GlobalResearch
Center for Research on Globalization

Welcome Home, War! Creating the "Domestic Surveillance State"

How America's Wars Are Systematically Destroying Our Liberties

By Prof Alfred McCoy
Global Research, November 16, 2009
Tom Dispatch 12 November 2009

Region: USA
Theme: Police State & Civil Rights, US NATO War Agenda

In his approach to National Security Agency surveillance, as well as CIA renditions, drone assassinations, and military detention, President Obama has to a surprising extent embraced the expanded executive powers championed by his conservative predecessor, George W. Bush. This bipartisan affirmation of the imperial executive could "reverberate for generations," warns Jack Balkin, a specialist on First Amendment freedoms at Yale Law School. And consider these but some of the early fruits from the hybrid seeds that the Global War on Terror has planted on American soil. Yet surprisingly few Americans seem aware of the toll that this already endless war has taken on our civil liberties.

Don't be too surprised, then, when, in the midst of some future crisis, advanced surveillance methods and other techniques developed in our recent counterinsurgency wars migrate from Baghdad, Falluja, and Kandahar to your hometown or urban neighborhood. And don't ever claim that nobody told you this could happen — at least not if you care to read on.

Think of our counterinsurgency wars abroad as so many living laboratories for the undermining of a democratic society at home, a process historians of such American wars can tell you has been going on for a long, long time. Counterintelligence innovations like centralized data, covert penetration, and disinformation developed during the Army's first protracted pacification campaignin a foreign land — the Philippines from 1898 to 1913 — were repatriated to the United States during World War I, becoming the blueprint for an invasive internal security apparatus that persisted for the next half century.

Almost 90 years later, George W. Bush's Global War on Terror plunged the U.S. military into four simultaneous counterinsurgency campaigns, large and small — in Somalia, Iraq, Afghanistan, and (once again) the Philippines — transforming a vast swath of the planet into an *ad hoc*"counterterrorism" laboratory. The result? Cutting-edge high-tech security and counterterror techniques that are now slowly migrating homeward.

As the War on Terror enters its ninth year to become one of America's longest overseas conflicts, the time has come to ask an uncomfortable question: What impact have the wars in Afghanistan and Iraq — and the atmosphere they created domestically — had on the quality of our democracy?

Every American knows that we are supposedly fighting elsewhere to defend democracy here at home. Yet the crusade for democracy abroad, largely unsuccessful in its own right, 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."

Even if its name is increasingly anathema in Washington, the ongoing Global War on Terror has helped bring about a massive expansion of domestic surveillance by the FBI and the National Security Agency (NSA) whose combined data-mining systems have already swept up several billion private documents from U.S. citizens into classified data banks. Abroad, after years of failing counterinsurgency efforts in the Middle East, the Pentagon began applying biometrics — the science of identification via facial shape, fingerprints, and retinal or iris patterns — to the pacification of Iraqi cities, as well as the use of electronic intercepts for instant intelligence and the split-second application of satellite imagery to aid an assassination campaign by drone aircraft that reaches from Africa to South Asia.

In the panicky aftermath of some future terrorist attack, Washington could quickly fuse existing foreign and domestic surveillance techniques, as well as others now being developed on distant battlefields, to create an instant digital surveillance state.

The Crucible of Counterinsurgency

For the past six years, confronting a bloody insurgency, the U.S. occupation of Iraq has served as a white-hot crucible of counterinsurgency, forging a new system of biometric surveillance and digital warfare with potentially disturbing domestic implications. This new biometric identification system first appeared in the smoking aftermath of "Operation Phantom Fury," a brutal, nine-day battle that U.S. Marines fought in late 2004 to recapture the insurgent-controlled city of Falluja. Bombing, artillery, and mortars destroyed at least half of that city's buildings and sent most of its 250,000 residents fleeing into the surrounding countryside. Marines then forced returning residents to wait endless hours under a desert sun at checkpoints for fingerprints and iris scans. Once inside the city's blast-wall maze, residents had to wear identification tags for compulsory checks to catch infiltrating insurgents.

The first hint that biometrics were helping to pacify Baghdad's far larger population of seven million came in April 2007 when the *New York Times* published an eerie image of American soldiers studiously photographing an Iraqi's eyeball. With only a terse caption to go by, we can still infer the technology behind this single record of a retinal scan in Baghdad: digital cameras for U.S. patrols, wireless data transfer to a mainframe computer, and a database to record as many adult Iraqi eyes as could be gathered. Indeed, eight months later, the *Washington Post* reported that the Pentagon had collected over a million Iraqi fingerprints and iris scans. By mid-2008, the U.S. Army had also confined Baghdad's population behind blast-wall cordons and was checking Iraqi identities by satellite link to a biometric database.

Pushing ever closer to the boundaries of what present-day technology can do, by early 2008, U.S. forces were also collecting facial images accessible by portable data labs called Joint Expeditionary Forensic Facilities, linked by satellite to a biometric database in West Virginia. "A war fighter needs to know one of three things," explained the inventor of this lab-in-a-box. "Do I let him go? Keep him? Or shoot him on the spot?"

A future is already imaginable in which a U.S. sniper could take a bead on the eyeball of a suspected terrorist, pause for a nanosecond to transmit the target's iris or retinal data via

backpack-sized laboratory to a computer in West Virginia, and then, after instantaneous feedback, pull the trigger.

Lest such developments seem fanciful, recall that *Washington Post* reporter Bob Woodward claims the success of George W. Bush's 2007 troop surge in Iraq was due less to boots on the ground than to bullets in the head — and these, in turn, were due to a top-secret fusion of electronic intercepts and satellite imagery. Starting in May 2006, American intelligence agencieslaunched a Special Action Program using "the most highly classified techniques and information in the U.S. government" in a successful effort "to locate, target and kill key individuals in extremist groups such as al-Qaeda, the Sunni insurgency and renegade Shia militias."

Under General Stanley McChrystal, now U.S. Afghan War commander, the Joint Special Operations Command (JSOC) deployed "every tool available simultaneously, from signals intercepts to human intelligence" for "lightning quick" strikes. One intelligence officer reportedly claimed that the program was so effective it gave him "orgasms." President Bush called it "awesome." Although refusing to divulge details, Woodward himself compared it to the Manhattan Project in World War II. This Iraq-based assassination program relied on the authority Defense Secretary Donald Rumsfeld granted JSOC in early 2004 to "kill or capture al-Qaeda terrorists" in 20 countries across the Middle East, producing dozens of lethal strikes by airborne Special Operations forces.

Another crucial technological development in Washington's secret war of assassination has been the armed drone, or unmanned aerial vehicle, whose speedy development has been another by-product of Washington's global counterterrorism laboratory. Half a world away from Iraq in the southern Philippines, the CIA and U.S. Special Operations Forces conducted an early experiment in the use of aerial surveillance for assassination. In June 2002, with a specially-equipped CIA aircraft circling overhead offering real-time video surveillance in the pitch dark of a tropical night, Philippine Marines executed a deadly high-seas ambush of Muslim terrorist Aldam Tilao (a.k.a. "Abu Sabaya").

In July 2008, the Pentagon proposed an expenditure of $1.2 billion for a fleet of 50 light aircraft loaded with advanced electronics to loiter over battlefields in Afghanistan and Iraq, bringing "full motion video and electronic eavesdropping to the troops." By late 2008, night flights over Afghanistan from the deck of the USS *Theodore Roosevelt* were using sensors to give American ground forces real-time images of Taliban targets — some so focused that they could catch just a few warm bodies huddled in darkness behind a wall.

In the first months of Barack Obama's presidency, CIA Predator drone strikes have escalated in the Pakistani tribal borderlands with a macabre efficiency, using a top-secret mix of electronic intercepts, satellite transmission, and digital imaging to kill half of the Agency's 20 top-priority al-Qaeda targets in the region. Just three days before Obama visited Canada last February, Homeland Security launched its first Predator-B drones to patrol the vast, empty North Dakota-Manitoba borderlands that one U.S. senator has called America's "weakest link."

Homeland Security

While those running U.S. combat operations overseas were experimenting with intercepts, satellites, drones, and biometrics, inside Washington the plodding civil servants of internal

security at the FBI and the NSA initially began expanding domestic surveillance through thoroughly conventional data sweeps, legal and extra-legal, and — with White House help — several abortive attempts to revive a tradition that dates back to World War I of citizens spying on suspected subversives.

"If people see anything suspicious, utility workers, you ought to report it," said President George Bush in his April 2002 call for nationwide citizen vigilance. Within weeks, his Justice Department had launched Operation TIPS (Terrorism Information and Prevention System), with plans for "millions of American truckers, letter carriers, train conductors, ship captains, utility employees and others" to aid the government by spying on their fellow Americans. Such citizen surveillancesparked strong protests, however, forcing the Justice Department to quietly bury the president's program.

Simultaneously, inside the Pentagon, Admiral John Poindexter, President Ronald Reagan's former national security advisor (swept up in the Iran-Contra scandal of that era), was developing a Total Information Awareness program which was to contain "detailed electronic dossiers" on millions of Americans. When news leaked about this secret Pentagon office with its eerie, all-seeing eye logo, Congress banned the program, and the admiral resigned in 2003. But the key data extraction technology, the Information Awareness Prototype System, migrated quietly to the NSA.

Soon enough, however, the CIA, FBI, and NSA turned to monitoring citizens electronically without the need for human tipsters, rendering the administration's grudging retreats from conventional surveillance at best an ambiguous political victory for civil liberties advocates. Sometime in 2002, President Bushgave the NSA secret, illegal orders to monitor private communications through the nation's telephone companies and its private financial transactions through SWIFT, an international bank clearinghouse.

After the *New York Times* exposed these wiretaps in 2005, Congress quickly capitulated, first legalizing this illegal executive program and then granting cooperating phone companies immunity from civil suits. Such intelligence excess was, however, intentional. Even after Congress widened the legal parameters for future intercepts in 2008, the NSA continued to push the boundaries of its activities, engaging in what the *New York Times* politely termed the systematic "overcollection" of electronic communications among American citizens. Now, for example, thanks to a top-secret NSA database called "Pinwale," analysts routinely scan countless "millions" of domestic electronic communications without much regard for whether they came from foreign or domestic sources.

Starting in 2004, the FBI launched an Investigative Data Warehouse as a "centralized repository for… counterterrorism." Within two years, it contained 659 million individual records. This digital archive of intelligence, social security files, drivers' licenses, and records of private finances could be accessed by 13,000 Bureau agents and analysts making a million queries monthly. By 2009, when digital rights advocates sued for full disclosure, the database had already grown to over a billion documents.

And did this sacrifice of civil liberties make the United States a safer place? In July 2009, after a careful review of the electronic surveillance in these years, the inspectors general of the Defense Department, the Justice Department, the CIA, the NSA, and the Office of National Intelligenceissued a report sharply critical of these secret efforts. Despite George W. Bush's claims that massive electronic surveillance had "helped prevent attacks," these auditors could not find any "specific instances" of this, concluding such surveillance had

“generally played a limited role in the F.B.I.’s overall counterterrorism efforts.”

Amid the pressures of a generational global war, Congress proved all too ready to offer up civil liberties as a bipartisan burnt offering on the altar of national security. In April 2007, for instance, in a bid to legalize the Bush administration’s warrantless wiretaps, Congressional representative Jane Harman (Dem., California) offered a particularly extreme example of this urge. Sheintroduced the Violent Radicalization and Homegrown Terrorism Prevention Act, proposing a powerful national commission, functionally a standing “star chamber,” to “combat the threat posed by homegrown terrorists based and operating within the United States.” The bill passed the House by an overwhelming 404 to 6 vote before stalling, and then dying, in a Senate somewhat more mindful of civil liberties.

Only weeks after Barack Obama entered the Oval Office, Harman’s life itself became a cautionary tale about expanding electronic surveillance. According to information leaked to the*Congressional Quarterly*, in early 2005 an NSA wiretap caught Harman offering to press the Bush Justice Department for reduced charges against two pro-Israel lobbyists accused of espionage. In exchange, an Israeli agent offered to help Harman gain the chairmanship of the House Intelligence Committee by threatening House Democratic majority leader Nancy Pelosi with the loss of a major campaign donor. As Harman put down the phone, she said, “This conversation doesn’t exist.”

How wrong she was. An NSA transcript of Harman’s every word soon crossed the desk of CIA Director Porter Goss, prompting an FBI investigation that, in turn, was blocked by then-White House Counsel Alberto Gonzales. As it happened, the White House knew that the *New York Times* was about to publish its sensational revelation of the NSA’s warrantless wiretaps, and felt it desperately needed Harman for damage control among her fellow Democrats. In this commingling of intrigue and irony, an influential legislator’s defense of the NSA’s illegal wiretapping exempted her from prosecution for a security breach discovered by an NSA wiretap.

Since the arrival of Barack Obama in the White House, the auto-pilot expansion of digital domestic surveillance has in no way been interfered with. As a result, for example, the FBI’s “Terrorist Watchlist,” with 400,000 names and a million entries, continues to grow at the rate of 1,600 new names daily.

In fact, the Obama administration has even announced plans for a new military cybercommandstaffed by 7,000 Air Force employees at Lackland Air Base in Texas. This command will be tasked with attacking enemy computers and repelling hostile cyber-attacks or counterattacks aimed at U.S. computer networks — with scant respect for what the Pentagon calls “sovereignty in the cyberdomain.” Despite the president’s assurances that operations “will not — I repeat — will not include monitoring private sector networks or Internet traffic,” the Pentagon’s top cyberwarrior, General James E. Cartwright, has conceded such intrusions are inevitable.

Sending the Future Home

While U.S. combat forces prepare to draw-down in Iraq (and ramp up in Afghanistan), military intelligence units are coming home to apply their combat-tempered surveillance skills to our expanding homeland security state, while preparing to counter any future domestic civil disturbances here.

Indeed, in September 2008, the Army's Northern Command announced that one of the Third Division's brigades in Iraq would be reassigned as a Consequence Management Response Force (CMRF) inside the U.S. Its new mission: planning for moments when civilian authorities may need help with "civil unrest and crowd control." According to Colonel Roger Cloutier, his unit's civil-control equipment featured "a new modular package of non-lethal capabilities" designed to subdue unruly or dangerous individuals — including Taser guns, roadblocks, shields, batons, and beanbag bullets.

That same month, Army Chief of Staff General George Casey flew to Fort Stewart, Georgia, for the first full CMRF mission readiness exercise. There, he strode across a giant urban battle map filling a gymnasium floor like a conquering Gulliver looming over Lilliputian Americans. With 250 officers from all services participating, the military war-gamed its future coordination with the FBI, the Federal Emergency Management Agency, and local authorities in the event of a domestic terrorist attack or threat. Within weeks, the American Civil Liberties Union filed an expedited freedom of information request for details of these deployments, arguing: "[It] is imperative that the American people know the truth about this new and unprecedented intrusion of the military in domestic affairs."

At the outset of the Global War on Terror in 2001, memories of early Cold War anti-communist witch-hunts blocked Bush administration plans to create a corps of civilian tipsters and potential vigilantes. However, far more sophisticated security methods, developed for counterinsurgency warfare overseas, are now coming home to far less public resistance. They promise, sooner or later, to further jeopardize the constitutional freedoms of Americans.

In these same years, under the pressure of War on Terror rhetoric, presidential power has grown relentlessly, opening the way to unchecked electronic surveillance, the endless detention of terror suspects, and a variety of inhumane forms of interrogation. Somewhat more slowly, innovative techniques of biometric identification, aerial surveillance, and civil control are now being repatriated as well.

In a future America, enhanced retinal recognition could be married to omnipresent security cameras as a part of the increasingly routine monitoring of public space. Military surveillance equipment, tempered to a technological cutting edge in counterinsurgency wars, might also one day be married to the swelling domestic databases of the NSA and FBI, sweeping the fiber-optic cables beneath our cities for any sign of subversion. And in the skies above, loitering aircraft and cruising drones could be checking our borders and peering down on American life.

If that day comes, our cities will be Argus-eyed with countless thousands of digital cameras scanning the faces of passengers at airports, pedestrians on city streets, drivers on highways, ATM customers, mall shoppers, and visitors to any federal facility. One day, hyper-speed software will be able to match those millions upon millions of facial or retinal scans to photos of suspect subversives inside a biometric database akin to England's current National Public Order Intelligence Unit, sending anti-subversion SWAT teams scrambling for an arrest or an armed assault.

By the time the Global War on Terror is declared over in 2020, if then, our American world may be unrecognizable — or rather recognizable only as the stuff of dystopian science fiction. What we are proving today is that, however detached from the wars being fought in

their name most Americans may seem, war itself never stays far from home for long. It's already returning in the form of new security technologies that could one day make a digital surveillance state a reality, changing fundamentally the character of American democracy.

Alfred W. McCoy *is the J.R.W. Smail Professor of History at the University of Wisconsin-Madison and the author of A Question of Torture, among other works. His most recent book is Policing America's Empire: The United States, the Philippines, and the Rise of the Surveillance State (University of Wisconsin Press) which explores the influence of overseas counterinsurgency operations throughout the twentieth century in spreading ever more draconian internal security measures here at home.*
