure punishable. Since so much of nuclear bomb and energy production was technical-industrial, it became ever more plausible to Congress that the secrets of the bomb

could be controlled by restrictions on patents. In fact, considerable controversy surrounding the atomic energy bill swirled around patent provisions. Essentially, the government claimed a form of intellectual eminent domain: nonpatentability, compulsory licensing, and government acquisition by a sweeping, a priori condemnation of the entire field. Inventors had to disclose to the commission any work useful in the production of "special materials" for power or weapons and notify the AEC of all patent applications falling in the government's nuclear dominion (Risenfeld 1959: 40-68).[5] For its part, the AEC would establish a Patent Compensation Board that would compensate the inventor, the way the government paid a family whose house it had condemned to build a highway.

Unlike a condemned piece of land, however, the condemned intellectual property was not something that already existed and for which positive government action was required. Here, in the nuclear domain, an entirely new process, device, or design could come into existence and be subject automatically and *from the outset* to condemnation by eminent domain. If it had to do with nuclear power or nuclear weapons, it was, as the philosophers would say, "always already" subject to government licensing, whether secret, partially secret, or open.

Here is a real case from January 1955 that illustrates precisely how the government and courts put the atomic patent monopoly into action, though in this instance the device was seized but not held secret. Harold Washburn of Consolidated Engineering Corporation had in hand three patents one from 1948 (first submitted in 1943), along with two from 1952, to defend the company's invention of a new kind of mass spectrometer, an instrument that can determine the chemical and isotope content of a gas. In particular, it could distinguish the relative presence of U235 from U238.

Consolidated Engineering, argued that the government had manufactured and used its G-107 line recorders without license—and so should pay compensation.[6] For its part, the Atomic Energy Commission frankly admitted that it was using "G-107 line recorders" equivalent to Consolidated's device. But the government claimed that the Atomic

Energy Act of 1946 excluded the suit, citing the statute "No patent [granted after 1 August 1946] shall confer any rights with respect to any invention of discovery to the extent that such invention or discovery is used in the production of fissionable material or in the utilization of fissionable material or atomic energy for a military weapon." The nuclear authorities contended that "used" in the act meant that the government not only had the right to employ but also to manufacture the invention. In reply, Consolidated said, first, that since their instrument was an analyzer, it was not part of the "production" process, and second, "used" did not convey the manufacturing rights (Van Young 1979: 28-32; 131 Ct. Cl. 819; 127 F.Supp. 558 1955).

The court zeroed in on those two questions: was the G-107 part of production, and did the Atomic Energy Act seizure of patents also confer control over manufacture? All existing methods of separating U235 from U238 involved preparing a gas, uranium hexafluoride. One method, the dominant one in World War II, came from diffusing that "hex" as it was called, through porous material. It was slow—each step in the diffusion let a bit more of the lighter U235 through than it did the heavier U238. On the far end of a barrier, the enriched gas (having a larger percentage of U235) was pumped out and delivered to the next barrier. After some 5,000 or so passages through porous barriers ("the cascade"), Oak Ridge could produce about 1 kg per day of highly enriched uranium—that is, almost pure U235 for a Hiroshima-type bomb every few weeks (1 kg/day from Van Young 1979: 30, from the Smyth Report).

In a typical civilian patent infringement suit, the accused would argue that the device was not much like the one the plaintiff held up for the court's examination, and then shrug off the purported infringement as incidental to the core of the defendant's industrial process. Here, in the upside-down black world, the logic functioned backward. The AEC insisted, with the aid of scientific evidence provided by John R. Mahoney, assistant superintendent of the Instrument Engineering Department for Carbide and Carbon Chemicals Company at Oak Ridge, that the line recorder was a fundamental, permanent, part of separa-

tion. It was, Mahoney contended, part of Carbide's operation at Oak Ridge, part of the isotope separation plant at Paducah, Kentucky, and would soon be part of a uranium enrichment plant being constructed by Goodyear Atomic Corporation at Portsmouth, Ohio. Only by monitoring the isotopic and chemical purity of the product could the whole process function:

> This information permits correction of malfunctioning of units of the cascades and thus secure[s] the optimum rate of production of the uranium isotope of mass 235 having the required chemical and isotopic purity and that the uranium isotope of mass 235 could not be produced with the required chemical and isotopic purity at the present production rats in the existing gaseous diffusion cascades without the use of Line Recorders. The separation of uranium isotopes by diffusion results in a concentration of the isotope Uranium 235 which is a fissionable material as defined in Section 5(a) of the Act. Defendant urges that this constitutes a production of fissionable material within the meaning of the Act (131 Ct. Cl. 819, 127 F.Supp. 558 (1955)).

The court concurred with the AEC, removing any claim that Consolidated Engineering might have: the patents held no protection for the plaintiff; having proven their worth within the apparatus of U235 production, the government had control. Judge Benjamin H. Littleton wrote for the court: "We hold therefore that the plaintiff's patents conferred no rights with respect to the inventions which were used or manufactured to be used in the specified instances in this case. The plaintiff obtained no rights under the patents insofar as and to the extent that the patented items were used by the defendant. It follows then that there can be no recovery" (131 Ct. Cl. 819, 127 F.Supp. 558 (1955)).

Alongside claims like that of Consolidated, there were lesser plaintiffs—like the retired dentist Cornell Joel Grossman, who

claimed to have a particularly lethal Nitro Hydrogen Bomb that would be produced by placing powdered uranium in a "High Voltage High Frequency Electro Thermic Furnace" and allowing it to explode—or by dropping in some potassium nitrate and zirconium powder, or maybe, the inventor added, some tanks of arsenic, hydrogen, and fluorine. Denying the claim, the Patent Compensation Board found nothing useful for the utilization of atomic weapons (or anything else) and, to nail the case closed, pointed out that the dentist had failed to submit his case within the required 60 days of August 1, 1946 (Van Young 1979: 42).

If Dr. Grossman had considerably less than Consolidated Engineering to offer the weapons program, there were others that had considerably more. Enrico Fermi and his colleagues had a claim on the use of slow neutrons to induce nuclear reactions (slow neutrons are essential to building a nuclear reactor). This discovery was key—reactor moderators that slow neutrons are central to the production of plutonium, including, of course, the fissile Pu core used in the bomb dropped on Nagasaki. Their patent, 2,206,634, "Process for the Production of Radioactive Substances" was issued on July 2, 1940 to Fermi, Edoardo Amaldi, Bruno Pontecorvo, Franco Rasetti, and Emilio Segrè. The reactor men spent years pursing $1,000,000 for their claim (at one point considerably more than that); in 1953, they were given $300,000. Glen Seaborg first separated plutonium—he too made a claim for which he received $100,000 in compensation. Physicist Herb Anderson, who had made key contributions to the uranium lattice in the reactor, filed late, but effectively, to get an award. The Patent Compensation Board: "[The purpose of the award provision] is to encourage and stimulate continued private research and activity in a field in which the government in the overall defense has necessarily circumscribed the proprietary recognition usually accorded invention" (Van Young 1979: 54).[7]

In comparing the Espionage Act with the Atomic Energy Act, we could focus on any one of a myriad contrasts. There are many similarities, intentionally so. The transmission of secret information to the enemy is forbidden—as are acts of sabotage. Language such as "docu-

ment, writing, sketch, photograph, plan, model, instrument, appliances, note or information" is taken nearly directly from the Espionage Act. So too are the crimes of using such material to "injure the United States" or to "secure an advantage to any foreign nation." Even the Atomic Energy Act's graduated system of punishments march in parallel to the Espionage Act—from fines up to a death sentence.

In contrasting the Espionage and Atomic Energy Acts there are three salient points that bear on changes to the referent of the hidden. First, unlike actions proscribed under the Espionage Act, atomic secrets are much less dependent on the status of the secret keeper: a scientist in a private laboratory, not privy to secrets, not in receipt of government funds, could be jailed for publishing his results if he had "reason to believe" that doing so would injure the United States. So secrets in the nuclear domain were more autonomous, in the sense of being freer from questions of intent or contractual status.[8] Second, the Espionage Act has "prohibited places," mainly government owned or controlled defense facilities: naval yards, coaling stations, arsenals, and railroads. These continued into the Atomic Energy Act—the fenced-off sites of Los Alamos, Sandia, Oak Ridge, Hanford, many of which were taken by the government by eminent domain. But the Atomic Energy Act extended this not only beyond the government's own sites but to all those places where secret work was taking place. Moreover, it broadened the government's eminent domain to the intellectual sphere—claiming monopoly power over fissionable materials (later the more general "special nuclear materials"), manufacturing sites *and* know-how. Any nuclear property, physical *or* intellectual, could be brought under government control (Newman 1946-1947: 792).

Third, the Espionage Act reserved its harshest punishment for acts intended to injure the United States when committed in wartime. This made sense, since the secrets themselves had a finite lifetime: troop positions, fort layouts, access points to munitions factory. By contrast, the Atomic Energy Act can mete out death or life imprisonment for restricted data abuse *even in peacetime*. Nothing in the Atomic Energy Act edicts about secrecy violations makes reference to war: secrets in the

nuclear domain could be permanent. That is, though you could block knowledge of a weapon invented, it was generally to be held in the netherworld of secrecy only until the end of hostilities. Nuclear weapons had no give-away date—because they are never so completely out of date as an obsolete howitzer or the address of the hotel where General George Patton was staying.

The eternal threat of even a crude nuclear weapon gave the "born secret" doctrine an entirely new meaning. We could say of nuclear weapons knowledge: born secret, some atomic secrets never die. This then is a shift in the ontology of secrets, with many structural implications. For example, during the Cold War, it might have seemed reasonable to respond to the challenge of dealing with *semi-infinite* dangerous knowledge (created in a time and place, then never obsolete) with monopolistic government control. Patents, key to that fabrication, would then seem a fitting instrument of that monopoly. When it came to the assessment of threats (and therefore the levying of punishment), we can ask: What could, in the eyes of the security establishment, alter the balance of power away from the United States? In World War I, these actions clearly included utterances as well as "traditional" spying and sabotage. Censorship seemed in 1917–1919 to be a riposte to these dangerously efficacious utterances. Black ink, postal repression, and jail terms for forbidden speech appeared to be precisely analogous to fences and guards.

What sort of thing might slide the balance of power away from the United States in the Long War? That might occur through espionage, of course—Ted Hall, Allan Nunn May, Klaus Fuchs, and Julius and Ethel Rosenberg—in addition to the fears of sabotage (destroying sketches, breaking equipment, etc.) But in the new world of scientific-technical secrecy, authorities feared as well the wrongful dissemination of knowledge to the wider world through an article or patent.

THE PATRIOT ACT: THE ETERNAL, PLANETARY BATTLEFIELD

With the end of the Cold War, the eerie oppositional symmetry broke. No longer was nuclear-tipped warhead pitted against nuclear-tipped

warhead; no more nuclear submarine duets in the North Sea. An end to target teams matching Soviet against American missile silos, White House against Kremlin. With the terror wars raging across the globe, sites previously invisible to the targeters—passenger trains, shopping centers, sports stadiums, monuments—suddenly came all too clearly into view. It is to this targetable infrastructure that we now turn to unravel the nature of secrecy in this, our time.

Back in the 1990s, President Bill Clinton issued an Executive Order (12958) that simplified and unified the classification system. One section, 1.8(b) forbade the status "classified" from being applied to "basic scientific research information not clearly related to the national security." After September 11, 2001, the whole system of national security began to shift, first with the Patriot Act (October 26, 2001) and then in a host of other alterations to the law. One key change in the secret universe was President George W. Bush's Executive Order 13292 of March 25, 2003 that amended Clinton's on classification. For Bush, the goal was to provide a system of information control that would continue the older "scientific, technological, or economic matters relating to the national security," but added to it the clause that this should "include defense against transnational terrorism" (Federal Research Division 2004: 1). The government would seek as well protection to cover (new language in italics) "vulnerabilities or capabilities of systems, installations, *infrastructure*, projects, plans, *or protection services* related to the national security, *which includes defense against transnational terrorism*." With this new vocabulary, especially in the inclusion of *infrastructure*, lay a sea change in the ontology of secrecy (Federal Research Division 2004: 1).

Never before had infrastructure per se been the referent of the secret, blacked-out word. But what was infrastructure? What came under this heading and how did it alter over time? Executive Order 13010 (July 15, 1996) by President Clinton defined critical infrastructure as societal structures "so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States." That, in 1996, included telecommunications, elec-

trical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply, emergency services, and continuity of government. New to this range of the vital was the addition of threats to electronic, radio frequency or computer based structures—"cyber threats."[9]

Just two years later, on May 22, 1998, Clinton came back to these issues with Presidential Decision Directive/NSC-63, Critical Infrastructure Protection: "The United States possesses both the world's strongest military and its largest national economy. Those two aspects of our power are mutually reinforcing and dependent. They are also increasingly reliant upon certain critical infrastructures and upon cyber-based information systems." NSC-63 set a national goal: before the year 2003, the United States should have achieved the ability to protect the critical infrastructure from assaults that the federal government could perform its national security missions, public health and safety; local governments could maintain order; and the private sector could continue the delivery of communication, energy, finance, and transportation. This meant appointing "lead agencies"—(for example, Commerce would stand at the front for information and communications, CIA would lead foreign intelligence), with the whole woven together through a new and more efficacious communication (White House 1998).

The September 11 attacks jumped the secrecy ratchet several more sprockets. President Bush issued a new Executive Order, 13228, on October 8, 2001, establishing the Office of Homeland Security and the Homeland Security Council: "The Office shall coordinate efforts to protect the United States and its critical infrastructure from the consequences of terrorist attacks," working with all levels of local and federal, private and public entities. Defining the critical infrastructure to include energy, transportation, or communication was by then routine—but Bush went on to include nuclear use, storage or disposal as well. These had to be protected from terrorist attack; new too were information systems or major public events, whether public or private. For the first time, agriculture and livestock, and more generally

"systems for the provision of water and food for human use" joined the widening circle of critical infrastructure to be guarded against terrorist attack—alongside a broad protection against chemical, biological, or nuclear materials that might be incorporated into such an assault.

Already before 9/11, the ambit of the hidden was spreading like black ink across a blotter; talk of asymmetric warfare had been on the rise just at the moment when the Cold War enemy was receding. But 9/11 crystallized the terrorist as the opposition and therefore also drew a line around who would be battling them and with what means. Introducing a "National Strategy for the Physical Protection of Critical Infrastructures" in February 2003, George Bush wrote: "The September 11, 2001, attacks demonstrated the extent of our vulnerability to the terrorist threat. In the aftermath of these tragic events, we, as a Nation, have demonstrated firm resolve in protecting our critical infrastructure and key assets from further terrorist exploitation." Only a combination of government, private sector, and "concerned citizens across the country" could counter threats ranging from the aviation industry to the 8,000 or so major dams; from nuclear reactors to chemical refineries—along with the fragile cyberstructures that controlled them. Key assets broadened the remit of infrastructure protection to embrace the "national monuments, symbols and icons" that stand for "our Nation's heritage, traditions and values, and political power." The "National Strategy" warned that tourists and the media flock to these symbolic sites, making an attack on them consequential and their protection vital to the preservation of public confidence. And once monuments, symbols, and icons were in the mix, so too, the report reasoned, should commercial centers, office buildings, sports stadiums. Reading the list makes one think back on Cold War target lists as modest indeed. Bush framed the national strategy with a picture of the opposition: "The terrorist enemy that we face is highly determined, patient, and adaptive" (U.S. Dept. of Homeland Security 2003: 71-72).

As the "National Strategy" began to grapple with this extended dominion, it leapt ever farther into new sectors of society. Mere "systems," that great categorical entity of the Long War, now seemed

too modest. The "National Strategy" enjoined policy makers to consider not only the systems they had to protect, but the "system of systems." Indeed, now that the terrorist enemy had been revealed as so capable ("creative" and "adaptive," showing "determination" and "sophistication"), a new anti-terrorist alliance would have to form, one that would not be held even to the national boundary. "Terrorists do not respect international boundaries," the report opined: the infrastructure protection effort would have to embrace Mexico, Canada, and friendly countries around the world. (U.S. Dept of Homeland Security 2003: 81-82). This was planetary warfare, and as became clear from the ever-shifting designation "enemy combatant," the battlefield could be anywhere from Arizona to Azerbaijan.

The scope of critical infrastructure expanded. So too did "critical infrastructure information" (CII), which would reveal its workings. Sometimes the definition bends the mind, as in this excerpt (one of five criteria) from a comprehensive sourcebook: "CII is specifically defined consisting of any of the five criteria, such that it: 1. Represents information directly relating to specific data, tasks, or information relating to any given critical infrastructure." Stripped down, that would include "information representing information relating to information relating to infrastructure" (there are, it seems, grammatical as well as terrorist enemies). One suspects (after some parsing) that the designation "critical infrastructure information" is mainly information about the operation and vulnerabilities of specific sites and networks. Operations having to do with everyday procedures ought be kept under wraps because they could provide guidance about how to interfere. Vulnerabilities would include not only gaps in security arrangements, revealing access points or maps, but also cyber, meteorological, or seismic threats (Radvanovsky and McDougall 2010: 161).

This immense and growing world of infrastructure and information about infrastructure fell largely outside the Cold War bounds on classification. This was not information about agents, cryptography, foreign relations, or for that matter about intelligence activities, sources, or methods. Nor were these strictures about infrastructure

also about weapons systems—or nuclear facilities, materials, or weapons. No, this was about the aviation industry, passenger trains, and water conduits—electrical generators, oil refineries, and telephone switching stations. Before September 11, by and large information about the operations and vulnerabilities of infrastructure had not been classifiable. By the end of October 2001, that had begun to change.

But there was another logic at work, quietly expanding the blacked-out dominion. It had begun out of public site with a plethora of abbreviations, a decentralized and ad hoc system of justifications that together constituted "sensitive but unclassified information." T Transportation Security Administration denotes it as "sensitive security information." Turn to the Department of Defense and you will find "Controlled Unclassified Information." The list continues: "For Official Use Only," "Sensitive Homeland Security Information," with dozens of agencies concocting their own rules and hidden drawers. By 2006, openthegovernment.org's "Secrecy Report Card" counted some 50 separate designations for this para-classification. By 2007, that same organization found over 100 such labels. The National Security Archive, looking over 37 agencies, found only 8 with the legal authority to do so. Of the others some had internally generated policies and others no policy at all (Banisar 2007: 18).

One 1994 report, entitled "Joint Commission on Security" and launched by the secretary of defense and the director of central intelligence, found that up to 75 percent of *all the information held by the federal government* might be "sensitive" (Kelley 2006). The implications of this are vast: it means that our tacitly assumed notion that our world of government is mostly open, with a few exceptional arenas of blacked-out secrecy, may well need revision. The terrorist threat, launched with boxcutters and a horrendous attack, had done what 70,000 nuclear warheads had failed to do over the course of 60 years: if the CIA director and the defense secretary could even hypothetically group the large majority of government documents as "sensitive," then the very idea of open government is in question.

On May 9, 2008, President Bush took this sprawling array of nomenclature and relabeled it "Controlled Unclassified Information" (CUI). At that moment CUI became "the single, categorical designation . . . throughout the executive branch." It was to protect information on one side, and allow it to move inside a new kind of fence ("the Information Sharing Environment") on the other. In the black world, three fundamental markings structured the flow of information: top secret, secret, and confidential. Now, paralleling this tripartite division, the gray world too would have its own three-fold marking system:

- "Controlled with Standard Dissemination," which means that the information requires standard safeguarding measures that reduce the risks of unauthorized or inadvertent disclosure. Dissemination is permitted to the extent that it is reasonably believed that it would further the execution of a lawful or official purpose.
- "Controlled with Specified Dissemination" [safeguarding as in the above designation] *and* "Material contains additional instructions on what dissemination is permitted."
- "Controlled Enhanced with Specified Dissemination." This is "safeguarding measures more stringent than those normally required since the inadvertent or unauthorized disclosure would create risk of substantial harm" and the material would contain additional instructions on dissemination (Bush 2008).

It is here, in the gray zone of "Controlled Unclassified Information"—between open and closed—that the government lodged critical infrastructure information, and with it the cornucopia of categories it absorbed and replaced. High on the agenda was blocking Controlled Unclassified Information from the Freedom of Information Act (FOIA). That act had left nine established exemptions—from information about law enforcement, wells and geology and interagency communication to personal and financial data. To immunize infrastructure information against the prying eyes of FOIA, the government invoked two of these escape clauses: exemption 3 (forbids disclosure if forbidden

under another statute) and exemption 4 (forbids disclosure of "trade secrets and commercial or financial information obtained from a person and privileged or confidential") (Radvanovsky and McDougall 2010: 263-265).

Congress has used FOIA exemption 3 (other statutes) to block release of information about cybersecurity and Homeland Security Information. Exemption 4 (sequestering trade and commercial items) blocks information from companies. This is especially important since the November 2002 Homeland Security Act aimed to pull information about critical infrastructure toward the government—and 85 percent of the designated critical infrastructures are in the private sector. As a result, industry pushed hard to prevent information about them from being disclosed under the Freedom of Information Act. Courts have backed the private sector here, securing against FOIA requests information ranging from real and cyber threats to infrastructures, vulnerabilities, and defensive measures, and all the repairs, reconstructions, insurance, or other operational issues that arise in their maintenance (Radvanovsky and McDougall 2010: 265).

When Controlled Unclassified Information is held closely by cabinet-level agencies, forbidden from public disclosure; when this body of documents has been made proof even against the legal structures of the Freedom of Information Act, secrecy has jumped its Cold War corral. Returning to our persistent question about the ontology of secrecy we can ask: What is the referent of Controlled Unclassified Information? Critical infrastructure alone widened hidden knowledge far past the old fences guarding Los Alamos, CIA agents, code-breakers or spy satellites, far beyond even the gates of private companies like DuPont, Union Carbide, or Kellogg that operated nuclear facilities. Here in Controlled Unclassified Information, we have new roads guiding the flow of information from every government agency: blacked-out crops and cows, hidden laws and procedures, withdrawn chemical disaster plans and contingencies about dam failures, unobtainable schematics of high-tension electrical lines, reservoirs, and chemical plants. But it is not just the government: by sweeping private industry into the concep-

tion of critical infrastructure, the para-secret world goes much farther than the Atomic Energy Act authors could have imagined.

At a certain point, the very idea of "behind the fence" fails us, even metaphorically. The fence fails to capture the new scope of secrecy; it fails to capture the virtual as well as physical dimension of secrecy; and it fails to capture the double breakdown of our old categories dividing public from private and war from peace. Our new security fence is everywhere, not delimited by time or space. And with these last steps, the war on terror loses, legally and practically, all ties to the now quaint and finite battlefields of Thermopylae or Ypres that one could still find on a map.

THE WIDENING GYRE OF SECRETS

Secrecy grows in leaps, fed by wars. But while conflicts may have begun in the hot and cold wars sparked in 1914, 1939, 1947, and 2001, secrecy, once ratcheted outward, seems ever harder to reverse. True, the worst excesses of the Sedition Act were repealed after World War I—and the 1954 Atomic Energy Act backed off a bit from the more dramatic 1946 restrictions. But start by protecting a fort or convoy and soon you are securing against discouraging speech. Try to hold on to the uranium bomb and it spirals out into an attempt to control a vast nuclear establishment embracing a world of techno-scientific knowledge, both private and public. Such jumps in the nature of secrecy: World War I secrecy was finite in duration even if disastrously wide in scope. The danger that a Ves Hall or a Robert Goldstein presented disappeared when the war ended—word and image saboteurs (and their products) could be released soon after the Germans surrendered in Marshal Foch's Versailles railway carriage. Atomic secrets, by contrast, had no time limit, and so had to be guarded by institutions that perpetuated themselves endlessly. Soldiers may have demobilized after World War I—but the Los Alamos laboratory has outlasted World War II, the Cold War, and is solidly in place for twenty-first century conflicts. Eternal vigilance was not a matter of physical property: the government monopoly

over nuclear intellectual property was absolute, from secret birth to eternal custodianship.

In their semi-eternal structure, the restricted data of scientific and patent nuclear know-how seemed, in the Cold War, to define the outer reaches of the grasp of secrets. In retrospect that pessimism may have been too optimistic. Even the half-century Cold War had a well-defined terminus: when the Berlin Wall fell, it was clear an era had ended. One cannot even imagine a parallel ending to the Terror Wars. What would the end mean in such a mutable conflict where no one agrees on who the "terrorist enemy" is, what that enemy wants, or what victory would designate? Without boundaries in space, time, or target we have produced a form of secrets appropriate to this day. Critical Unclassified Information fits our age exactly: a form of secrecy with no end date, no limit of scope, and little access through the Freedom of Information Act. In short we have a new ontology of hidden knowledge: multiply infinite secrets for a boundless conflict.

NOTES

1. It is worth noting, however, that the 1911 Defense Secrets Act, along with several federal statutes in 1909, preceded the Espionage Act and had some of the same goals. See "Safegarding Classified Information" (1975: 258-259, 288); and American Protective League (1918).
2. On the *Los Angeles Times* see Slide (1993: xviii). Though never proved, the causal efficacy of dangerous speech was reiterated time after time. "By the living God, the president of the United States publicly declares that he will banish millions of American citizens, and send them to die on foreign fields of blood! In the name of the Almighty, what spirit of evil has taken possession of the Federal government?" This pamphlet, a screed with a reprinted speech by Thomas E. Watson, blasted the government for adopting the very totalitarianism it purported to oppose. That a Mr. Blodgett sent the broadside to registered 21–23-year-old male Americans brought him under the gun of one clause (causing mutiny, insubordination, refusal of service) and another (obstructing recruitment). Blodgett tried

defending himself—on grounds of insanity, which would, were it to have been sustained, have exempted him from the "willful" clause within the act. It was not an implausible claim since the state of Iowa had, on April 13, in fact determined him insane. Blodgett claimed his was nothing more than a sign in the road. Well, Judge Martin Joseph Wade responded, you see a sign in the road that says "Stop! The bridge is out!" at the very least, you stop and go back, maybe you investigate whether the bridge was, in fact, out. But this is precisely what the government does not want: a Stop! sign just before new conscripts arrive at the enlistment office. Was Blodgett seeking to "discourage, persuade, frighten, scare or in any other manner" obstruct military enlistment? Then, so said the court, he should be convicted. He was: 20 years' imprisonment. See Nelles (1918: 51-53).

3. For a history of nuclear weapons patenting see Wellerstein (2008: 57-87).
4. On foreign information exchange and AEC control, see Leon (2005). León sees the 1954 Atomic Energy Act as an attempt to control information: "The initiative adopted the prestige cause of offering the underdeveloped world the gift of nuclear energy as a means of having control in the nuclear programs that incorporated American aid and technology."
5. Eminent domain claims for patents were not new with nuclear fission. For example, in 1912, the Supreme Court of the United States refused to stop the chief of ordnance from making gun carriages using a patent owned by Krupp. The court did order the Unites States to pay the owner of the mechanism for hermetically sealing the breech at the instant of explosion. But the American government had the right to produce the "Bange gas check" by "right of eminent domain." See *New York Times* (1912: 6).
6. There are four elements to a spectrometer typically: 1) a heated filament that generates electrons; 2) an ionization chamber where these electrons ionize the atoms of the sample gas; 3) an analyzer that separates the sample gas beam into sub-beams according to the charge-

to-mass ratio of its ions; and 4) an accumulator or detector that measures the densities of the constituent sub-beams. Washburn's invention improved the accuracy of mass spectroscope by holding gas in the electron-source chamber at a lower pressure than the ionization chamber. This minimized contact by the sample gas with the filament surface. Such contact corrupted the electron-emission process and made the ionization irregular. The new instrument was therefore more accurate, more stable, and more durable than its predecessors.

7. For the award given Fermi and associates, and more generally for a case study of patent 2,206,634 by Fermi et al., see Turchetti (2006: 2). Turchetti also rightly observes that the spread of nuclear power and energy to other countries challenged the effectiveness of the American government monopoly on atomic patents (see Turchetti "Patenting the Atom").
8. On the comparison of punishments in the Espionage and Atomic Energy Acts, see Newman (1946-47: 769-802). On "reason to believe," see p. 793.
9. Cybersecurity has become a vast arena within national security. A few sources sketching the problem are Clarke and Knake (2010); Zittrain (2008, esp. chap. 3); Kramer, Starr, and Wentz (2009).

REFERENCES

American Protective League. *Counter-Espionage Laws of the United States*. Washington, DC: American Protective League, 1918.

"Atomic Bomb Patents." *Bulletin of the Atomic Scientists* (1946): 30-31.

Atomic Energy Act of 1946 and Amendments. Washington, D.C.: U.S. Government Printing Office. 1975.

Banisar, David. "Government Secrecy: Decisions Without Democracy." *Openthegovernment.org* (2007) <www.openthegovernment.org/govt-secrecy.pdf>.

Bush, George W.."Memorandum for the Heads of Executive Departments and Agencies. Subject: Designation and Sharing of Controlled Unclassified Information." May 9, 2008.

Federal Research Division, Library of Congress. *Laws and Regulations Governing the Protection of Sensitive but Unclassified Information*. 2004.

Espionage Act of 1917. 40 Stat. 217, 1917-1919.

Gutfield, Arnon. "The Ves Hall Case, Judge Bourquin, and the Sedition Act of 1918." *Pacific Historical Review* 37 (1968): 163-78.

Cheh, Mary M. "The *Progressive* Case and the Atomic Energy Act: Waking to the Dangers of Government Information Controls." *George Washington Law Review* 48 (1979-1980).

Clarke, Richard A., and Robert K. Knake. *Cyber War. The Next Threat to National Security and What to Do About It.* New York: HarperCollins, 2010.

Hewlett, Richard G. "Born Classified in the AEC: An Historian's View." *Bulletin of the Atomic Scientists* 37 (1981): 20-27.

Kelley, Sara E.."Features—A Select Bibliography on 'Sensitive but Unclassified' and Similarly Designated Information Held by the Federal Govt." *LLRX,* June, 10 2006 <http://www.llrx.com/node/1557/print>.

Kramer, Franklin D., Stuart H. Starr, and Larry I. Wentz. *Cyberpower and National Security.* Washington, D.C.: Potomac Books, 2009.

Leon, Juan Andres. "Nuclear Politics in a Subordinated Country." Third Milano Workshop, "The Physical Sciences in the Third World." Bogota, Colombia, 2005.

National Center for Public Policy Research. "Text of Joint Declaration of War Passed by the Senate and the House of Representatives" <http://www.nationalcenter.org/DeclarationofWWI.html>.

Nelles, Walter. *Espionage Act Cases with Certain Others on Related Points. New Law in Making as to Criminal Utterances in War-Time*. New York: National Civil Liberties Bureau, 1918.

———. "In the Wake of the Espionage Act." *The Nation* 111 (1920): 684-86.

Newman, James R."Control of Information Relating to Atomic Energy." *Yale Law Journal* 56 (1946-47): 769-802.

New York Times, April 9, 1912: 6.

Noah, Timothy "The Unluckiest Man in Movie History." *Slate* (June 13, 2000) <http://www.slate.com/id/1005493>.

Radvanovsky, Robert, and Allan McDougall. *Critical Infrastructure: Homeland Security and Emergency Preparedness*. Boca Raton, London, New York: CRC Press, 2010.

Risenfeld, Stefan A. "Patent Protection and Atomic Energy Legislation." *California Law Review* 46 (1958): 40-68.

"Safegarding Classified Information: The Evolution of Present Federal Law." *Congressional Digest* (November 1975).

Sedition Act of 1918. 40 Stat. 553 1918.

"Senate Hearings on Atomic Energy." *Bulletin of the Atomic Scientists* (1946): 10-11.

Slide, Anthony, ed. *Robert Goldstein and "The Spirit of '76."* Metuchen, N.J.: Scarecrow Press, 1993.

U.S. Dept. of Homeland Security. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.* February 2003.

Turchetti, Simone. "For Slow Neutrons, Slow Pay," *Isis* 97 (2006): 1-27

———. "Patenting the Atom." Unpublished ms.

Van Young, James. *Judges and Science. The Case Law on Atomic Energy*. New York: Arno Press, 1979.

Wellerstein, Alex. "Patenting the Bomb: Nuclear Weapons, Intellectual Property, and Technological Control," *Isis* 99 (2008): 57-87.

White House. Presidential Decision Directive/NSC-63. May 22, 1998.

Woodrow Wilson to Arthur Brisbane, April 25, 1917. Wilson-McAdoo Collection, Bernath Mss. 18, Department of Special Collections, University Libraries, University of California, Santa Barbara.

Zittrain, Jonathan. *The Future of the Internet and How to Stop It*. New Haven and London: Yale University Press, 2008.