By Alfred W. McCoy

From TomDispatch.com | Original Article

Surveillance Blowback
The Making of the U.S. Surveillance State, 1898-2020

The American surveillance state is now an omnipresent reality, but its deep history is little known and its future little grasped. Edward Snowden's leaked documents reveal that, in a post-9/11 state of war, the National Security Agency (NSA) was able to create a surveillance system that could secretly monitor the private communications of almost every American in the name of fighting foreign terrorists. The technology used is state of the art; the impulse, it turns out, is nothing new. For well over a century, what might be called "surveillance blowback" from America's wars has ensured the creation of an ever more massive and omnipresent internal security and surveillance apparatus. Its future (though not ours) looks bright indeed.

In 1898, Washington occupied the Philippines and in the years that followed pacified its rebellious people, in part by fashioning the world's first full-scale "surveillance state" in a colonial land. The illiberal lessons learned there then migrated homeward, providing the basis for constructing America's earliest internal security and surveillance apparatus during World War I. A half-century later, as protests mounted during the Vietnam War, the FBI, building on the foundations of that old security structure, launched large-scale illegal counterintelligence operations to harass antiwar activists, while President Richard Nixon's White House created its own surveillance apparatus to target its domestic enemies.

In the aftermath of those wars, however, reformers pushed back against secret surveillance. Republican privacy advocates abolished much of President Woodrow Wilson's security apparatus during the 1920s, and Democratic liberals in Congress created the FISA courts in

the 1970s in an attempt to prevent any recurrence of President Nixon's illegal domestic wiretapping.

Today, as Washington withdraws troops from the Greater Middle East, a sophisticated intelligence apparatus built for the pacification of Afghanistan and Iraq has come home to help create a twenty-first century surveillance state of unprecedented scope. But the past pattern that once checked the rise of a U.S. surveillance state seems to be breaking down. Despite talk about ending the war on terror one day, President Obama has left the historic pattern of partisan reforms far behind. In what has become a permanent state of "wartime" at home, the Obama administration is building upon the surveillance systems created in the Bush years to maintain U.S. global dominion in peace or war through a strategic, ever-widening edge in information control. The White House shows no sign -- nor does Congress -- of cutting back on construction of a powerful, global Panopticon that can surveil domestic dissidents, track terrorists, manipulate allied nations, monitor rival powers, counter hostile cyber strikes, launch preemptive cyberattacks, and protect domestic communications.

Writing for TomDispatch four years ago during Obama's first months in office, I suggested that the War on Terror has "proven remarkably effective in building a technological template that could be just a few tweaks away from creating a domestic surveillance state -- with omnipresent cameras, deep data-mining, nano-second biometric identification, and drone aircraft patrolling 'the homeland.'"

That prediction has become our present reality -- and with stunning speed. Americans now live under the Argus-eyed gaze of a digital surveillance state, while increasing numbers of surveillance drones fill American skies. In addition, the NSA's net now reaches far beyond our borders, sweeping up the personal messages of many millions of people worldwide and penetrating the confidential official communications of at least 30 allied nations. The past has indeed proven prologue. The future is now.

The Coming of the Information Revolution

The origins of this emerging global surveillance state date back over a century to "America's first information revolution" for the management of textual, statistical, and analytical data -- a set of innovations whose synergy created the technological capacity for mass surveillance.

Here's a little litany of "progress" to ponder while on the road to today's every-email-all-the-time version of surveillance.

Within just a few years, the union of Thomas A. Edison's quadruplex telegraph with Philo Remington's commercial typewriter, both inventions of 1874, allowed for the accurate transmission of textual data at the unequalled speed of 40 words per minute across America and around the world.

In the mid-1870s as well, librarian Melvil Dewey developed the "Dewey decimal system" to catalog the Amherst College Library, thereby inventing the "smart number" for the reliable encoding and rapid retrieval of limitless information.

The year after engineer Herman Hollerith patented the punch card (1889), the U.S. Census Bureau adopted his Electrical Tabulating machine to count 62,622,250 Americans within weeks -- a triumph that later led to the founding of International Business Machines, better known by its acronym IBM.

By 1900, all American cities were wired via the Gamewell Corporation's innovative telegraphic communications, with over 900 municipal police and fire systems sending 41 million messages in a single year.

A Colonial Laboratory for the Surveillance State

On the eve of empire in 1898, however, the U.S. government was still what scholar Stephen Skowronek has termed a "patchwork" state with a near-zero capacity for domestic security. That, of course, left ample room for the surveillance version of modernization, and it came with surprising speed after Washington conquered and colonized the Philippines.

Facing a decade of determined Filipino resistance, the U.S. Army applied all those American information innovations -- rapid telegraphy, photographic files, alpha-numeric coding, and Gamewell police communications -- to the creation of a formidable, three-tier colonial security apparatus including the Manila Police, the Philippines Constabulary, and above all the Army's

Division of Military Information.

In early 1901, Captain Ralph Van Deman, later dubbed “the father of U.S. Military Intelligence,” assumed command of this still embryonic division, the Army’s first field intelligence unit in its 100-year history. With a voracious appetite for raw data, Van Deman’s division compiled phenomenally detailed information on thousands of Filipino leaders, including their physical appearance, personal finances, landed property, political loyalties, and kinship networks.

Starting in 1901, the first U.S. governor-general (and future president) William Howard Taft drafted draconian sedition legislation for the islands and established a 5,000-man strong Philippines Constabulary. In the process, he created a colonial surveillance state that ruled, in part, thanks to the agile control of information, releasing damning data about enemies while suppressing scandals about allies.

When the Associated Press’s Manila bureau chief reported critically on these policies, Taft’s allies dug up dirt on this would-be critic and dished it out to the New York press. On the other hand, the Division of Military Information compiled a scandalous report about the rising Filipino politician Manuel Quezon, alleging a premarital abortion by his future first lady. Quezon, however, served the Constabulary as a spy, so this document remained buried in U.S. files, assuring his unchecked ascent to become the first president of the Philippines in 1935.

American Blueprint

During the U.S. conquest of the Philippines, Mark Twain wrote an imagined history of twentieth-century America. In it, he predicted that a “lust for conquest” had already 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.” Indeed, just a decade after Twain wrote those prophetic words, colonial police methods came home to serve as a template for the creation of an American internal security apparatus in wartime.

After the U.S. entered World War I in 1917 without an intelligence service of any sort, Colonel Van Deman brought his Philippine experience to bear, creating the U.S. Army’s Military Intelligence Division (MID) and so laying the institutional foundations for a future internal security state.

In collaboration with the FBI, he also expanded the MID's reach through a civilian auxiliary organization, the American Protective League, whose 350,000 citizen-operatives amassed more than a million pages of surveillance reports on German-Americans in just 14 months, arguably the world's most intensive feat of domestic surveillance ever.

After the Armistice in 1918, Military Intelligence joined the FBI in two years of violent repression of the American left marked by the notorious Luster raids in New York City, J. Edgar Hoover's "Palmer Raids" in cities across the northeast and the suppression of union strikes from New York City to Seattle.

When President Wilson left office in 1921, incoming Republican privacy advocates condemned his internal security regime as intrusive and abusive, forcing the Army and the FBI to cut their ties to patriotic vigilantes. In 1924, Attorney General Harlan Fiske Stone, worrying 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." Epitomizing the nation's retreat from surveillance, Secretary of War Henry Stimson closed the Military Intelligence cipher section in 1929, saying famously, "Gentlemen do not read each other's mail."

After retiring at the rank of major general that same year, Van Deman and his wife continued from their home in San Diego to coordinate an informal intelligence exchange system, compiling files on 250,000 suspected "subversives." They also took reports from classified government files and slipped them to citizen anti-communist groups for blacklisting. In the 1950 elections, for instance, Representative Richard Nixon reportedly used Van Deman's files to circulate "pink sheets" at rallies denouncing California Congresswoman Helen Gahagan Douglas, his opponent in a campaign for a Senate seat, launching a victorious Nixon on the path to the presidency.

From retirement, Van Deman, in league with FBI Director J. Edgar Hoover, also proved crucial at a 1940 closed-door conference that awarded the FBI control over domestic counterintelligence. The Army's Military Intelligence, and its successors, the CIA and NSA, were restricted to foreign espionage, a division of tasks that would hold, at least in principle, until the post-9/11 years. So armed, during World War II the FBI used warrantless wiretaps, "black bag" break-ins, and surreptitious mail opening to track suspects, while mobilizing more than 300,000 informers to secure defense plants against wartime threats that ultimately proved "negligible."

The Vietnam Years

In response to the civil rights and anti-Vietnam protests of the 1960s, the FBI deployed its COINTELPRO operation, using what Senator Frank Church's famous investigative committee later called "unsavory and vicious tactics... including anonymous attempts to break up marriages, disrupt meetings, ostracize persons from their professions, and provoke target groups into rivalries that might result in deaths."

In assessing COINTELPRO's 2,370 actions from 1960 to 1974, the Church Committee branded them a "sophisticated vigilante operation" that "would be intolerable in a democratic society even if all of the targets had been involved in violent activity." Significantly, even this aggressive Senate investigation did not probe Director Hoover's notorious "private files" on the peccadilloes of leading politicians that had insulated his Bureau from any oversight for more than 30 years.

After *New York Times* reporter Seymour Hersh exposed illegal CIA surveillance of American antiwar activists in 1974, Senator Church's committee and a presidential commission under Nelson Rockefeller investigated the Agency's "Operation Chaos," a program to conduct massive illegal surveillance of the antiwar protest movement, discovering a database with 300,000 names. These investigations also exposed the excesses of the FBI's COINTELPRO, forcing the Bureau to reform.

To prevent future abuses, President Jimmy Carter signed the Foreign Intelligence Surveillance Act (FISA) in 1978, creating a special court to approve all national security wiretaps. In a bitter irony, Carter's supposed reform ended up plunging the judiciary into the secret world of the surveillance managers where, after 9/11, it became a rubberstamp institution for every kind of state intrusion on domestic privacy.

How the Global War on Terror Came Home

As its pacification wars in Afghanistan and Iraq sank into bloody quagmires, Washington brought electronic surveillance, biometric identification, and unmanned aerial vehicles to the

battlefields. This trio, which failed to decisively turn the tide in those lands, nonetheless now undergirds a global U.S. surveillance apparatus of unequalled scope and unprecedented power.

After confining the populations of Baghdad and the rebellious Sunni city of Falluja behind blast-wall cordons, the U.S. Army attempted to bring the Iraqi resistance under control in part by collecting , as of 2011, three million Iraqi fingerprints,iris, and retinal scans. These were de posited
in a biometric database in West Virginia that American soldiers at checkpoints and elsewhere on distant battlefields could at any moment access by satellite link. Simultaneously, the Joint Special Operations Command under General Stanley McChrystal
centralized
all electronic and satellite surveillance in the Greater Middle East to identify possible al-Qaeda operatives for
assassination
by Predator drones or hunter-killer raids by Special Operations commandos from Somalia to Pakistan.

Domestically, post-9/11, the White House tried to create a modern version of the old state-citizen alliance for domestic surveillance. In May 2002, President Bush's Justice Department launched Operation TIPS with "millions of American truckers, letter carriers, train conductors, ship captains, utility employees, and others" spying on fellow citizens. But there was vocal opposition from members of Congress, civil libertarians, and the media, which soon forced Justice to quietly kill the program.

In a digital iteration of the same effort, retired admiral John Poindexter began to set up an ominously titled Pentagon program called Total Information Awareness to amass a "detailed electronic dossier on millions of Americans." Again the nation recoiled, Congress banned the program, and the admiral was forced to resign.

Defeated in the public arena, the Bush administration retreated into the shadows, where it launched secret FBI and NSA domestic surveillance programs. Here, Congress proved far more amenable and pliable. In 2002, Congress erased the bright line that had long barred the CIA from domestic spying, granting the agency the power to access U.S. financial records and audit electronic communications routed through the country.

Defying the FISA law, in October 2001 President Bush ordered the NSA to commence covert monitoring of private communications through the nation's telephone companies without the requisite warrants. According to the Associated Press, he also "secretly authorized the NSA to plug into the fiber optic cables that enter and leave the United States" carrying the world's "emails, telephone calls, video chats, websites, bank transactions, and more." Since his administration had already conveniently decided that "metadata was not constitutionally protected," the NSA began an open-ended program, Operation Stellar Wind, "to collect bulk telephony and Internet metadata."

By 2004, the Bush White House was so wedded to Internet metadata collection that top aides barged into Attorney General John Ashcroft's hospital room to extract a reauthorization signature for the program. They were blocked by Justice Department officials led by Deputy Attorney General James Comey, forcing a two-month suspension until that FISA court, brought into existence in the Carter years, put its first rubber-stamp on this mass surveillance regime.

Armed with expansive FISA court orders allowing the collection of data sets rather than information from specific targets, the FBI's " Investigative Data Warehouse " acquired more than a billion documents within five years, including intelligence reports, social security files, drivers' licenses, and private financial information. All of this was accessible to 13,000 analysts making a million queries monthly. In 2006, as the flood of data surging through fiber optic cables strained NSA computers, the Bush administration launched the Intelligence Advanced Research Projects Activity to develop supercomputing searches powerful enough to process this torrent of Internet information.

In 2005, a *New York Times* investigative report exposed the administration's illegal surveillance for the first time. A year later, *USA Today* reported that 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 was "to create a database of every call ever made."

In August 2007, in response to these revelations, Congress capitulated. It passed a new law,

the Protect America Act, which retrospectively legalized this illegal White House-inspired set of programs by requiring greater oversight by the FISA court. This secret tribunal -- acting almost as a " parallel Supreme Court " that rules on fundamental constitutional rights without adversarial proceedings or higher review -- has removed any real restraint on the National Security Agency's bulk collection of Internet metadata and regularly rubberstamps almost 100% of the government's thousands of surveillance requests. Armed with expanded powers, the National Security Agency promptly launched its PRISM program (recently revealed by Edward Snowden). To feed its hungry search engines, the NSA has compelled nine Internet giants, including Microsoft, Yahoo, Google, Facebook, AOL, and Skype, to transfer what became billions of emails to its massive data farms.

Obama's Expanding Surveillance Universe

Instead of curtailing his predecessor's wartime surveillance, as Republicans did in the 1920s and Democrats in the 1970s, President Obama has overseen the expansion of the NSA's wartime digital operations into a permanent weapon for the exercise of U.S. global power.

The Obama administration continued a Bush-era NSA program of "bulk email records collection" until 2011 when two senators protested that the agency's "statements to both Congress and the Court... significantly exaggerated this program's effectiveness." Eventually, the administration was forced to curtail this particular operation. Nonetheless, the NSA has continued to collect the personal communications of Americans by the billions under its PRISM and other programs.

In the Obama years as well, the NSA began cooperating with its long-time British counterpart, the Government Communications Headquarters (GCHQ), to tap into the dense cluster of Trans-Atlantic Telecommunication fiber optic cables that transit the United Kingdom. During a visit to a GCHQ facility for high-altitude intercepts at Menwith Hill in June 2008, NSA Director General Keith Alexander asked, "Why can't we collect all the signals all the time? Sounds like a good summer project for Menwith."

In the process, GCHQ's Operation Tempora achieved the "biggest Internet access" of any partner in a "Five Eyes" signals-intercept coalition that, in addition to Great Britain and the U.S., includes Australia, Canada, and New Zealand. When the project went online in 2011, the GCHQ sank probes into 200 Internet cables and was soon collecting 600 million telephone messages daily, which were, in turn, made accessible to 850,000 NSA employees.

The historic alliance between the NSA and GCHQ dates back to the dawn of the Cold War. In deference to it, the NSA has, since 2007, exempted its "2nd party" Five Eyes allies from surveillance under its "Boundless Informant" operation. According to another recently leaked NSA document, however, "we can, and often do, target the signals of most 3rd party foreign partners." This is clearly a reference to close allies like Germany, France, and Italy.

On a busy day in January 2013, for instance, the NSA collected 60 million phone calls and emails from Germany -- some 500 million German messages are reportedly collected annually -- with lesser but still hefty numbers from France, Italy, and non-European allies like Brazil. To gain operational intelligence on such allies, the NSA taps phones at the European Council headquarters in Brussels, bugs the European Union (EU) delegation at the U.N., has planted a "Dropmire" monitor "on the Cryptofax at the EU embassy DC," and eavesdrops on 38 allied embassies worldwide.

Such secret intelligence about its allies gives Washington an immense diplomatic advantage, says 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." And who knows what scurrilous bits of scandal about world leaders American surveillance systems might scoop up to strengthen Washington's hand in that global poker game called diplomacy.

This sort of digital surveillance was soon supplemented by actual Internet warfare. Between 2006 and 2010, Washington launched the planet's first cyberwar , with Obama ordering devastating cyberattacks against Iran's nuclear facilities. In 2009, the Pentagon formed the U.S. Cyber Command (CYBERCOM), with a cybercombat center at Lackland Air Base initially staffed by 7,000 Air Force employees. Over the next two years, by

appointing
NSA chief Alexander as CYBERCOM's concurrent commander, it created an enormous concentration of power in the digital shadows. The Pentagon has also
declared
cyberspace an "operational domain" for both offensive and defensive warfare.

Controlling the Future

By leaking a handful of NSA documents, Edward Snowden has given us a glimpse of future U.S. global policy and the changing architecture of power on this planet. At the broadest level, this digital shift complements Obama's new defense strategy, announced in 2012, of reducing
costs
(cutting, for example, infantry troops by 14%), while conserving Washington's overall power by developing a
capacity
for "a combined arms campaign across all domains -- land, air, maritime, space, and cyberspace."

While cutting conventional armaments, Obama is investing billions in constructing a new architecture for global information control. To store and process the billions of messages sucked up by its worldwide surveillance network (totaling 97 billion items for March alone), the NSA is employing 11,000 workers
to build a $1.6 billion data center in Bluffdale, Utah, whose
storage capacity
is measured in "yottabytes," each the equivalent of a trillion terabytes. That's almost unimaginable once you realize that just 15 terabytes could store every publication in the Library of Congress.

From its new $1.8 billion headquarters, the third-biggest building in the Washington area, the National Geospatial-Intelligence Agency deploys 16,000 employees and a $5 billion budget to coordinate a rising torrent of surveillance data from Predators, Reapers, U-2 spy planes, Global Hawks, X-37B space drones, Google Earth, Space Surveillance Telescopes, and orbiting satellites.

To protect those critical orbiting satellites, which transmit most U.S. military communications, the Pentagon is building an aerospace shield of pilotless drones. In the exosphere, the Air

Force has since April 2010 been successfully testing the X-37B space drone that can carry missiles to strike rival satellite networks such as the one the Chinese are currently creating.

For more extensive and precise surveillance from space, the Pentagon has been replacing its costly, school-bus-sized spy satellites with a new generation of light, low cost models such as the ATK-A200. Successfully launched in May 2011, this module is orbiting 250 miles above the Earth with remote-controlled, U-2 quality cameras that now provide the "U.S. Central Command an assured ISR (Intelligence, Surveillance, and Reconnaissance) capability."

In the stratosphere, close enough to Earth for audiovisual surveillance, the Pentagon is planning to launch an armada of 99 Global Hawk drones -- each equipped with high-resolution cameras to surveil all terrain within a 100-mile radius, electronic sensors to intercept communications, and efficient engines for continuous 24-hour flight.

Within a decade, the U.S. will likely deploy this aerospace shield, advanced cyberwarfare capabilities, and even vaster, more omnipresent digital surveillance networks that will envelop the Earth in an electronic grid capable of blinding entire armies on the battlefield, atomizing a single suspected terrorist, or monitoring millions of private lives at home and abroad.

Sadly, Mark Twain was right when he warned us just over 100 years ago that America could not have both empire abroad and democracy at home. To paraphrase his prescient words, by "trampling upon the helpless abroad" with unchecked surveillance, Americans have learned, "by a natural process, to endure with apathy the like at home."

Alfred W. McCoy is the J.R.W. Smail Professor of History at the University of Wisconsin-Madison. A TomDispatch regular , he is the author Policing America's Empire: The United States, the Philippines, and the Rise of the Surveillance State *(University of Wisconsin), which is the source for much of the material in this essay.*