Surveillance & Society

Article

Policing the Imperial Periphery: The Philippine-American War and the Origins of U.S. Global Surveillance

Alfred McCoy

Department of History, University of Wisconsin–Madison, U.S.
awmccoy@wisc.edu

Abstract

Using a methodology that inserts the current controversy over NSA surveillance into its historical context, this essay traces the origins of U.S. internal security back to America's emergence as a global power circa 1898. In the succeeding century, Washington's information infrastructure advanced through three technological regimes: first, the manual during the Philippine War (1898–1907); next, the computerized in the Vietnam War (1963–75); and, recently, the robotic in Afghanistan and Iraq (2001–14). While these military missions have skirted defeat if not disaster, the information infrastructure, as if driven by some in-built engineering, has advanced to higher levels of data management and coercive capacity. With costs for conventional military occupations now becoming prohibitive, the U.S. will likely deploy, circa 2020, its evolving robotic regime—with a triple-canopy aerospace shield, advanced cyberwarfare, and digital surveillance—to envelop the earth in an electronic grid capable of blinding entire armies on the battlefield or atomizing a single insurgent in field or *favela*.

Introduction

From the first hours of the American colonial conquest in August 1898, the Philippines served as the site of a social experiment in the use of police as an instrument of state power. During the next decade, the U.S. Army plunged into a crucible of counterinsurgency, forming its first field intelligence unit that combined voracious data gathering with rapid dissemination of tactical intelligence. At this periphery of empire, freed from the constraints of courts, constitution, and civil society, the U.S. imperial regime fused new technologies, the product of America's first information revolution, to create a modern police and fashion what was arguably the world's first full surveillance state.

A decade later, these illiberal lessons percolated homeward through the invisible capillaries of empire to foster a domestic security apparatus during the social crisis surrounding World War I. In the first weeks of war, a small cadre of Philippine veterans established the Military Intelligence Division, creating U.S. counterintelligence as a unique fusion of federal security agencies and citizen adjuncts that persisted for the next half century. America's experimentation with policing at this periphery of its global power was thus seminal in the formation of a U.S. internal security apparatus with extensive domestic surveillance.

Over the past century, this same process has recurred, with striking similarities, as three U.S. pacification campaigns in Asia have dragged on for a decade or more, skirting defeat if not disaster. During each of these attempts to subjugate a dense Asian rural society, the U.S. military was pushed to the breaking point

McCoy, A. 2015. Policing the Imperial Periphery: The Philippine-American War and the Origins of U.S. Global Surveillance. *Surveillance & Society* 13(1): 4-26.
http://www.surveillance-and-society.org | ISSN: 1477-7487

and responded by drawing together all extant information resources, fusing them into an infrastructure of unprecedented power, and producing a new regime for data management—creating innovative systems for domestic surveillance and global control.

Forged in these crucibles of counterinsurgency, the U.S. military's information infrastructure has advanced through three distinct technological regimes: first, the manual during the Philippine War, 1898–1907; next, the computerized in the Vietnam War, 1963–75; and, most recently, the robotic in Afghanistan and Iraq, from 2001 to perhaps 2014. These campaigns have proved seminal in fostering a distinctive U.S. imperial epistemology that privileges extrinsic, quantifiable data over deep cultural knowledge—a defining attribute evident during America's computerized information regime in Vietnam and its robotic regime now taking form in space and cyberspace.

At the level of methodology, such historical analysis adds analytical depth to contemporary events, such as Edward Snowden's revelations about the National Security Agency (NSA). Indeed, the salience, and significance, of contemporary surveillance practices explored in this article can only be fully understood via an approach that contextualizes their historical unfolding within the changing character of U.S. imperial controls. Through the historian's habitual search for origins or watersheds, we can push the formation of the U.S. security apparatus back another half century to the Philippine Insurrection and World War I, mitigating what one historian has called the "debilitating liability" (Walker 2009: xi) of the usual focus on World War II or the Vietnam War as seminal and the consequent omission of any antecedents (Immerman 2014: 9–19, 76–88; Prados 1996: 15–22; Moran and Murphy 2013: 1–14). Such a shift can also broaden our analysis to actors beyond the FBI, showing that the U.S. surveillance state did not simply spring, Athena-like, full grown from the head of J. Edgar Hoover (Weiner 2013: xvi, 3, 9–10, 13, 25, 40–43, 61–62, 84–90, 195–201, 264–87). This broader time frame indicates that, once introduced, potent covert controls such as surveillance prove persistent, resisting reform and reviving in any crisis. Moreover, a comparison of colonial policing and political scandal offers insight into the logic of current NSA surveillance of allied leaders worldwide. With Clio thus whispering in our ear, we can sort through these billions of purloined bytes to discern nothing less than a changing array of global power.

At the level of theory, this history of U.S. intelligence compels a revision of Max Weber's hypothesis about the monopoly of physical force as the distinctive attribute of the modern state (Gerth and Mills 1946: 77–78). The state is not defined solely by a monopoly on raw physical force, but instead by its use of coercion to extract information for heightened social control, simultaneously shaping mass consciousness and penetrating private lives. At the start of the 19th century, as James C. Scott argues, the European state launched bureaucratic reforms that rendered land and society "legible" by extrinsic means such as the metric standard for measurement and patronyms for conscription—a fundamental change but one that still left the state politically blind (Scott 1998: 1–3, 11–72, 373). At the start of the 20th century, however, America moved beyond such passive data collection to become the site of an accelerating information revolution whose synergies represent a second, significant phase in the perfection of modern state power—rendering its subjects not simply legible but permeable.

America's First Information Revolution

During an extraordinary decade, the 1870s to the 1880s, America's first information revolution arose from a synergy of innovations in the management of textual, statistical, and visual data that created the technical capacity for surveillance of the many rather than just a few—a defining attribute of the modern state. Within these few years, the sum of Thomas Edison's quadruplex telegraph (1874), Philo Remington's commercial typewriter (1874), and Alexander Graham Bell's telephone (1876) allowed the transmission and recording of textual data in unprecedented quantities at unequaled speed, and with unsurpassed accuracy (Richards 1964: 23–25; Coe 1993: 89).

These dynamic years also saw parallel progress in the management of statistical and visual data. After Herman Hollerith patented the punch card (1889), the U.S. Census Bureau adopted his Electrical Tabulating machine in 1890 to enumerate 62,622,250 Americans within a few weeks—a stunning success that later led to the founding of International Business Machines, better known by its acronym IBM (Howell 1995: 33–34, 40–42; Austin 1992: 13–21; Wines 1900: 34–36; Kistermann 2005: 56–66; Pugh 1995: 1–36; *American Machinist* 1902: 1073–75; Koon 1914: 533–36; Jones n.d.; Howells 2000). Almost simultaneously, the development of photoengraving (1881) and George Eastman's roll film (1889) extended this information revolution to visual data (Gernsheim and Gernsheim 1969: 403–09).

With a surprising simultaneity, parallel innovations emerged in data storage. In the mid-1870s, Melvil Dewey cataloged the Amherst College Library with his "Dewey decimal system" and Charles A. Cutter worked at Boston's Athenaeum Library to create what became the current Library of Congress system—both, in effect, inventing the "smart number" for reliable encoding and rapid retrieval to manage this rising tide of information (Wiegand 1996: 14–24; Wiegand and Davis 1994: 147–50; Comaromi and Satija 1988: 4–9; LaMontagne 1961: 52–99, 179–233).

Within a decade, U.S. libraries, hospitals, and armed forces applied the "smart number" to create systems that reduced otherwise inchoate masses of data to numerical codes for rapid filing, retrieval, and cross-referencing—allowing a modernization of the Federal bureaucracy. In quick succession, the Office of Naval Intelligence created a card method for recording intelligence (1882), and the U.S. Army's Military Information Division (MID) adopted a similar system three years later. Indicative of the torrid tempo of this information revolution, MID's intelligence cards grew from just 4,000 in 1892 to over 300,000 just a decade later (Bethel 1947: 17–24).

Since American police were then the province of big-city bosses, this information revolution came to crime detection from a mix of foreign and domestic sources. At Paris police headquarters in 1882, Alphonse Bertillon developed the first biometric criminal identification system with eleven cranial and corporeal measurements as well as two facial photographs (front and side view) that was adopted, within a decade, as the American standard (Bertillon 1899/1977: 6, 17, 91–94; Morn 1982: 124–27; Henry 1900: 61; Rhodes 1956: 71–109; Thorwald 1965: 20–26). During the 1890s, moreover, the inspector general of police for India, Sir Edward R. Henry, finalized the modern system of fingerprint classification, bringing this biometric method to Scotland Yard in 1901, from whence it migrated to America three years later at the St. Louis World's Fair. Major U.S. cities soon adopted fingerprinting as their sole standard for criminal identification. Although the Bureau of Investigation (later the FBI) did not follow suit until 1924, its files passed the six million mark within a decade and its director was soon urging compulsory fingerprinting for all citizens. Only months after a young J. Edgar Hoover became head of the Bureau's Radical Division in 1919, he could boast of 80,000 file cards "covering the activities of not only the extreme anarchists but also the more moderate radicals" (Dilworth 1977: 1–3, 6–8, 60–106, 131, 161–66; Henry 1900: 4–7, 61–69; Bertillon 1899/1977: 10–12; *Police Chiefs News Letter* 1934: 2; *Police Chiefs News Letter* 1936: 2; Polenberg 1987: 165).

While an imitator in criminal identification, America was an innovator in the field of police and fire communications, with the Gamewell Corporation adapting telegraphy and telephony to create centralized fire-alarm systems that became the world's standard (Gamewell Fire Alarm Telegraph Co. 1916: chaps. 2–7; Maver Jr. 1903: 440–53; Ditzel 1990: 5, 16–28, 40–42; Werner 1974: 177–84). By 1900, America's cities were wired with a total of 764 municipal fire-alarm systems and 148 police-patrol networks handling a total of 41 million messages in a single year (Little Jr. 1976: 83; Heath 1981: 32, 45, 69–71; Ditzel 1990: 27; U.S. Bureau of the Census 1904: 421–22). On the eve of empire in 1898, however, Congress and courts restrained any national application of these innovations, leaving the Federal government with a limited capacity for law enforcement or domestic security beyond the Customs barrier.

Intelligence Apparatus

After 1898, the conquest of the Philippines made America an imperial power, unleashing the potential of its new information technology. In a sprawling U.S. empire of Western plains and tropical islands, only the Philippines strained America's coercive capacities with a fifteen-year war against an extraordinary array of insurgents—national army, urban underground, militant unions, messianic peasants, and Muslim separatists.

In this protracted pacification after 1898, the U.S. Army formed three new services seminal for a U.S. counterintelligence capacity—its own Division of Military Information, which developed methods later applied to America; the Philippines Constabulary that pacified the new colony's insurgency through pervasive surveillance; and the Manila Metropolitan Police, which became the most advanced force then operating under the American flag.

In retrospect, the sum of such surveillance provided the nascent U.S. imperial regime with key elements of colonial control: first, basic intelligence on leaders and movements to be countered with raw coercion; second, scurrilous information about derelictions of local leaders useful in assuring their compliance with an alien authority; and, finally, the empowerment of an imperial gaze. Through the clandestine accumulation of knowledge—routine, intimate, or scandalous—about native collaborators, the so-called "subordinate elites" critical for colonial rule, American officials gained a sense of omniscience, infusing them with an aura of authority for the exercise of dominion (Robinson 1972: 132–33, 138–39).

Landing in the Philippine Islands without maps, language, or intelligence, the U.S. Army soon became, as one senior intelligence officer put it, "a blind giant" that was "more than able to annihilate, to completely smash" anything it faced, but found it "impossible to get any information" about where or when to unleash this lethal force. Complicating the army's intelligence efforts, Filipino officers, despite limited combat experience, were skilled at espionage, developing codes to conceal identities (Linn 2000: 127, 191; Linn 1991: 90–96).[1] As it struggled to uproot guerrillas immersed in rugged terrain and hostile populations, the U.S. Army discovered the imperative of accurate intelligence and established the Division of Military Information, or DMI—the first field intelligence unit in its hundred-year history.

In early 1901, Captain Ralph Van Deman, later known as the "father of U.S. Military Intelligence," assumed command of the DMI and began developing procedures that would influence later intelligence operations for the entire U.S. Army (Jensen 1991: 112; Powe 1975: 18–21; Campbell 1987: 13; Bigelow 1990: 38). Instead of passively filing documents like staff at the Military Information Division in Washington, Van Deman's Manila command combined reports from the Army's 450 post information officers with data from the colony's civil police. With telegraph lines knitting nets around guerrilla zones and the captain pressing subordinates for fast, accurate information, the DMI's field units proved agile in tracking rebel movements and identifying their locations for timely raids (Weber 1988: 7–8; Linn 1991: 100–08; Linn 1989: 155–56).

With a voracious appetite for raw data, DMI launched, in March 1901, a "confidential" project to map the entire guerilla infrastructure by compiling information cards for every influential Filipino—documenting physical appearance, personal finances, political loyalties, and kinship networks. For rapid retrieval, the DMI's clerks transcribed these cards into indexed, alphabetical rosters for each military zone (Barry 1901). With few military precedents to guide him, Van Deman thus developed comprehensive doctrines

[1] See also the testimony of Colonel Arthur L. Wagner, former head of the Military Intelligence Division, in U.S. Senate, 57th Congress, 1st Session, doc. no. 331, part 3, *Affairs in the Philippine Islands: Hearings before the Committee on the Philippines of the United States Senate* (Washington, DC: Government Printing Office, 1902), 2850–51.

for intelligence and counterintelligence (Weber 1988: 8–18; Gates 1973: 250–51; Linn 1991: 104–05; Van Deman 1901).

Philippine Police and Constabulary

During its three-year pacification of Manila, 1898–1901, the U.S. Army also created a metropolitan police force that applied military intelligence and data management for an efficient counterintelligence. When U.S. civil rule started in 1901, Manila's colonial police added the most advanced of America's crime control technologies—a centralized phone network, the Gamewell system of police-fire alarms, incandescent electrical lighting for city streets, Bertillon's photo identification, and fingerprinting. Within 20 years, Manila's police files would amass 200,000 alphabetized file cards covering 70 per cent of the city's population (*Khaki and Red* 1927: 5–8, 9; *Khaki and Red* 1932: 12; *Philippines Free Press* 1918: 3).

After his inauguration in July 1901, the first U.S. civil governor, William Howard Taft, elaborated military methods into a modern surveillance state, creating a distinctive colonial regime that ruled through a total control over information. Only weeks after taking office, Taft established the Philippines Constabulary as a long-arm mobile police—with 325 officers, many of them Americans, and 4,700 constables, all of them Filipino—and assigned it the dual mission of counterinsurgency and colonial intelligence.

The Constabulary's founder was Captain Henry T. Allen, a West Point graduate who understood the import of intelligence and secret police from an earlier assignment as military attaché at the czar's court in St. Petersburg (Twitchell Jr. 1974: 4–86, 290). With its network of 200 Filipino spies, the Constabulary's Information Division drew data through intensive surveillance, covert penetration, and monitoring of press and public discourse. All this intelligence flowed into the division's headquarters where it was translated, typed, numbered, and filed in dossiers for retrieval. These numbered files also allowed juxtaposition of related intelligence for psychological profiling, order-of-battle rosters, and longitudinal studies of entire movements—creating a colonial frame for analysis and action (McCoy 2009: 104–06, 129).

Politics of Scandal

Within this police panopticon, the Constabulary was systematic in its collection of incriminating information and selective in its release—suppressing scandal to protect allies and releasing scurrilous information to destroy enemies. By late 1904, Archbishop Gregorio Aglipay was about to legitimate his nationalist schism, the Iglesia Filipina Independiente, which controlled 30 per cent of the country's Catholic parishes, with a final, critical step: the grant of apostolic succession from the U.S. Episcopal Church. The U.S. colonial regime saw this schism as a serious threat to its alliance with the Catholic Church and regarded Archbishop Aglipay himself as an unrepentant revolutionary (Clifford 1969: 234–45; Grove 1903; Achutegui and Bernad 1961: 206–08).

Thus, as Episcopalian bishops gathered at Boston in 1904 to consider an affiliation with this Philippine schismatic church, Chief Allen blocked any alliance by sending the American bishops an intelligence profile of Aglipay—stating spuriously he had, during the Revolution against Spain, ordered a Spanish bishop flogged with 300 lashes and later prowled the halls of a Catholic convent with lecherous intent (Brent 1904a; Allen 1904; Brent 1904b; Brent 1904c; Clymer 1986: 122). In a closed session, the Episcopal bishops rejected recognition of the Aglipayan Church, delaying the natural union of these two churches for another 60 years, long after Philippine independence (Brent n.d.; Achutegui and Bernad 1961: 388–90; Clymer 1986: 120–22). Along with other colonial pressures, this setback contributed to a rapid decline in the strength and status of the Aglipayan nationalist schism.

Other documents offer instances of Constabulary suppression of sensitive information about a close Filipino collaborator. Among the thousands of reports that crossed his desk, General Allen carried just one document with him through wartime service in France and into retirement near Washington, D.C.—a DMI report titled "The Family History of M.Q." Among its scandalous tales, this report alleged that an influential Filipino politician, identified only as MQ, had concealed a premarital liaison with his half-sister and future wife by arranging an abortion. And he had also buried the fruit of a similar liaison with another half-sister in Manila's Paco Cemetery.[2]

During the first decade of his political career, MQ, or Manuel Quezon, served the Constabulary as a secret agent and was, in turn, protected from the taint of such scandal. In 1903, the future PC chief Rafael Crame, then a lieutenant in its Information Division, retained the young Attorney Quezon as a "private spy … used in all sorts of cases in the early days of the Constabulary" (Wood 1923). Since Quezon cooperated fully, the "The Family History of M.Q." remained safely buried in General Allen's private files until his death, thereby assuring Quezon's unchecked rise to become the first Philippine president in 1935 and, after independence in 1946, the namesake for his nation's new capital.

Colonial Blueprint

At the close of the U.S. pacification of the Philippines, Mark Twain wrote an imagined history of 20th century America arguing that its "lust for conquest" had destroyed "the Great [American] Republic" because "trampling upon the helpless abroad had taught her, by a natural process, to endure with apathy the like at home; multitudes who had applauded the crushing of other people's liberties, lived to suffer for their mistake" (Twain 1992: 78–79). Indeed, just a decade after Twain wrote those prophetic words, these colonial police methods were repatriated to provide blueprints for the foundation of a U.S. internal security apparatus.

For the U.S., Philippine conquest provided the first manifestation of the repressive potential of its new information technology. On the eve of empire in 1898, the country was what Stephen Skowronek has called a "patchwork" state with a loosely structured administrative apparatus, leaving ample room for innovation that came, with stunning speed, in these years of empire. Whatever one might think of Skowronek's overall assessment, his weak state thesis seems useful in assessing a key area he overlooks—Federal capacity for law enforcement and state security (Skowronek 1982: 8–18, 39–46).

When America entered World War I in April 1917, it had the only army on the battlefield without an intelligence service of any description. With surprising speed, these colonial police methods migrated homeward through the invisible capillaries of empire to provide templates for two new U.S. Army commands that fostered a domestic security apparatus—Military Intelligence and Military Police.

Within weeks, Colonel Ralph Van Deman drew upon his Philippine experience to establish U.S. Military Intelligence, quickly recruiting a staff that grew from one employee (himself) to 1,700 and devising the entire institutional architecture for America's first internal security agency. Just as the Philippine Constabulary had used civilian operatives, so Van Deman designed U.S. internal security as a unique fusion of federal agencies and civil auxiliaries that would mark its operations for the next half-century. In collaboration with the FBI, Van Deman presided over a counterintelligence auxiliary, the American Protective League, with 350,000 civilian operatives who amassed over a million pages of surveillance

[2] "The Family History of M.Q." [ca. 1900], Box 7, File: 1900 Oct, Henry T. Allen Papers, Manuscript Division, U.S. Library of Congress. Although the document only gives the author's name as "Captain Pyle, P.S.," U.S. Army records show that a Frank L. Pyle joined the Philippine Scouts as a second lieutenant on June 27, 1902, while retaining the permanent rank of sergeant in Troop D, U.S. First Cavalry. See also, Military Secretary's Office, *Official Army Register for 1905* (Washington, DC: Government Printing Office, 1904), 359; and Hartford Beaumont, letter to the Honorable Henry C. Ide, December 7, 1904, Book 21:II, Dean C. Worcester Papers, Harlan Hatcher Library, University of Michigan.

reports on German Americans in just fourteen months (Kornweibel Jr. 1998: 7, 184; Dorwart 1983: 7; McCormick 1997: 3, 12–13; Jeffreys-Jones 2007: 65–72).

Military Police

Similarly, in the war's final months General Harry Bandholtz, drawing on what he called his "long experience in command of the Philippine Constabulary" (1907–13), established the U.S. Military Police or MPs, charged with managing the chaos of postwar occupation and demobilization. Following their formation in October 1918, Bandholtz quickly built the MPs into a corps of 31,627 men stationed in 476 cities and towns of five nations—France, Italy, Belgium, Luxembourg, and the German Rhineland. By training over 4,000 officers and men at service schools in France, Bandholtz ended early complaints of disrespect or even "brutality" and established a record of "kindness … to the native inhabitants" (*Washington Evening Star* 1940; Bandholtz 1919/1991: 313–28; Wright, Jr. 1992: 8–9).

After the war as well, Bandholtz applied lessons learned from repressing Filipino radical movements to lead the Army in crushing the only armed uprising that the U.S. faced in the 20th century. In 1921, as 10,000 striking mineworkers armed with rifles shot it out with sheriffs and private security across Mingo and Logan counties in West Virginia, Bandholtz quelled the violence without firing a shot. Using the psychological tactics learned from his years in the colonial Constabulary to dominate the union leaders, he deployed 2,100 federal troops to demobilize 5,400 miners, confiscate 278 firearms, and send everyone home. Sixteen men died in the five-day Battle of Blair Mountain, but none was shot by U.S. Army troops (Institute for the History of Technology and Industrial Anthropology 1992: 35–50; Laurie and Cole 1997: 320–24).[3]

Postwar Surveillance

With war's end in 1918, Military Intelligence revived the Protective League and organized the American Legion for two years of repression against the socialist left—marked by mob action across the Midwest, the notorious Lusk raids in New York City, J. Edgar Hoover's "Palmer raids" across the northeast, and suppression of strikes from New York to Seattle. But once Congress and the press exposed these excesses, Republican conservatives quickly curtailed Washington's internal security apparatus. In May 1924, Attorney General Harlan Fiske Stone, worried that "a secret police may become a menace to free government," announced, "the Bureau of Investigation is not concerned with political or other opinions of individuals." Five years later, Secretary Henry Stimson abolished the State Department's cryptography unit with the admonition, "Gentlemen do not read each other's mail" (Jensen 1968: 287–89; Hyman 1959: 323–24; McCormick 1997: 202; Kornweibel Jr. 1998: 174–75; Kahn 2004: 94–103; Talbert Jr. 1991: 208–11; Van Deman 1928; U.S. Senate 1976b: 105–06; Schmidt 2000: 324–28, 368).

If General Van Deman's wartime service won him the title "father of U.S. Military Intelligence," then his subsequent surveillance should earn him another honorific, "father of the American blacklist." After retiring from the army in 1929, Van Deman and his wife worked tirelessly for the next quarter-century from their bungalow in San Diego, coordinating an elaborate information exchange among military intelligence, police red squads, business security, and citizen vigilante groups to amass detailed files on 250,000 suspected subversives. Indicative of his influence over internal security, Van Deman attended the confidential National Intelligence Conference in 1940 between J. Edgar Hoover and the chief of Army

[3] See also, Major General J. G. Harbord, To: Brigadier General H. H. Bandholtz, August 31, 1921; Brig. Gen. H. H. Bandholtz, Proclamation, September 2, 1921; A Proclamation by the President of the United States, n.d.; Bandholtz, Copy Telegram No. 2, To: Adjutant General, n.d.; Minutes, Twenty-Ninth Consecutive and Fourth Biennial Convention of District No. 5, United Mine Workers of America, First Day, Pittsburg, Pa., September 6, 1921; Brigadier General H. H. Bandholtz, To: the Adjutant General, September 12, 1921, Reel 9, Harry H. Bandholtz Papers, Michigan Historical Society.

intelligence who, like the Pope at Tordesillas, divided the world through the "Delimitations Agreement"—assigning counterintelligence for the Americas to the FBI and intelligence gathering for the rest of the world to the Army's Military Intelligence and its descendant, the Office of Strategic Services (OSS) (Talbert Jr. 1991: 255–59; U.S. Senate 1976a: 33–38).

Communist Witch Hunt

In the aftermath of World War II, the nation's public–private security alliance revived to create the anti-communist movement identified with Senator Joseph McCarthy. In this witch-hunt, Van Deman worked closely with the FBI and the California Committee on Un-American Activities in a public exposé of the Communist Party, particularly in Hollywood. In June 1949, that California committee, headed by Senator Jack Tenney, drew upon Van Deman's archive to issue a sensational 709-page report denouncing hundreds of Hollywood luminaries as "red appeasers"—including Charlie Chaplin, Katherine Hepburn, Gregory Peck, Orson Welles, Frank Sinatra, and, particularly, Helen Gahagan Douglas (*New York Times* 1949a, 1949b, 1971; California Legislature 1949: 411, 448–49, 488–537; McGilligan and Buhle 1997: 368–69).[4]

Within this wider public–private alliance, Van Deman's archive served as an informal conduit for moving security reports from closed, classified government files into the hands of citizen anti-communist groups for public black listing. In the 1946 congressional elections, for example, an obscure Los Angeles lawyer named Richard Nixon reportedly used Van Deman's files for red baiting to defeat five-term Democratic congressman, Jerry Voorhis. Four years later, Representative Nixon reportedly used the same files and tactics to beat Representative Helen Gahagan Douglas in the race for the U.S. Senate, launching him on a path to the presidency (Halloran 1971: 35).

This archive did not die with its creator. Only hours after Van Deman passed away in 1952, a team from the U.S. Army Counter Intelligence Corps secured his voluminous files. For the next 20 years, his records were used by the army, and then, in 1971, delivered to the U.S. Senate Internal Security Committee where they assisted in the investigation of suspected communists until the late 1970s (Talbert Jr. 1991: 270–71; Halloran 1971).[5]

More broadly, Van Deman's methods were perpetuated inside the FBI, particularly after 1940 when Hoover's bureau gained control of U.S. counterintelligence and used wartime conditions for illegal break-ins, wiretaps, and mail intercepts. To curtail enemy espionage, President Franklin D. Roosevelt authorized Hoover, in May 1940, to engage in limited wiretapping that the bureau expanded into widespread surveillance. During the war, the bureau planted 6,769 wiretaps and 1,806 bugs that provided the president with phone transcripts from his domestic enemies—notably, aviator Charles Lindberg, Senator Burton K. Wheeler, and Representative Hamilton Fish. Upon taking office in early 1945, President Harry Truman soon discovered the extraordinary extent of FBI surveillance. "We want no Gestapo or Secret Police," Truman told his diary that May. "FBI is tending in that direction. They are dabbling in sex-life scandals and plain blackmail" (Weiner 2013: 77, 86–90, 134–35). Yet after only a few months in office, Truman

---

[4] The famous Appendix 9 of HUAC's 1944 report, which includes a similarly massive list of communists, was unknown to the public and restricted to a narrow circle of government investigators as late as 1951. See Edward L. Barrett Jr., *The Tenney Committee: Legislative Investigation of Subversive Activities in California* (Ithaca, NY: Cornell University Press, 1951), 20–22.

[5] See also, R. R. Roach, letter to D. M. Ladd, July 13, 1945; D.M. Ladd, letter to E.A. Tamm, October 29, 1945; Colonel F.W. Hein to Commanding Officer 115th CIC Detachment, March 8, 1951; A.H. Belmont, letter to D.M. Ladd, November 9, 1951; Colonel H.S. Isaacson, letter to Major General A.R. Bolling, November 27, 1951; Director to SAC San Diego, December 11, 1951; V.P. Keay, letter to A.H. Belmont, January 22, 1952; Santoiana to Director, January 22, 1952; SAC San Diego to Director, February 4, 1952; SAC SF to Director, n.d.; Subject: Van Deman, Ralph Henry, Files 65-37516, 94-37515, Federal Bureau of Investigation, Washington, DC.

ordered FBI phone taps on Thomas G. Corchran, President Roosevelt's trusted aide whom Truman now regarded as "poison" (Burnham 1986).

OSS in World War II

The manual information regime reached its apotheosis during World War II when Washington established the Office of Strategic Services (OSS) as America's first global espionage agency. Among this agency's nine branches, Research & Analysis recruited 1,950 academics who amassed 300,000 photographs, one million maps, and three million file cards—which it deployed to produce over 3,000 staff studies and answer countless tactical questions (Winks 1987: 60, 74–75, 104, 111, 113–14).

By early 1944, however, OSS found itself, in the words of historian Robin Winks, "drowning under the flow of information" with documents stacking up, unread and unanalyzed. Without technological change to allow more efficient data management, this manual regime might have eventually collapsed under its own weight, imposing limits on America's voracious imperial epistemology (Winks 1987: 104–05).

Vietnam War

Under the pressures of a protracted counterguerrilla campaign in South Vietnam from 1964 to 1974, the U.S. launched a computerized information infrastructure that was nothing less than a second American information regime.

After Defense Secretary McNamara told the CIA in 1966 to "design me something that will tell us the status of control in the countryside," the agency identified eighteen variables that allowed U.S. military advisers to assess security in South Vietnam's 12,000 hamlets on a scale from A (secure) to E (Viet Cong control). Every month, the U.S. command's IBM computers arrayed the results of this Hamlet Evaluation Survey (HES) on an illusory dot-matrix computer map. Unable to measure the critical variable of "popular commitment, because we couldn't," the HES faced an impossible dilemma. "We were trying desperately to find countrywide indicators," explained U.S. pacification chief Robert Komer, "and naturally the only indicators we could use were those that were statistically comparable and measureable" (Komer 1970: 198–204, 207–08, 243). Thus, the share of South Vietnam's population rated "secure" climbed relentlessly to 75 per cent on the eve of the disastrous 1968 Tet Offensive (Gibson 1986: 305–15; Lester 1990: 2–5). Six years later as the Saigon regime plunged toward defeat, this HES survey found South Vietnam 84 per cent pacified. In the end, these automated indices led South Vietnam's government, said CIA director William Colby, "to delude itself about its standing with its own people" (Hunt 1990: 185–86, 194–95, 197–99, 260–61; Lester 1990: 2).

More successfully, the U.S. Air Force retrofitted the dumb Ryan "Firebee" target drone for 3,500 unmanned surveillance sorties over China and North Vietnam. By 1972, the "SC/TV" model drone with a camera in the nose could fly 2,400 miles while the "airborne remote control officer … could now navigate using a low-resolution television image" (Ehrhard 2000: 413, 417–18; Goebel 2006; U.S. Air Force 2005: 1–2). Even though all this computerized data contributed to America's soul-searing defeat in Vietnam, in retrospect they served as a significant experimental step toward the formation of a third, robotic information regime.

During the Vietnam era as well, the FBI's COINTELPRO and the CIA's Operation Chaos conducted illegal acts of domestic surveillance against the anti-war left. After a quarter-century of warrantless wiretaps, the bureau had already built its "Sex Deviate Files" and "Official/Confidential" files into veritable archives on the sexual peccadilloes of America' powerful. Hoover used such scandal to shape the direction of U.S. politics—distributing a dossier on Adlai Stevenson's homosexuality to assure his defeat in the 1952 presidential election, circulating audiotapes of Martin Luther King Jr.'s philandering, and

telling President Kennedy he knew of his affair with mafia mistress Judith Exner (Weiner 2013: 178, 249–50; O'Brien 1999; Kelly 1988).

"The moment [Hoover] would get something on a senator," recalled William Sullivan, then the bureau's third-ranking official, "he'd send one of the errand boys up and advise the senator that 'we're in the course of an investigation, and we by chance happened to come up with this data on your daughter …' From that time on, the senator's right in his pocket" (Kessler 2011: 37–41). By the time of Hoover's death in 1972, locked file cabinets inside his personal office held 722 files on congressmen and 883 on senators, documenting their indiscretions (Summers 2011).

At the end of the Vietnam War, the Church and Rockefeller committees investigated the excesses of this domestic surveillance, prompting formation, under the Foreign Intelligence Surveillance Act of 1978, of so-called FISA courts authorized to issue warrants for national security wiretaps. In effect, the combination of media exposé and legislative reform corrected these Cold War excesses, much as Republican conservatives had done in the aftermath of World War I (Hersh 1974: 1; Horrock 1975a: 1; Horrock 1975b: 1; Horrock 1976: 1; Wicker 1976: 21; Charlton 1977: 1; Burnham 1978: 19; Binder 1978; Horrock 1979: 17).

War on Terror

As its pacification of Afghanistan and Iraq sank into the miasma of these dense social formations after 9/11, Washington adopted electronic surveillance, biometric identification, and unmanned aerial vehicles—whose sum is now forming a third U.S. information regime. This amorphous war's voracious appetite for information soon produced a veritable "fourth branch" of the federal government with 854,000 vetted security officials and over 3,000 private and public intelligence organizations pumping out, in 2010, a total of 50,000 intelligence reports annually, many redundant and unread (Priest and Arkin 2010).

After vocal public opposition to its overt attempts at systemic domestic surveillance under Operation TIPS and Pentagon's Total Information Awareness, the Bush administration retreated into the shadows to launch secret domestic surveillance by the FBI and NSA (Shenon 2002: A-12; Lichtblau 2003: A-1; Lichtblau 2004: A-17; Lichtblau 2005: A-12; Hentoff 2002a; Eggen 2002: A-1; Crossen 2002; Hentoff 2002b). In 2002, Congress erased the bright line that had long barred the CIA from domestic spying, granting the agency power to access U.S. financial records and audit electronic communications routed through the country (Weiner 2002: C-1, Weiner 2007: 482–83).

Not satisfied, President Bush, starting in October 2001, ordered the NSA to commence covert monitoring of private communications through the nation's telephone companies without warrants (Risen and Lichtblau 2013). Since the Bush administration decided "metadata was not constitutionally protected," the NSA launched a sweeping attempt under Operation Stellar Wind "to collect bulk telephone and Internet metadata" (National Security Agency 2009: 7–13).

Armed with expansive FISA court orders allowing collection of data sets rather than specific targets, the FBI's "Investigative Data Warehouse" acquired over a billion documents within five years—including intelligence reports, social security files, drivers' licenses, and private financial information—accessible to 13,000 analysts making a million queries monthly (Mueller 2006; Nakashima 2006,: A-6; Gellman and Poitras 2013). As the sheer masses of data strained computer capacities, the Bush administration launched the Intelligence Advanced Research Projects Activity in 2006, using IBM's Watson supercomputer to sift the rising haystack of internet data (Risen and Lichtblau 2013).

In 2005, the *New York Times* exposed this illegal surveillance for the first time (Risen and Lichtblau 2005). A year later, *USA Today* reported the NSA was "secretly collecting the phone call records of tens of millions of Americans, using data provided by AT&T, Verizon and Bell South." One expert called it "the largest database ever assembled in the world," adding presciently that the agency's goal is "to create a database of every call ever made" (Cauley 2006). Armed with expanded powers by Congressional legislation in 2007 and 2008 that legalized Bush's once illegal program, the NSA launched its PRISM program by compelling nine internet service providers to transfer what became billions of emails to its massive data farms (Gellman and Poitras 2013). And the FISA courts, created to check the security state, instead became its close collaborator, approving nearly 100 per cent of government wiretap requests and renewing mass metadata collection of all U.S. phone calls 36 consecutive times from 2007 to 2014 (Litchblau 2013; Gross 2014).

Surveillance Under Obama

Instead of curtailing his predecessor's wartime surveillance, President Obama expanded the NSA's digital panopticon into a permanent weapon for the exercise of U.S. global power. Under Obama, the NSA's foreign and domestic internet penetration became so pervasive that the U.S. surveillance state moved beyond legibility to permeability—not merely monitoring movement, but seeing inside Americans' lives.

By the end of Obama's first term in 2012, the NSA's global surveillance was remarkable for its ability to sweep up billions of messages worldwide and monitor specific international leaders. To achieve this extraordinary capability, the NSA under Obama completed the agency's architecture for a global surveillance regime—including, access points for penetration of the worldwide web of fiber optic cables; ancillary intercepts through special protocols and "backdoor" software flaws; supercomputers to crack the encryption of this digital torrent; and massive data farms to store the endless "yottabytes" (each equivalent to a trillion terabytes) of purloined data.

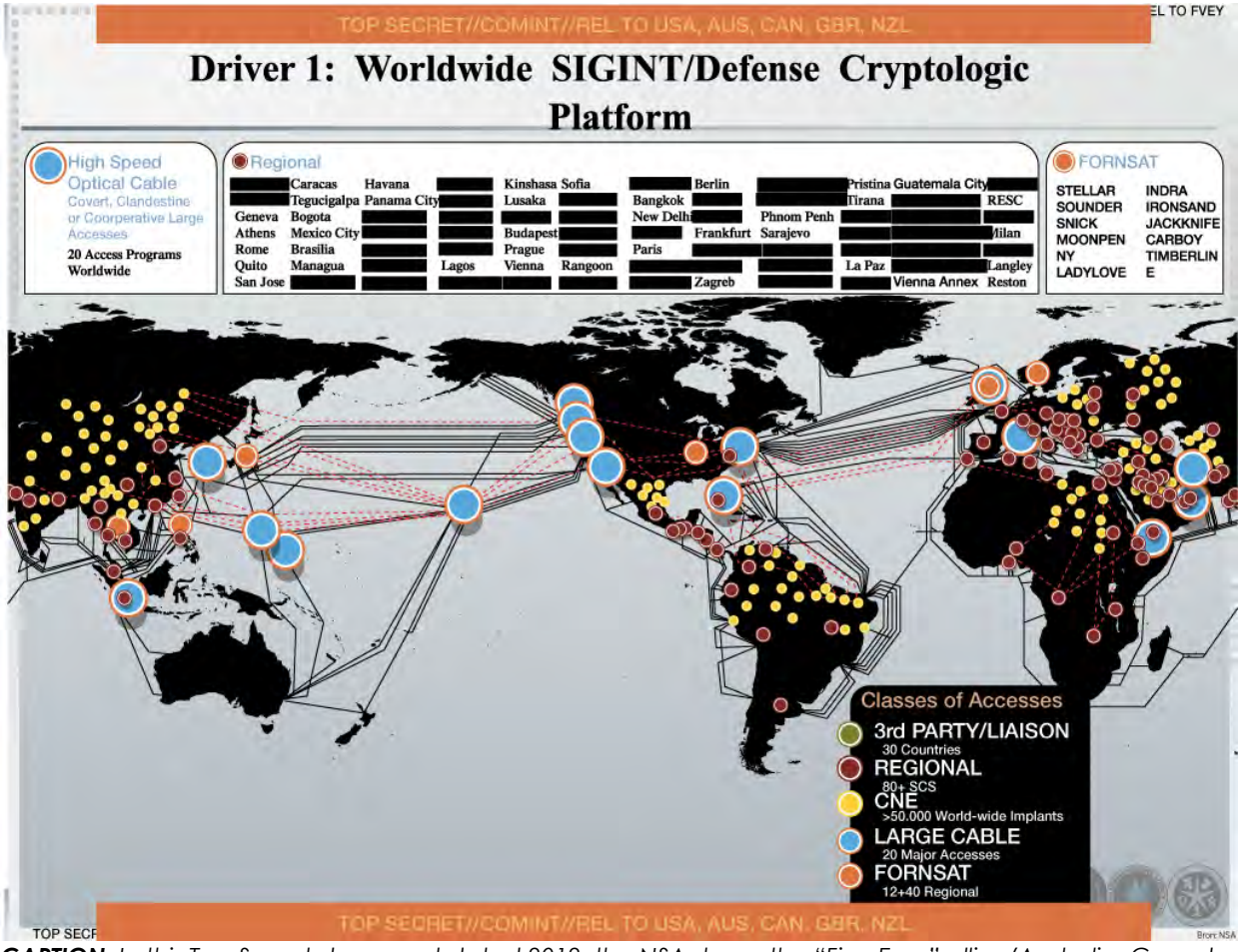
In August 2013, the *New York Times* reported that the FISA court had chastised the NSA two years earlier for intercepting some 250 million email messages from Americans annually while supposedly tracking foreign suspects and maintaining a log of all domestic phone calls since 2006 (Savage and Shane 2013). A month later, the paper revealed that the NSA had, since 2010, applied sophisticated software to create "social network diagrams … to unlock as many secrets about individuals as possible … and pick up sensitive information like regular calls to a psychiatrist's office [and] late-night messages to an extramarital partner" (Risen and Poitras 2013a).

The NSA's so-called "bulk email records collection" under the sweeping Patriot Act continued until 2011 when two U.S. senators protested that the agency's "statements to both Congress and the Court … significantly exaggerated this program's effectiveness"—eventually forcing Obama to curtail this operation (Wyden 2013). Nonetheless, the NSA continued to collect U.S. personal communications by the billions under its PRISM program, authorized by a FISA court order requiring Verizon to transfer all phone calls, foreign and domestic, on an "ongoing daily basis" (Greenwald 2013a). Beyond that "front-door access" provided by PRISM, the NSA's surreptitious MUSCULAR project, according to a January 2013 agency document, penetrated data transfers between internet giants Google and Yahoo to capture 181 million new records in just 30 days (Gellman and Soltani 2013).

The ongoing War on Terror provided both the political impetus and technical innovation for this rapid growth in U.S. surveillance. By the time the U.S. withdrew from Iraq in late 2011, the U.S. Army's Biometrics Identity Management Agency (BIMA) had collected fingerprints and iris scans for three million people, or 10 per cent of that country's population. In Afghanistan by early 2012, U.S. military computers held biometrics for two million Afghans, again about 10 per cent of this country's population (Mansfield-Devine 2012: 5–6). Two years after the Pentagon's Homeland Security commander, General

Victor Renuart, called for the domestic application of this technology in 2009, a company called BI2 Technologies in Plymouth, Massachusetts, began marketing the Mobile Offender Recognition and Information System (MORIS), with smart phone-based iris recognition, to dozens of police forces across America (Howard 2011; Hodge 2009). Similarly, the military's experimental Biometric Optical Surveillance System (BOSS), designed to spot suicide bombers in crowds of Afghans or Iraqis, was transferred to Homeland Security in 2010, which continued to develop facial recognition through surveillance cameras for future use by local police (Savage 2013).

Beyond U.S. borders, the World Wide Web's centralization of most communications into a global network of fiber optic cables, routed through relatively few data hubs that are all accessible to the NSA, has allowed the U.S. a capacity for global surveillance far beyond the British Empire's yield from its trans-oceanic telegraph cables. The NSA's 2012 schematic for its "Worldwide SIGINT/Defense Cryptologic Platform" indicates that the agency inserted malware on 50,000 computers worldwide through just 20 "covert, clandestine, or cooperative" cable access points, supplemented by 170 secondary and tertiary entries—an extraordinary economy of force for worldwide surveillance and cyberwarfare (National Security Agency 2012).



***CAPTION**: In this Top Secret document dated 2012, the NSA shows the "Five Eyes" allies (Australia, Canada, New Zealand, United Kingdom) its 190 "access programs" for penetrating the Internet's global grid of fiber optic cables for both surveillance and cyberwarfare. (Source: NRC Handelsblad, November 23, 2013).*

Leaked NSA documents published in *The Guardian* indicate that the agency's X-KeyScore program collected "staggering large" quantities of internet communications, including 850 billion "call events" in

2007 and 41 billion records for a single month in 2012, about "nearly everything a user does on the internet" from chat rooms to online searches (Greenwald 2013b). Through expenditures of $250 million annually under its Sigint Enabling Project, the NSA systematically and stealthily penetrated all encryption designed to protect privacy. "In the future, superpowers will be made or broken based on the strength of their cryptanalytic programs," reads a 2007 NSA document. "It is the price of admission for the U.S. to maintain unrestricted access to and use of cyberspace" (Perlroth, Larson and Shane 2013).

Under Obama as well, the NSA cooperated with its long-time British counterpart, the Government Communications Headquarters (GCHQ), to tap the dense cluster of Trans-Atlantic Telecommunication (TAT) fiber optic cables that pass through the United Kingdom. Two years after turning its gaze from the skies above to probe the cables below at its Cornwall station, GCHQ's Operation Tempora achieved the "biggest internet access" of any partner in the "Five Eyes" signals intercept coalition that includes the UK, U.S., Australia, Canada, and New Zealand. When the operation went online in 2011, GCHQ sank probes into 200 internet cables and was soon collecting 600 million telephone messages daily, accessible to 850,000 NSA employees (MacAskill *et al*. 2013).

This close cooperation between the NSA and GCHQ dates back to the dawn of the Cold War in March 1946 when the two powers signed the top secret British–U.S. Communication Intelligence Agreement (BRUSA), then focused on high-altitude interception of Soviet bloc radio waves. During the next decade, this British–U.S. intercept program expanded into a worldwide listening apparatus by adding close partners in the Five Eyes coalition and allies—such as Norway, Germany, Italy, and Turkey—as adjuncts in the Echelon network (Norton-Taylor 2010; National Security Agency 1946).

Apart from tracking terrorists, the NSA has conducted extensive surveillance of Allied nations to more efficiently control the nexus of so-called "subordinate elites" that has been the fulcrum for the U.S. exercise of global power since the mid-1950s. Just as colonial police such as the Philippines Constabulary once surveilled thousands of local influentials who collaborated with European colonial rule, so the CIA and NSA have monitored the several hundred national leaders who now play an analogous role in America's global imperium.

What is the aim of such sensitive surveillance, which runs the risk of serious political repercussion if exposed? Here, situating U.S. colonial policing in historical perspective provides a precedent that explains the strategic significance underlying the NSA's aggressive global surveillance.

In a parallel with U.S. colonial policing in the Philippines, such worldwide surveillance provides Washington with the information needed for global hegemony—first, operational intelligence on dissidents to be countered with covert action or military intervention; second, basic political and economic intelligence to advantage American diplomats in bi- or multi-lateral negotiations; third, scurrilous information about derelictions of national leaders useful in encouraging their compliance; and, finally, the empowerment of a neo-imperial gaze. Through the clandestine accumulation of knowledge about national leaders worldwide, Washington's empowered rulers gain not only actual information, whether strategic or scandalous, but a deeper sense of omniscience for the exercise of dominion over inherently independent national leaders.

In deference to the historic Five Eyes alliance, the NSA has, since 2007, generally exempted close "2nd party" allies from surveillance programs such as its "Boundless Informant" operation. But, says a leaked NSA document, "we can, and often do, target the signals of most 3rd party foreign partners"—meaning those 30 Echelon allies such as Germany, France, and Italy. On a busy day in January 2013, the NSA collected 60 million phone calls and emails from Germany—with similar numbers for France, Italy, and Spain. To gain operational intelligence on these U.S. allies, the NSA tapped phones at European Council headquarters in Brussels and 38 "targets" in Washington and New York—including the European Union

(EU) delegation at the UN, and a "Dropmire" monitor "on the Cryptofax at the EU embassy DC" (Castle and Schmitt 2013; MacAskill and Borger 2013; Poitras *et al*. 2013).

By late 2013, in the words of the *New York Times*, there were "more than 1,000 targets of American and British surveillance in recent years," reaching down to even mid-level actors in the international arena. Apart from obvious subjects such as Israeli Prime Minister Ehud Olmert and Defense Minister Ehud Barak, the NSA and GCHQ monitored the vice-president of the European Commission, Joaquin Almunia, who oversaw anti-trust issues; the French energy company Total; and German government communications with Georgia, Rwanda, and Turkey (Ball and Hopkins 2013; Glanz and Lehren 2013).

Such secret intelligence about its allies gives the U.S. a significant diplomatic advantage. According to NSA expert James Bamford, "it's the equivalent of going to a poker game and wanting to know what everyone's hand is before you place your bet" (Erlanger 2013). Indeed, during the diplomatic wrangling at the UN over the Iraq invasion in 2002–03, the NSA intercepted Secretary-General Kofi Anan's conversations and monitored the "Middle Six" of Third World nations on the Security Council—"listening in as the delegates communicated back to their home countries … to discover which way they might vote," and offering "a highway, a dam, or a favorable trade deal … in a subtle form of bribery" (Bamford 2008: 141–42).

More recently, in October 2012, an NSA official identified as "DIRNSA," or Director General Keith Alexander, proposed that in countering Muslim radicals their "vulnerabilities, if exposed, would likely call into question a radicalizer's devotion to the jihadist cause, leading to the degradation or loss of his authority." Citing the two timeless sources of scandal, sex and money, the agency suggested such vulnerabilities would likely include "viewing sexually explicit material online" or "using a portion of the donations they are receiving … to defray personal expenses." The NSA document identified one potential target as a "respected academic" whose "vulnerabilities" are "online promiscuity." According to author Bamford: "The NSA's operation is eerily similar to the FBI's operations under J. Edgar Hoover in the 1960s where the bureau used wiretapping to discover vulnerabilities, such as sexual activity, to 'neutralize' their targets." In response to this leaked NSA document, the deputy legal director of the American Civil Liberties Union, Jameel Jaffer, warned that the "president will ask the NSA to use the fruits of surveillance to discredit a political opponent, journalist or human rights activist" (Greenwald, Gallagher, and Grim 2013).

Indeed, famed whistleblower Edward Snowden has accused the NSA of actually conducting such surveillance, saying: "They even keep track of who is having an affair or looking at pornography, in case they need to damage their target's reputation … These programs were never about terrorism … They're about power" (Snowden 2013).

Just as the internet has centralized communications, so it has moved most commercial sex into cyberspace, providing the NSA easy access to the embarrassing habits of targets worldwide, whether Muslim militants or European leaders. With an estimated 25 million salacious sites worldwide and 10.6 billion page views *per month* at the top five sex sites in 2013, online pornography has become, as of 2006, a $97 billion global business (Rosen 2013; *TopTenReviews* 2007).

Revelations from Snowden's cache of leaked documents in late 2013 indicate the NSA has conducted close surveillance of leaders in 35 nations worldwide—including Brazilian president Dilma Rousseff's personal phone; cabinet communications of former Mexican president Felipe Calderon and the email of his successor, Enrique Peña Nieto; intercepts for Chancellor Angela Merkel's cell phone calls since 2002; phones taps of Indonesia's president Susilo Bambang Yudhoyono; and "widespread surveillance" of world leaders during the Group 20 summit meeting at Ottawa in June 2010 (Romero and Archibold 2013;

Rubin 2013; Smale 2013a; Sanger and Mazzetti 2013; Smale 2013b; Editorial 2013; Mazzetti and Sanger 2013; Cochrane 2013; Austen 2013).

Such digital surveillance has tremendous political potency for scandal, exemplified by New York Governor Elliot Spitzer's forced resignation in 2008 after phone taps revealed his use of escort services; and the ouster of France's budget minister Jérôme Cahuzac in 2013 following phone taps that exposed his secret Swiss bank account (Feuer 2008; Pitney 2008; Chrisafis 2012, 2013). Again, the source of such scandal remains sex or money, both of which are readily tracked by the electronic surveillance that is the NSA's forte.

Indicating the acute sensitivity of such executive communications, world leaders have reacted strongly to reports of NSA surveillance—a response with potentially deleterious consequences for U.S. relations with key allies. Chancellor Merkel demanded Five-Eyes exempt status for Germany (Smale 2013d, 2013c, 2013a). France's Prime Minister François Hollande insisted, "We cannot accept this kind of behavior between partners and allies" (Erlanger 2013; Rubin 2013). After the European Parliament voted to curtail sharing of bank data with Washington, its president Martin Shultz explained: "When you approach a negotiation and you need to be afraid that the other side … has already spied out what you are going to say in that negotiation, then we are not talking about equal partners any more" (*TV Newsroom—European Council of the EU* 2013). Not only did Brazil's President Rousseff cancel a state visit to Washington in September 2013 after reports about NSA taps on her phone, but within two months the state telecom company Telebras announced a joint venture with Embraer for a $560 million satellite network that will free Brazil from the internet and thereby "ensure the sovereignty of its strategic communications" (Romero 2013; *MercoPress* 2013).

Information and the Future of U.S. Global Power

By leaking a swelling stream of NSA documents, whistleblower Edward Snowden has given us a glimpse of future U.S. defense policy and the changing architecture of its global power. At the broadest level, this digital pivot complements Obama's overall defense strategy, announced in 2012, of cutting costs (slashing infantry by 14 per cent) while conserving America's global power through a capacity for "a combined arms campaign across all domains—land, air, maritime, space, and cyberspace" (Barnes and Hodge 2012; U.S. Department of Defense 2012: 2–5).

Since 2009, digital surveillance has morphed into "cyberwarfare" when Obama formed the U.S. Cyber Command (CYBERCOM), with a cybercombat center at Lackland Air Base initially staffed by 7,000 air force employees (*New York Times* 2009). Over the next two years, the Pentagon created an enormous concentration of power by appointing the NSA's chief, General Keith Alexander, as CYBERCOM's concurrent commander and declaring cyberspace an "operational domain" for offensive and defensive warfare (Armed Forces News Service 2010; Alexander 2011). Simultaneously, Washington deployed its first cyber-viruses with devastating effect against Iran's nuclear facilities from 2006 to 2010 (*New York Times* 2008, 2011, 2012; Brenner 2011: 102–05; Traynor 2007; Baldior 2010, 2012).

While cutting conventional armaments, President Obama has invested billions to build a new architecture for global information control. According to documents Snowden leaked to the *Washington Post* in August 2013, the U.S. has spent $500 billion on intelligence agencies in the dozen years since 9/11, including 2012 appropriations of $10.3 billion for the National Reconnaissance Office, $10.8 billion for the NSA, and $14.7 billion for the CIA (Shane 2013). If we add the $791 billion expended on the Department of Homeland Security to this $500 billion for global intelligence in the dozen years since 9/11, then Washington has made a $1.2 trillion investment in hardware, software, and personnel to build a formidable apparatus with enormous, unexplored implications for U.S. state controls at home and abroad (Kramer and Hellman 2013).

So formidable has this security bureaucracy become that, in December 2013, Obama's executive review committee recommended regularization, not reform, of current NSA practices, allowing the agency to continue tapping all domestic and international communications. Any monitoring of foreign leaders would now require presidential approval, a power Obama has already exercised by promising Germany's Chancellor Merkel that her phone will no longer be tapped and by refusing to extend the same assurance to the presidents of Brazil and Mexico, America's now insubordinate subordinate elites (Sanger 2013).

To store and process the billions of messages swept up by its worldwide surveillance, the NSA employed, as of June 2013, 11,000 workers constructing, at a cost of $1.6 billion, a Data Center in Bluffdale, Utah, with an immense storage capacity measured in yottabytes. Since each yottabyte is equivalent to a trillion terabytes, this is an unimaginably vast capacity when one realizes that just fifteen terabytes could store every publication in the Library of Congress (MacAskill and Borger 2013; Poitras *et al*. 2013). In its quest for ever more powerful supercomputers for data processing and decoding encryption, the NSA deployed the Cray Cascade in 2010, developed by Defense Advanced Research Projects Agency (DARPA) at an unprecedented cost of $250 million and capable of a quadrillion calculations per second (Bamford 2008: 338–39; Gruner 2012).

From its new $2 billion headquarters, the third-biggest building in Washington, D.C., the National Geospatial-Intelligence Agency deploys 16,000 employees and a $5 billion budget to coordinate a rising torrent of surveillance data from U-2 spy planes, Global Hawks, X-37B space drones, Google Earth, and orbital satellites (Easterbrook 2011; National Geospatial-Intelligence Agency 2006, 2007; Priest and Arkin 2010).

By 2020, moreover, the U.S. will deploy a triple-canopy aerospace shield, advanced cyberwarfare, and digital surveillance to envelop the earth in an electronic grid capable of blinding entire armies on the battlefield or atomizing a single insurgent in field or *favela*. At the outer level in the Exosphere, the weaponization of space started in April 2010 when the U.S. Air Force launched its first space drone, a mini space shuttle called the X-37B, that circled the globe for nine months in a low orbit of 255 miles with the potential for terrestrial surveillance and missile strikes against rival space targets (Broad 2010; Weeden 2010). To prevent China from blinding U.S. command communications by shooting down its satellites, DARPA is developing the F-6 fractionated satellite that scatters key components, preventing both enemy attack and equipment failure (Brown 2007; DARPA 2011b).

Closer to earth in the Upper Stratosphere, the Pentagon is developing the Falcon Hypersonic Cruise Vehicle that will fly at 13,000 miles per hour, 20 times the speed of sound, to "deliver 12,000 pounds of payload," destroying any target "anywhere in the world on 30 minutes notice" (Defense Advanced Research Projects Agency 2008; Singer 2009: 121; Shanker 2011).

In the Lower Stratosphere, within striking distance of earth, the Pentagon is launching an armada of 99 Global Hawk drones that cruise at 60,000-feet elevation—equipped with high-resolution cameras to surveil all terrain within a 100-mile radius, electronic sensors to intercept microwave communications, and efficient engines for 24-hour flight (Drew 2011). By late 2011, the U.S. Air Force and CIA had ringed the entire Eurasian landmass with a network of 60 bases for Reaper and Predator drones, stretching from Sicily across the Indian Ocean to Guam. With a range of 1,150 miles when armed with Hellfire missiles and GBU-30 bombs, U.S. Reaper drones could strike targets anywhere in Europe, Africa, and Asia (Turse 2011, 2012).

Ultimately, the third technological regime requires integration of this aerospace array into a robotic command structure that will coordinate operations across all combat domains—space, cyberspace, sky, sea, and earth. To manage this torrent of information, the system will need to become self-maintaining

through "robotic manipulator technologies" such as DARPA's FREND system that can fuel, repair, or reposition satellites. Thus, in its "Signit Strategy 2012–2016," the NSA planned to "dramatically increase mastery of the global network" by integration of its systems into a national matrix of robotic sensors that interactively "sense, respond and alert one another at machine speed" (Risen and Poitras 2013b; DARPA 2011a). In future, Washington will require such an automated system capable of translating this Babel of digital data, captured from drones in the skies above and fiber optic cables in the earth below, into actionable intelligence for the effective exercise of global power.

Conclusion

Through three Asian wars over the span of a century, these crucibles of counterinsurgency in the Philippines, Vietnam, and Iraq/Afghanistan have pushed U.S. pacification to its technological limits, forcing the formation of new systems of surveillance and information warfare. This ongoing process of technological innovation within its third information regime has significant but still uncertain implications for the future of U.S. global hegemony. However, what *is* certain is that understandings of that future require the methodological task, as demonstrated in this article, of historical inflection.

As the disparity grows between Washington's global reach and its withering mailed fist, as it struggles to maintain 40 per cent of the world's armaments circa 2012 with only 23 per cent of its gross output, the U.S. will need to find ways to exercise its global power more economically (Perlo-Freeman *et al*. 2013: 2; Johansson *et al*. 2012: 23, fig. 10). As its share of world output falls to 17 per cent by 2016 and its social welfare costs climb from 4 per cent of GDP in 2010 to 18 per cent by 2050, savings will become imperative for Washington's survival as a world power (International Monetary Fund 2011; Weisbrot 2011; Mandelbaum 2010: 20, 46–52, 185).

Compared to the trillion-dollar cost of conventional U.S. military intervention in Iraq, the NSA's 2012 budget of just $11 billion for worldwide surveillance and cyberwarfare is a cost-savings the Pentagon cannot afford to forego (Shane 2013). Cyberspace offers Washington a budget-priced arena of global power, albeit at the cost of trust by its closest allies—a contradiction that will bedevil America's global leadership for years to come.

Looking inward for the domestic implications of this history, the process of imperial mimesis leads a nation like the U.S., that exercises power beyond its borders through pervasive surveillance, to exhibit many of those same coercive features in its own society. Sadly, it seems that Mark Twain was right when he warned us, just over a hundred years ago, that America could not have both empire abroad and democracy at home.

References

Achutegui, Pedro S., S.J., and Miguel A. Bernad, S.J. 1961. *Religious Revolution in the Philippines, Volume 1: 1860–1940.* Quezon City: Ateneo de Manila.

Alexander, David. 2011. "Pentagon to Treat Cyberspace as 'Operational Domain'." *Reuters,* July 14. Accessed June 1, 2014. http://www.reuters.com/article/2011/07/14/us-usa-defense-cybersecurity-idUSTRE76D5FA20110714

Allen, Henry T. 1904. Letter to C. H. Brent, July 12. File: July to December 1904, Box 6, Charles Henry Brent Papers, Manuscript Division, U.S. Library of Congress (hereafter CHB).

American Machinist. 1902. "The Electric Tabulating Machine Applied to Cost Accounting." 1902. *American Machinist,* August 16.

Armed Forces News Service. 2010. "Gates Established US Cyber Command, Names First Commander." *U.S. Strategic Command*, May 21. Accessed June 1, 2014. http://www.stratcom.mil/news/2010/161/Gates_establishes_US_Cyber_Command_and_names_first_commander/

Austen, Ian. 2013. "Ire in Canada Over Report N.S.A. Spied From Ottawa." *New York Times*, November 29.

Austin, Charles J. 1992. *Information Systems for Health Services Administration.* Ann Arbor: University of Michigan Press.

Baldior, Lolita C. 2010. "Pentagon Takes Aim at China Cyber Threat." *Associated Press*, August 19. Accessed June 1, 2014. http://www.guardian.co.uk/world/feedarticle/9227669

Baldior, Lolita C. 2012. "U.S., China to Cooperate More on Cyber Threat." *Associated Press*, May 8. Accessed June 1, 2014. http://www.politico.com/news/stories/0512/76036.html
Ball, James, and Nick Hopkins. 2013. "GCHQ and NSA Targeted Charities, Germans, Israeli PM and EU Chief." *The Guardian*, December 20. Accessed June 1, 2014. http://www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner
Bamford, James. 2008. *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America.* New York: Random House.
Bandholtz, H. H. n.d. Copy Telegram No. 2, To: Adjutant General. Reel 9, Harry H. Bandholtz Papers, Michigan Historical Society (hereafter HHB).
Bandholtz, H. H. 1919/1991. "Provost Marshal General's Department," April 30. *United States Army in the World War 1917–1919: Reports of the Commander-in-Chief, Staff Sections and Services.* Washington, DC: Government Printing Office.
Bandholtz, H. H. 1921. Proclamation, September 2. Reel 9, HHB.
Bandholtz, H. H. 1921. To: the Adjutant General, September 12. Reel 9, HHB.
Barnes, Julian E., and Nathan Hodge. 2012. "Military Faces Historic Shift." *Wall Street Journal,* January 6.
Barrett Jr., Edward L. 1951. *The Tenney Committee: Legislative Investigation of Subversive Activities in California.* Ithaca, NY: Cornell University Press.
Barry, Thomas H. 1901. Brigadier General U.S. Volunteers, Chief of Staff, to the Commanding General, Department of Northern Luzon, March 11. Entry 4337, RG 395, National Archives and Records Administration (hereafter NARA).
Beaumont, Hartford. 1904. Letter to Honorable Henry C. Ide, December 7. Book 21:II, Dean C. Worcester Papers, Harlan Hatcher Library, University of Michigan.
Belmont, A.H. 1951. Letter to D.M. Ladd, November 9. Subject: Van Deman, Ralph Henry, Files 65-37516, 94-37515, Federal Bureau of Investigation, Washington, DC (hereafter RVD).
Bertillon, Alphonse. 1899/1977. *Alphonse Bertillon's Instructions for Taking Descriptions for the Identification of Criminals and Others by the Means of Anthropometric Indications.* New York: AMS Press.
Bethel, Elizabeth. 1947. "The Military Information Division: Origin of the Intelligence Division." *Military Affairs* 11(1): 17–24.
Bigelow, Michael E. 1990. "Van Deman." *Military Intelligence* 16(4): 38–40.
Binder, David. 1978. "Carter Signs Order to Reorganize Intelligence and Curb Surveillance." *New York Times,* January 15.
Brenner, Joel. 2011. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare.* New York: Penguin.
Brent, Charles H. n.d. "Private Addendum to Report on Religious Conditions in the Philippine Islands (For Bishops Only)." Box 6, CHB.
Brent, C. H. 1904a. Letter to General Henry T. Allen, July 11. Box 8, File: 1904 June–Aug, Henry T. Allen Papers, Manuscript Division, U.S. Library of Congress (hereafter HTA).
Brent, C. H. 1904b. Letter to General Henry T. Allen, October 12. Box 8, File: 1904 Sept–Oct, HTA.
Brent, C. H. 1904c. Letter to General Henry T. Allen, October 12. Box 6, File: July to December 1904, CHB.
Broad, William J. 2010. "Surveillance is Suspected As Main Role Of Spacecraft." *New York Times,* May 23.
Brown, Owen. 2007. Speech. August 8.
Burnham, David. 1978. "Congress Studies Bill to Require Judicial Scrutiny of Some Spying." *New York Times,* January 25.
Burnham, David. 1986. "Truman Wiretaps on Ex-New Deal Aide Cited." *New York Times*, February 1. Accessed June 1, 2014. http://www.nytimes.com/1986/02/01/us/truman-wiretaps-on-ex-new-deal-aide-cited.html
California Legislature. 1949. *Fifth Report of the Senate Fact-Finding Committee on Un-American Activities, 1949.* Sacramento: Senate of the State of California.
Campbell, Kenneth. 1987. "Major General Ralph H. Van Deman: Father of Modern American Military Intelligence." *American Intelligence Journal* 8: 13–19.
Castle, Stephen, and Eric Schmitt. 2013. "Europeans Voice Anger Over Reports of Spying by U.S. on Allies." *New York Times,* July 1.
Cauley, Leslie. 2006. "NSA Has Massive Database of Americans' Phone Calls." *USA Today*, May 11. Accessed June 1, 2014. http://yahoo.usatoday.com/news/washington/2006-05-10-nsa_x.htm
Charlton, Linda. 1977. "Senate Gets Carter Bill to Curb Foreign Intelligence Wiretapping." *New York Times,* May 19.
Chrisafis, Angelique. 2012. "French Budget Minister Accused of Hiding Swiss Bank Account." *The Guardian*, December 27. Accessed June 1, 2014. http://www.theguardian.com/world/2012/dec/27/french-budget-minister-swiss-account
Chrisafis, Angelique. 2013. "France's Former Budget Minister Admits Lying about Secret Offshore Account." *The Guardian,* April 2. Accessed June 1, 2014. http://www.theguardian.com/world/2013/apr/02/jerome-cahuzac-france-offshore-account
Clifford, Mary Dorita, B.V.M. 1969. "Iglesia Filipina Independiente: The Revolutionary Church." In *Studies in Philippine Church History,* edited by Gèrald H. Anderson, 223–55. Ithaca, NY: Cornell University Press.
Clymer, Kenton J. 1986. *Protestant Missionaries in the Philippines, 1898–1916: An Inquiry into the American Colonial Mentality.* Urbana: University of Illinois Press.
Cochrane, Joe. 2013. "N.S.A. Spying Scandal Tarnishes Relations Between Two Friendly Nations." *New York Times*, November 20.
Coe, Lewis. 1993. *The Telegraph: A History of Morse's Invention and Its Predecessors in the United States.* Jefferson, NC: McFarland.

Comaromi, John, and M. Satija. 1988. *Dewey Decimal Classification: History and Current Status.* New York: Envoy.
Crossen, Cynthia. 2002. "Early TIPS Corps Did More Harm Than Good in Hunt for Subversives." *Wall Street Journal*, October 2.
Defense Advanced Research Projects Agency (DARPA). 2008. "Falcon Technology Demonstration Program HTV-3X Blackswift Test Bed." Accessed June 1, 2014. http://www.scribd.com/doc/180954975/Falcon-Blackswift-FS-Oct08
Defense Advanced Research Projects Agency (DARPA), Tactical Technology Office. 2011a. "Front-End Robotic Enabling Near-Term Demonstration (FREND)." Accessed Feb 16, 2015. http://www.darpa.mil/WorkArea/DownloadAsset.aspx?id=2147486079
Defense Advanced Research Projects Agency (DARPA), Tactical Technology Office. 2011b. "System F6." Accessed Feb 16, 2015. https://www.fbo.gov/utils/view?id=522ee0572c59fd5479e477decb4afddd
Dilworth, Donald C., ed. 1977. *Identification Wanted: Development of the American Criminal Identification Systems, 1893–1943.* Gaithersburg, MD: International Association of Chiefs of Police, Police Management & Operations Divisions.
Director. 1951. Letter to SAC San Diego, December 11. RVD.
Ditzel, Paul. 1990. *Fire Alarm!: The Story of a Fire Department.* New Albany: Van Nostrand-Reinhold.
Dorwart, Jeffrey M. 1983. *Conflict of Duty: The U.S. Navy's Intelligence Dilemma, 1919–1945.* Annapolis: Naval Institute Press.
Drew, Christopher. 2011. "Under an Unblinking Eye." *New York Times*, August 2.
Easterbrook, Greg. 2011. "Undisciplined Spending in the Name of Defense." *Reuters*, January 20. Accessed June 1, 2014. http://blogs.reuters.com/gregg-easterbrook/2011/01/20/undisciplined-spending-in-the-name-of-defense/
Editorial. 2013. "More Damage from N.S.A. Snooping." *New York Times*, October 26.
Eggen, Dan. 2002. "Under Fire, Justice Shrinks TIPS Program." *Washington Post*, August 10.
Ehrhard, Thomas P. 2000. "Unmanned Aerial Vehicles in the United States Armed Services: A Comparative Study of Weapon System Innovation." PhD diss., John Hopkins University.
Erlanger, Steven. 2013. "Outrage in Europe Grows Over Spying Disclosures." *New York Times,* July 2.
"Family History of M.Q." ca. 1900. Box 7, File: 1900 Oct, HTA.
Feuer, Alan. 2008. "Four Charged with Running Online Prostitution Ring." *New York Times*, March 7.
Gamewell Fire Alarm Telegraph Co. 1916. *Emergency Signaling.* New York: Gamewell Fire Alarm Telegraph Co.
Gates, John Morgan. 1973. *Schoolbooks and Krags: The United States Army in the Philippines, 1898–1902.* Westport, CT: Greenwood.
Gellman, Barton and Laura Poitras. 2013. "U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program." *Washington Post*, June 6. Accessed June 1, 2014. http://articles.washingtonpost.com/2013-06-06/news/39784046_1_prism-nsa-u-s-servers
Gellman, Barton and Ashkan Soltani. 2013. "NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say." *Washington Post*, October 30. Accessed June 1, 2014. http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html
Gernsheim, Helmut and Alison Gernsheim. 1969. *The History of Photography: From the Camera Obscura to the Beginning of the Modern Era.* New York: McGraw-Hill.
Gerth, H. H. and C. Wright Mills, eds. 1946. *From Max Weber: Essays in Sociology.* New York: Oxford University Press.
Gibson, James William. 1986. *Perfect War: The War We Couldn't Lose and How We Did.* New York: Vintage.
Glanz, James and Andrew W. Lehren. 2013. "U.S. and Britain Extended Spying to 1,000 Targets." *New York Times*, December 21.
Goebel, Greg. 2006. "The Lightning Bug Reconnaissance Drones." Accessed June 1, 2014. http://web.archive.org/web/20060925145823/www.vectorsite.net/twuav_04.html
Greenwald, Glenn. 2013a. "NSA Collecting Phone Records of Millions of Verizon Customers Daily." *The Guardian*, June 5. Accessed June 1, 2014. http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order
Greenwald, Glenn. 2013b. "XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet'." *The Guardian*, July 31. Accessed June 1, 2014. http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data
Greenwald, Glenn, Ryan Gallagher and Ryan Grim. 2013. "Top-Secret Document Reveals NSA Spied On Porn Habits As Part Of Plan To Discredit 'Radicalizers'." *Huffington Post*, November 26. Accessed June 1, 2014. http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html
Gross, Grant. 2014. "Surveillance Court Renews NSA Phone Records Program." *Computer World*, January 3. Accessed June 1, 2014. http://www.computerworld.com/s/article/9245152/Surveillance_court_renews_NSA_phone_records_program
Grove, Winfield S. 1903. To: Brig. Gen. Henry T. Allen. Box 8, File: 1903 Nov-Dec, HTA.
Gruner, Wolfgang. 2012. "Cray's New Supercomputer KC30 Delivers 66 TFlops/Cabinet." *Tom's Hardware*, November 12. Accessed June 1, 2014. http://www.tomshardware.com/news/cray-xc30-supercomputer,19014.html
Halloran, Richard. 1971. "Senate Panel Holds Vast 'Subversives' File Amassed by Ex-Chief of Army Intelligence." *New York Times*, September 7.
Harbord, J. G. 1921. To: Brigadier General H. H. Bandholtz, August 31. Reel 9, HHB.
Heath, Richard. 1981. *Mill City Firefighters: The First Hundred Years, 1879–1979.* Minneapolis: Extra Alarm Association of the Twin Cities.
Hein, F.W. 1951. To: Commanding Officer 115th CIC Detachment, March 8. RVD.
Henry, E. R. 1900. *Classification and Uses of Fingerprints.* London: Routledge.
Hentoff, Nat. 2002a. "Rescued by Dick Armey from Big Brother." *Washington Times*, July 29.

Hentoff, Nat. 2002b. "The Death of Operation TIPS." *Village Voice*, December 18.
Hersh, Seymour M. 1974. "Huge C.I.A. Operation Reported in U.S. Against Antiwar Forces, Other Dissidents in Nixon Years." *New York Times,* December 22.
Hodge, Nathan. 2009. "General Wants to Scan More U.S. Irises, Fingerprints." *Wired.com*, January 29. Accessed June 1, 2014. http://www.wired.com/dangerroom/2009/01/biometrics-need/
Horrock, Nicholas M. 1975a. "Report on Spying Released by C.I.A." *New York Times,* July 9.
Horrock, Nicholas M. 1975b. "Tightened Controls Over Agency Urged." *New York Times*, June 11.
Horrock, Nicholas M. 1976. "Ford Bill Opposes Taps on Citizens." *New York Times,* March 17.
Horrock, Nicholas M. 1979. "Senate Passes Bill to Bar Bugging in U.S. Without Court Order." *New York Times,* April 21.
Howard, Zach. 2011. "Police to Begin iPhone Iris Scans Amid Privacy Concerns." *Reuters,* July 20. Accessed June 1, 2014. http://www.reuters.com/article/2011/07/20/us-crime-identification-iris-idUSTRE76J4A120110720
Howell, Joel D. 1995. *Technology in the Hospital: Transforming Patient Care in the Early Twentieth Century.* Baltimore: The Johns Hopkins University Press.
Howells, Mark. 2000. "High Tech in the 90s: The 1890 Census." Accessed June 1, 2014. http://www.oz.net/~markhow/writing/holl.htm
Hunt, Richard A. 1990. *Pacification: The American Struggle for Vietnam's Hearts and Minds.* Boulder, CO: Westview.
Hyman, Harold M. 1959. *To Try Men's Souls: Loyalty Tests in American History.* Berkeley: University of California Press.
Immerman, Richard H. 2014. *The Hidden Hand: A Brief History of the CIA*. Malden: Wiley Blackwell.
Institute for the History of Technology and Industrial Anthropology. 1992. *The Battle of Blair Mountain (West Virginia): Cultural Resource Survey and Recording Project.* Morgantown: West Virginia University.
International Monetary Fund. 2011. "World Economic Outlook Database." Accessed June 1, 2014. http://www.imf.org/external/pubs/ft/weo/2011/01/weodata/index.aspx
Isaacson, H.S. 1951. To: Major General A.R. Bolling, November 27. RVD.
Jeffreys-Jones, Rhodri. 2007. *The FBI: A History.* New Haven: Yale University Press.
Jensen, Joan M. 1968. *The Price of Vigilance.* Chicago: Rand McNally.
Jensen, Joan M. 1991. *Army Surveillance in America, 1775–1980.* New Haven: Yale University Press.
Johansson, Åsa, Yvan Guillemette, Fabrice Murtin, David Turner, Giuseppe Nicoletti, Christine de la Maisonneuve, Philip Bagnoli, Guillaume Bousquet and Francesca Spinelli. 2012. "Looking to 2060: Long-Term Global Growth Prospects." *OECD Economic Policy Papers*, *No. 3.*
Jones, Douglas W. n.d. "Punched Cards: A Brief Illustrated Technical History." Accessed June 2, 2014. http://homepage.cs.uiowa.edu/~jones/cards/history.html
Kahn, David. 2004. *The Reader of Gentlemen's Mail: Herbert O. Yardley and the Birth of American Codebreaking.* New Haven: Yale University Press.
Keay, V.P. 1952. Letter to A.H. Belmont, January 22. RVD.
Kelly, Kitty. 1988. "The Dark Side of Camelot." *People Magazine,* January 29. Accessed June 2, 2014. http://archive.people.com/people/archive/jpgs/19880229/19880229-750-113.jpg
Kessler, Ronald. 2011. *The Secrets of the FBI.* New York: Random House.
Khaki and Red, September 1927.
Khaki and Red, September 1932.
Kistermann, Friedrich W. 2005. "Hollerith Punched Card System Development (1905–1913)." *IEEE Annals of the History of Computing* 27, no. 1: 56–66.
Komer, R. W. 1970. *Organization and Management of the "New Model" Pacification Program—1966–1969.* Santa Monica, CA: Rand.
Koon, S. G. 1914. "Cost Accounting by Machines." *American Machinist,* March 26.
Kornweibel Jr., Theodore. 1998. *"Seeing Red": Federal Campaigns against Black Militancy, 1919–1925.* Bloomington: Indiana University Press.
Kramer, Mattea and Chris Hellman. 2013. "'Homeland Security': The Trillion-Dollar Concept That No One Can Define." *TomDispatch*, February 28. Accessed June 2, 2014. http://www.tomdispatch.com/blog/175655/
Ladd, D.M. 1945. Letter to E.A. Tamm, October 29. RVD.
LaMontagne, Leo E. 1961. *American Library Classification with Special Reference to the Library of Congress.* Hamden, CT: Shoestring Press.
Laurie, Clayton D. and Ronald H. Cole. 1997. *The Role of Federal Military Forces in Domestic Disorders, 1877–1945.* Washington, DC: Government Printing Office.
Lester, Robert. 1990. *A Guide to the Microfilm Edition of the Records of the Military Assistance Command Vietnam: Part 3. Progress Reports on Pacification in South Vietnam, 1965–1973.* Bethesda: University Publications of America.
Lichtblau, Eric. 2003. "Administration Plans Defense of Terror Law." *New York Times*, August 19.
Lichtblau, Eric. 2004. "Secret Warrant Requests Increased in 2003." *New York Times*, May 3.
Lichtblau, Eric. 2005. "Large Volume of F.B.I. Files Alarms U.S. Activist Groups." *New York Times*, July 18.
Litchblau, Eric. 2013. "In Secret, Court Vastly Broadens Powers of N.S.A." *New York Times*, July 7.
MacAskill, Ewen, Julian Borger, Nick Hopkins, Nick Davies and James Bell. 2013. "GCHQ Taps Fibre-optic Cables for Secret Access to World's Communications." *The Guardian*, June 21. Accessed June 2, 2014. http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

MacAskill, Ewen and Julian Borger. 2013. "New NSA Leaks Show How US is Bugging its European Allies." *The Guardian*, June 30. Accessed June 2, 2014. http://www.guardian.co.uk/world/2013/jun/30/nsa-leaks-us-bugging-european-allies
Mazzetti, Mark and David E. Sanger. 2013. "Tap on Merkel Provides Peek at Vast Spy Net." *New York Times*, October 31.
Linn, Brian McAllister. 1989. *The U.S. Army and Counterinsurgency in the Philippine War, 1899–1902.* Chapel Hill: University of North Carolina Press.
Linn, Brian McAllister. 1991. "Intelligence and Low-Intensity Conflict in the Philippine War, 1899–1902." *Intelligence and National Security* 6, no. 1: 90–96.
Linn, Brian McAllister. 2000. *The Philippine War: 1899–1902.* Lawrence: University of Kansas Press.
Little Jr., Robert W. 1976. *York City Fire Department, York, Pennsylvania.* York: n.p.
Mandelbaum, Michael. 2010. *The Frugal Superpower: America's Global Leadership in a Cash-Strapped Era.* New York: PublicAffairs.
Mansfield-Devine, Steve. 2012. "Biometrics at War: The US Military's Need for Identification and Authentication." *Biometric Technology Today* 5: 5–8.
Maver, Jr., William. 1903. *American Telegraphy and Encyclopedia of the Telegraph: Systems, Apparatus, Operation.* New York: Holt.
McCormick, Charles H. 1997. *Seeing Reds: Federal Surveillance of Radicals in the Pittsburgh Mill District, 1917–1921.* Pittsburgh: University of Pittsburgh Press.
McCoy, Alfred W. 2009. *Policing America's Empire: The United States, the Philippines, and the Rise of the Surveillance State.* Madison: University of Wisconsin Press.
McGilligan, Patrick and Paul Buhle. 1997. *Tender Comrades: A Backstory of the Hollywood Blacklist.* New York: St. Martin's.
MercoPress (Montevideo). 2013. "Brazil Will Have Its Own National-made Secure Communications Satellite by 2016." November 29. Accessed June 2, 2014. http://en.mercopress.com/2013/11/29/brazil-will-have-its-own-national-made-secure-communications-satellite-by-2016
Military Secretary's Office. 1904. *Official Army Register for 1905.* Washington, DC: Government Printing Office.
Minutes. 1921. Twenty-Ninth Consecutive and Fourth Biennial Convention of District No. 5, United Mine Workers of America, First Day, Pittsburg, Pa., September 6. Reel 9, HHB.
Moran, Christopher R. and Christopher J. Murphy, eds. 2013. *Intelligence Studies in Britain and the US: Historiography Since 1945*. Edinburgh: Edinburgh University Press.
Morn, Frank. 1982. *"The Eye That Never Sleeps": A History of the Pinkerton National Detective Agency.* Bloomington: Indiana University Press.
Mueller, III, Robert M. 2006. Testimony, U.S. Senate Committee on the Judiciary: "FBI Oversight," May 2. Accessed June 2, 2014. http://www.fas.org/irp/congress/2006_hr/050206mueller.html
Nakashima, Ellen. 2006. "FBI Show Off Counterterrorism Database." *Washington Post*, August 30.
National Geospatial-Intelligence Agency. 2006. *Geospatial Intelligence Standards: Enabling A Common Vision.* Washington, D.C.: National Geospatial-Intelligence Agency. Accessed June 2, 2014. http://www.fas.org/irp/agency/nga/standards.pdf
National Geospatial-Intelligence Agency. 2007. *National System for Geospatial Intelligence (NSG), Statement of Strategic Intent.* Washington, DC: National Geospatial-Intelligence Agency. Accessed June 2, 2014. https://www1.nga.mil/About/Documents/nsg_strategic_intent.pdf
National Security Agency. 1946. "Minutes of the Inauguration Meeting British Signal Intelligence Conference, 11–27 March" (UKUSA Agreement Release 1940–1956). Accessed June 2, 2014. http://www.nsa.gov/public_info/_files/ukusa/minutes_inauguration_11mar46.pdf
National Security Agency, Office of Inspector General. 2009. "Working Draft," March 24. Accessed June 2, 2014. http://apps.washingtonpost.com/g/page/world/national-security-agency-inspector-general-draft-report/277/
National Security Agency. 2012. "Driver 1: Worldwide SIGINT/Defense Cryptologic Platform." In "NSA Infected 50,000 Computer Networks with Malicious Software," by Floor Boon, Steven Derix and Huib Modderkolk, *NRC Handelsblad*, November 23, 2013. Accessed June 2, 2014. http://www.nrc.nl/nieuws/2013/11/23/nsa-infected-50000-computer-networks-with-malicious-software/
New York Times. 1949a. June 9.
New York Times. 1949b. June 10.
New York Times. 1971. September 7.
New York Times. 2008. August 12.
New York Times. 2009. June 12.
New York Times. 2011. October 18.
New York Times. 2012. June 1.
Norton-Taylor, Richard. 2010. "Not So Secret: Deal at the Heart of UK–US Intelligence." *The Guardian*, June 24. Accessed June 2, 2014. http://www.guardian.co.uk/world/2010/jun/25/intelligence-deal-uk-us-released
O'Brien, Michael. 1999. "The Exner File—Judith Campbell Exner, John F. Kennedy's Mistress." *Washington Monthly*, December 1. Accessed June 2, 2014. http://www.highbeam.com/doc/1G1-58170292.html
Perlo-Freeman, Sam, Elisabeth Sköns, Carina Solmirano and Helen Wilandh. 2013. *Trends in World Military Expenditure, 2012.* Stockholm: Stockholm International Peace Research Institute.

Perlroth, Nicole, Jeff Larson and Scott Shane. 2013. "N.S.A. Able To Foil Basic Safeguards of Privacy on Web." *New York Times,* September 6.
Philippines Free Press. 1918. May 11.
Pitney, Nico. 2008. "Spitzer As Client 9: Read Text Messages From Spitzer To Prostitute." *Huffington Post*, March 10. Accessed June 2, 2014. http://www.huffingtonpost.com/2008/03/10/spitzer-as-client-9-read-_n_90787.html
Poitras, Laura, Rosenbach, Marcel, Schmid, Fidelius, Stark, Holger, and Jonathan Stock. 2013. "How the NSA Targets Germany and Europe." *Der Spiegel*, July 1. Accessed June 2, 2014. http://www.spiegel.de/international/world/secret-documents-nsa-targeted-germany-and-eu-buildings-a-908609.html
Polenberg, Richard. 1987. *Fighting Faiths: The Abrams Case, the Supreme Court, and Free Speech.* New York: Penguin.
Police Chiefs News Letter 2, no. 3 (March 1934).
Police Chiefs News Letter 3, no. 7 (July 1936).
Powe, Marc B. 1975. "American Military Intelligence Comes of Age." *Military Review* 40, no. 12: 17–30.
Prados, John. 1996. *President's Secret Wars: CIA and Pentagon Covert Operations from World War II Through the Persian Gulf.* Chicago: Ivan R. Dee.
Priest, Dana, and William M. Arkin. 2010. "Top Secret America." *Washington Post,* July 18, 19, 20, and 21.
A Proclamation by the President of the United States, n.d., Reel 9, HHB.
Pugh, Emerson W. 1995. *Building IBM: Shaping an Industry and Its Technology.* Cambridge: MIT Press.
Risen, James, and Eric Lichtblau. 2005. "Bush Let U.S. Spy on Callers Without Courts." *New York Times*, December 16. Accessed June 2, 2014. http://www.nytimes.com/2005/12/16/politics/16program.html
Risen, James, and Eric Lichtblau. 2013. "How the U.S. Uses Technology to Mine More Data More Quickly." *The New York Times*, June 8. Accessed June 2, 2014. http://www.nytimes.com/2013/06/09/us/revelations-give-look-at-spy-agencys-wider-reach.html
Risen, James, and Laura Poitras. 2013a. "N.S.A. Examines Social Networks of U.S. Citizens." *New York Times,* September 29.
Risen, James, and Laura Poitras. 2013b. "N.S.A. Report Outlined Goals for More Power." *New York Times*, November 23.
Roach, R. R. 1945. Letter to D. M. Ladd, July 13. RVD.
Rhodes, Henry T. F. 1956. *Alphonse Bertillon: Father of Scientific Detection.* London: G. G. Harrap.
Richards, G. Tilghman. 1964. *The History and Development of Typewriters.* London: H. M. Stationery Office.
Robinson, Ronald. 1972. "Non-European Foundations of European Imperialism: Sketch for a Theory of Collaboration." In *Studies in the Theory of Imperialism,* edited by Roger Owen and Bob Sutcliffe, 117–42. London: Longman.
Romero, Simon. 2013. "Brazil's Leader Postpones State Visit to Washington Over Spying." *New York Times,* September 17. Accessed June 2, 2014. http://www.nytimes.com/2013/09/18/world/americas/brazils-leader-postpones-state-visit-to-us.html
Romero, Simon, and Randal C. Archibold. 2013. "Brazil Angered Over Report N.S.A. Spied on President." *New York Times*, September 3.
Rosen, David. 2013. "Is Success Killing the Porn Industry?" *Alternet*, May 27. Accessed June 2, 2014. http://www.alternet.org/sex-amp-relationships/success-killing-porn-industry.
Rubin, Alissa J. 2013. "French Condemn Surveillance by N.S.A." *New York Times*, October 22.
SAC San Diego. 1952. To Director, February 4. RVD.
SAC SF (San Francisco). n.d. To Director. RVD.
Sanger, David E. 2013. "Obama Panel Said to Urge N.S.A. Curbs." *New York Times*, December 13.
Sanger, David E., and Mark Mazzetti. 2013. "Allegation of U.S. Spying on German Leader Puts Obama at Crossroads." *New York Times*, October 25.
Santoiana. 1952. To Director, January 22. RVD.
Savage, Charles. 2013. "Facial Scanning is Making Gains in Surveillance," *New York Times*, August 21.
Savage, Charles, and Scott Shane. 2013. "Top-Secret Court Castigated N.S.A. on Surveillance." *New York Times,* August 22.
Schmidt, Regin. 2000. *Red Scare: FBI and the Origins of Anticommunism in the United States, 1919–1943.* Copenhagen: Museum Tusculanum Press.
Scott, James C. 1998. *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed.* New Haven: Yale University Press.
Shane, Scott. 2013. "New Leaked Document Outlines U.S. Spending on Intelligence Agencies." *New York Times*, August 30.
Shanker, Thom . 2011. "Military's Test Vehicle is Launched, Then Crashes." *New York Times*, August 12.
Shenon, Philip. 2002. "Secret Court Weighs Wiretaps." *New York Times*, September 10.
Singer, P.W. 2009. *Wired for War: The Robotics Revolution and Conflict in the 21st Century.* New York: Penguin.
Skowronek, Stephen. 1982. *Building a New American State: The Expansion of National Administrative Capacities, 1877–1920.* Cambridge: Cambridge University Press.
Smale, Alison. 2013a. "Anger Growing Among Allies On U.S. Spying." *New York Times*, October 24.
Smale, Alison. 2013b. "Data Suggests U.S. Spying on Merkel Dates to '02." *New York Times*, October 28.
Smale, Alison. 2013c. "Indignation Over Spying on Merkel May Harm U.S." *New York Times*, October 25.
Smale, Alison. 2013d. "Surveillance Revelations Shake U.S.-German Ties." *New York Times*, August 26.
Snowden, Edward. 2013. "An Open Letter to the People of Brazil." *Folha de S. Paulo*, December 16. Accessed June 2, 2014. http://www1.folha.uol.com.br/internacional/en/world/2013/12/1386296-an-open-letter-to-the-people-of-brazil.shtml

Summers, Anthony. 2011. "The Secret Life of J Edgar Hoover." *The Observer*, December 31. Accessed June 2, 2014. http://www.theguardian.com/film/2012/jan/01/j-edgar-hoover-secret-fbi

Talbert, Jr., Roy. 1991. *Negative Intelligence: The Army and the American Left, 1917–1941.* Jackson: University Press of Mississippi.

Thorwald, Jürgen. 1965. *The Century of the Detective.* New York: Harcourt, Brace & World.

TopTenReviews. 2007. "Press Releases," March 12. Accessed June 2, 2014. http://www.toptenreviews.com/3-12-07.html

Traynor, Ian. 2007. "Russia Accused of Unleashing Cyberwar to Disable Estonia." *The Guardian,* May 16. Accessed June 2, 2014. http://www.guardian.co.uk/world/2007/may/17/topstories3.russia

TV Newsroom—European Council of the EU. 2013. "Arrival and Doorstep by Martin Schulz, President of the European Parliament, Prior to the European Council Taking Place on 24 October 2013 in Brussels." Accessed on June 1, 2014. http://tvnewsroom.consilium.europa.eu/video/shotlist/arrival-and-doorstep-ep-president-schulz4

Turse, Nick. 2011. "America's Secret Empire of Drone Bases: Its Full Extent Revealed for the First Time." *TomDispatch,* October 16. Accessed June 2, 2014. http://www.tomdispatch.com/blog/175454/tomgram%3A_nick_turse%2C_mapping_america%27s_shadowy_drone_wars

Turse, Nick. 2012. "The Crash and Burn Future of Robot Warfare: What 70 Downed Drones Tell Us About the New American Way of War." *TomDispatch*, January 15. Accessed June 2, 2014. http://www.tomdispatch.com/archive/175489/.

Twain, Mark. 1992. "Passage from 'Outlines of History' (suppressed) Date, 9th Century" (early 1900s). In *Mark Twain's Weapons of Satire: Anti-Imperialist Writings on the Philippine-American War,* edited by Jim Zwick, 376–77. Syracuse, NY: Syracuse University Press.

Twitchell Jr., Heath. 1974. *Allen: The Biography of an Army Officer, 1859–1930.* New Brunswick, NJ: Rutgers University Press.

U.S. Air Force. 2005. *The U.S. Air Force Remotely Piloted Aircraft and Unmanned Aerial Vehicle Strategic Vision.* Accessed June 2, 2014. http://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1000&context=usafresearch

U.S. Bureau of the Census. 1904. *Abstract of the Twelfth Census of the United States, 1900.* Washington, DC: Government Printing Office.

U.S. Department of Defense. 2012. *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense.* Washington, DC: U.S. Department of Defense. Accessed June 2, 2014. http://www.defense.gov/news/Defense_Strategic_Guidance.pdf

U.S. Senate. 1976a. Select Committee to Study Governmental Operations with Respect to Intelligence Activities, 94th Congress, 2d Session. *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, Book 2. Washington, DC: Government Printing Office.

U.S. Senate. 1976 b. Select Committee to Study Governmental Operations with Respect to Intelligence Activities, 94th Congress, 2d Session. *Supplementary Reports on Intelligence Activities,* Book 6. Washington, DC: Government Printing Office.

Van Deman, R. H. 1901. For the information of the Division Commander, December 9. Philippine Insurgent Records, Special Documents, Publication 254, Microreel 80, Folder 1303, NARA.

Van Deman, R. H. 1928. Office of Chief of Staff, Cross Reference Card, December 15. Microform 1194, RG 350, NARA.

Walker, William O. III. 2009. *National Security and Core Values in American History*. New York: Cambridge University Press.

Wagner, Arthur L. 1902. In U.S. Senate, 57th Congress, 1st Session, doc. no. 331, part 3, *Affairs in the Philippine Islands: Hearings before the Committee on the Philippines of the United States Senate.* Washington, DC: Government Printing Office.

Washington Evening Star. 1940. February 20. Personal Name Information Files: John R. White, Entry 21, RG 350, NARA.

Weber, Ralph E. ed. 1988. *The Final Memoranda: Major General Ralph H. Van Deman, USA Ret., 1865–1952, Father of U.S. Military Intelligence.* Wilmington, DE: Scholarly Resources.

Weeden, Brian. 2010. "X-37B Orbital Test Vehicle Fact Sheet." *Secure World Foundation.* Accessed June 2, 2014. http://swfound.org/media/1791/swf_x-37b_otv_fact_sheet_updated_2012.pdf

Weiner, Tim. 2002. "Look Who's Listening." *New York Times*, January 20.

Weiner, Tim. 2007. *Legacy of Ashes: The History of the CIA*. New York: Penguin.

Weiner, Tim. 2013. *Enemies: A History of the FBI.* New York: Random House.

Weisbrot, Mark. 2011. "2016 When China Overtakes the US." *The Guardian,* April 27. Accessed June 2, 2014. http://www.guardian.co.uk/commentisfree/cifamerica/2011/apr/27/china-imf-economy-2016

Werner, William. 1974. *History of the Boston Fire Department and Boston Fire Alarm System.* Boston: Boston Sparks Association.

Wicker, Tom. 1976. "Is Oversight Enough?" *New York Times,* May 14.

Wiegand, Wayne A. 1996. *Irrepressible Reformer: A Biography of Melvil Dewey.* Chicago: American Library Association.

Wiegand, Wayne A. and Donald G. Davis, Jr. 1994. *Encyclopedia of Library History.* New York: Routledge.

Wines, F. H. 1900. "The Census of 1900." *National Geographic,* January.

Winks, Robin W. 1987. *Cloak and Gown 1939–1961: Scholars in the Secret War.* New York: Morrow.

Wood, Leonard. 1923. "Diaries, 1921–27," August 15. Leonard Wood Papers, Manuscript Division, U.S. Library of Congress.

Wright, Jr., Robert. 1992. *Army Lineage Series: Military Police.* Washington, DC: Government Printing Office.

Wyden, Ron. 2013. "Wyden, Udall Statement on the Disclosure of Bulk Email Records Collection Program." *Ron Wyden, Senator for Oregon,* July 2. Accessed June 2, 2014. http://www.wyden.senate.gov/news/press-releases/wyden-udall-statement-on-the-disclosure-of-bulk-email-records-collection-program