GlobalResearch
Center for Research on Globalization

“FINAL CURTAIN CALL” IN AMERICA? DEEP POLICE STATE SURVEILLANCE AND THE DEATH OF DEMOCRACY

By Tom Burghardt
Global Research, April 01, 2012
Antifascist Calling... 1 April 2012

Region: USA
Theme: Intelligence, Police State & Civil Rights

Over the decades, the maintenance of power and class privileges by corporate, financial and political elites have relied on covert and overt forms of violence, oftentimes in unspoken arrangements with transnational criminal networks (the global drug trade) or intelligence-connected far-right terrorists: the minions who staffed and profited from Operations Condor and Gladio come to mind.

Once viewed as the proverbial “tip” of the imperial spear that advanced elitist dreams of “full-spectrum dominance,” the “plausibly deniable” puppeteering which formerly characterized such projects now take place in full-daylight with nary a peep from bought-off guardians of our ersatz democratic order, or a public narcotized by tawdry spectacles: *Kony 2012* or *American Idol*, take your pick!

Mixing intellectual and moral squalor in equal measure with the latest high-tech gizmos on offer from Silicon Valley or Chengdu, the general societal drift towards *data totalitarianism*, once a hallmark of police states everywhere, is the backdrop where “too big to fail” is code for “too important to jail”!

With the current global economic crisis, brought on in no small part by private and public actors resorting to various frauds and market manipulations which reward privileged insiders, we have reached a social endpoint that analyst Michel Chossudovsky has accurately described as the “criminalization of the state,” that is, the historical juncture where “war criminals legitimately occupy positions of authority, which enable them to decide ‘who are the criminals’, when in fact they are the criminals.”

It should hardly surprise us then that American “hero,” Staff Sergeant Robert Bales, accused of murdering 17 innocent Afghan civilians, including 9 children and then burning their bodies, joined the Army after the 9/11 attacks not out of a sense of patriotic “duty,” but because he was a thief and swindler who went on the lam to avoid accounting for his crimes.

Indeed, ABC News reported that Bales “enlisted in the U.S. Army at the same time he was trying to avoid answering allegations he defrauded an elderly Ohio couple of their life savings in a stock fraud.”

Meanwhile Bales’ attorney John Henry Browne told CBS News that his client has “no memory” of the massacre and that it was “too early” to determine “what factors” may have led to the “incident.”

Some hero.

Keeping Us 'Safe'

However, there are powerful institutional forces at work today which have extremely long–and exceedingly deep–memories, able to catalog and store everything we do electronically, "criminal evidence, ready for use in a trial," or, more in keeping with the preferences of our Hope and Change™ administration, a one-way ticket to indefinite military detention for dissident Americans in the event of a "national security emergency" as a recent White House Executive Order threatened.

> "In an Electronic Police State," Cryptohippie averred, "every surveillance camera recording, every email you send, every Internet site you surf, every post you make, every check you write, every credit card swipe, every cell phone ping… are all criminal evidence, and they are held in searchable databases, for a long, long time. Whoever holds this evidence can make you look very, very bad whenever they care enough to do so. You can be prosecuted whenever they feel like it–the evidence is already in their database."

In stark contrast to feckless promises to undo the egregious constitutional violations of the Bush regime, *The New York Times* reported that the "Obama administration is moving to relax restrictions on how counterterrorism analysts may access, store and search information about Americans gathered by government agencies for purposes other than national security threats."

On March 22, U.S. Attorney General Eric Holder signed-off on new guidelines for the National Counterterrorism Center (NCTC) that "will lengthen to five years–from 180 days–the center's ability to retain private information about Americans when there is no suspicion that they are tied to terrorism," investigative journalist Charlie Savage wrote.

"The guidelines," the *Times* disclosed, "are also expected to result in the center making more copies of entire databases and 'data-mining them'–using complex algorithms to search for patterns that could indicate a threat–than it currently does."

We're told that the relaxation of existing guidelines "grew out of reviews launched after the failure to connect the dots about Umar Farouk Abdulmutallab, the so-called underwear bomber, before his Dec. 25, 2009, attempt to bomb a Detroit-bound airliner."

"'There is a genuine operational need to try to get us into a position where we can make the maximum use of the information the government already has to protect people,' said Robert S. Litt, the general counsel in the office of the Director of National Intelligence, which oversees the National Counterterrorism Center," the *Times* reported.

However, as *Antifascist Calling* disclosed in previous reports on the Abdulmutallab affair (see here, here, here and here) former NCTC Director Michael E. Leiter made a startling admission during hearings before the Senate Homeland Security and Governmental Affairs Committee shortly after the incident.

During those hearings intelligence officials acknowledged that the secret state knowingly allows "watch-listed" individuals, including terrorists, to enter the country in order "to track their movements and activities."

Leiter told congressional grifters: “I will tell you, that when people come to the country and they are on the watch list, it is because we have generally made the choice that we want them here in the country for some reason or another.”

As I wrote at the time: “An alternative explanation fully in line with well-documented inaction, or worse, by U.S. security agencies prior to the September 11, 2001 terrorist attacks and now, Christmas Day’s aborted airline bombing, offers clear evidence that a ruthless ‘choice’ which facilitates the murder of American citizens are cynical pretexts in a wider game: advancing imperialism’s geostrategic goals abroad and attacks on democratic rights at home.”

Commenting on the ramp-up of new surveillance powers grabbed by the Obama administration, Michael German, a former FBI investigator now with the ACLU’s legislative office warned that “the ‘temporary’ retention of nonterrorism-related citizen and resident information for five years essentially removes the restraint against wholesale collection of our personal information by the government, and puts all Americans at risk of unjustified scrutiny.”

Anonymous administration officials who spoke to *The Washington Post* tried to assure us that “a number different agencies looked at these [guidelines] to try to make sure that everyone was comfortable that we had the correct balance here between the information sharing that was needed to protect the country and protections for people’s privacy and civil liberties.”

However, as journalist Marcy Wheeler pointed out “oversight” of the secret state’s surveillance activities are being handled by the ODNI’s Civil Liberties Protection Officer, Alexander Joel, a Bush appointee who was so “concerned” about protecting our privacy that he found no civil liberties violations when he reviewed NSA’s illegal warrantless wiretapping programs.

Joel, a former attorney with the CIA’s Office of General Counsel, told *The Wall Street Journal* that public fears about NSA’s driftnet spying activities were “overblown.”

“Although you might have concerns about what might potentially be going on, those potentials are not actually being realized and if you could see what was going on, you would be reassured just like everyone else,” Joel said.

Despite Joel’s soothing bromides spoon-fed to compliant media, Michael German warned that “such unfettered collection risks reviving the Bush administration’s Total Information Awareness program, which Congress killed in 2003.”

Documents obtained by the Electronic Privacy Information Center (EPIC) through the Freedom of Information Act revealed that TIA aimed “to give law enforcement access to private data without suspicion of wrongdoing or a warrant.”

EPIC learned that “The project called for the development of ‘revolutionary technology for ultra-large all-source information repositories,’ which would contain information from multiple sources to create a ‘virtual, centralized, grand database.’ This database would be populated by transaction data contained in current databases such as financial records, medical records, communication records, and travel records as well as new sources of information. Also fed into the database would be intelligence data.”

Although Congress allegedly "killed" TIA in 2003 when it closed the Pentagon office, we now know from multiple investigations by journalists and from the government's own internal reports, Total Information Awareness never went away but rather, was hidden behind impenetrable layers of above top secret Special Access Programs and code-name protected projects, most of which are controlled by the National Security Agency.

'A Turnkey Totalitarian State'

The secret state's "virtual, centralized, grand database" will shortly come on line.

As investigative journalist James Bamford recently reported in *Wired Magazine*, "new pioneers" are taking up residence in the small Utah town of Bluffdale, home to the largest sect of renegade Mormon polygamists: the National Security Agency's Utah Data Center.

"A project of immense secrecy," Bamford wrote, "it is the final piece in a complex puzzle assembled over the past decade. Its purpose: to intercept, decipher, analyze, and store vast swaths of the world's communications as they zap down from satellites and zip through the underground and undersea cables of international, foreign, and domestic networks. The heavily fortified $2 billion center should be up and running in September 2013."

Wired disclosed that all manner of communications will flow into Bluffdale's "near-bottomless databases" including "the complete contents of private emails, cell phone calls, and Google searches, as well as all sorts of personal data trails–parking receipts, travel itineraries, bookstore purchases, and other digital 'pocket litter'."

Additionally, one top NSA official involved with the program told Bamford that the agency "made an enormous breakthrough several years ago in its ability to cryptanalyze, or break, unfathomably complex encryption systems employed by not only governments around the world but also many average computer users in the US. The upshot, according to this official: 'Everybody's a target; everybody with communication is a target'."

"For the first time since Watergate and the other scandals of the Nixon administration–the NSA has turned its surveillance apparatus on the US and its citizens," Bamford averred. "It has established listening posts throughout the nation to collect and sift through billions of email messages and phone calls, whether they originate within the country or overseas."

Since the dawn of the Cold War, the National Security Agency operated outside its charter, illegally spying on the communications of dissident Americans. In a companion piece for *Wired*, Bamford detailed how NSA denied that it was eavesdropping on Americans.

"For example," Bamford wrote, "NSA can intercept millions of domestic communications and store them in a data center like Bluffdale and still be able to say it has not 'intercepted' any domestic communications. This is because of its definition of the word. 'Intercept,' in NSA's lexicon, only takes place when the communications are 'processed' 'into an intelligible form intended for human inspection,' not as they pass through NSA listening posts and transferred to data warehouses."

NSA mendacity aside, "for decades," Bamford informed us, "the agency secretly hid from Congress the fact that it was copying, without a warrant, virtually every telegram traveling through the United States, a program known as Project Shamrock. Then it hid from Congress the fact that it was illegally targeting the phone calls of anti-war protesters during the Vietnam War, known as Project Minaret."

But as we learned when *The New York Times* disclosed some aspects of the Bush regime's Stellar Wind program, the NSA was caught red-handed illegally spying on tens of thousands of Americans without benefit of a warrant and did so with the full cooperation of America's giant telecom firms and internet service providers who were then immunized by Congress under provisions of 2008's despicable FISA Amendments Act (FAA).

Even as Congress granted retroactive immunity to telecoms and ISPs, and politicians, including President Obama, scrambled to downplay serious violations to individual political and privacy rights, the enormous reach of these programs are still misunderstood by the public.

William Binney, a former NSA official who was a senior "crypto-mathematician largely responsible for automating the agency's worldwide eavesdropping network," went on the record with *Wired* and denounced NSA's giant domestic eavesdropping machine.

Binney explained "that the agency could have installed its tapping gear at the nation's cable landing stations–the more than two dozen sites on the periphery of the US where fiber-optic cables come ashore. If it had taken that route, the NSA would have been able to limit its eavesdropping to just international communications, which at the time was all that was allowed under US law."

"Instead," Binney told *Wired*, the agency "chose to put the wiretapping rooms at key junction points throughout the country–large, windowless buildings known as switches–thus gaining access to not just international communications but also to most of the domestic traffic flowing through the US. The network of intercept stations goes far beyond the single room in an AT&T building in San Francisco exposed by a whistle-blower in 2006. 'I think there's 10 to 20 of them,' Binney says. 'That's not just San Francisco; they have them in the middle of the country and also on the East Coast'."

Readers will recall that back in 2006, former AT&T technician Marc Klein blew the lid off the technical details of Stellar Wind, disclosing internal AT&T documents on how the firm gave NSA free-reign to install ultra-secret Narus machines. Those devices split communications as they flowed into AT&T's "secret rooms" and diverted all internet traffic into NSA's bottomless maw.

Klein, the author of *Wiring Up the Big Brother Machine* said that the program "was just the tip of an eavesdropping iceberg" which is not only targeted at suspected "terrorists" but rather is "an untargeted, massive vacuum cleaner sweeping up millions of peoples' communications every second automatically."

Narus, an Israeli firm founded by retired members of the IDF's secretive Unit 8200, now owned by The Boeing Corporation, and Verint, now Comverse Infosys, another Israeli firm, were close partners alongside NSA in these illegal projects; one more facet of the U.S. and Israel's "special relationship."

The former official turned whistleblower told *Wired* that "Stellar Wind was far larger than has been publicly disclosed and included not just eavesdropping on domestic phone calls but the inspection of domestic email."

> "At the outset the program recorded 320 million calls a day," Bamford wrote, "which represented about 73 to 80 percent of the total volume of the agency's

> worldwide intercepts. The haul only grew from there. According to Binney–who has maintained close contact with agency employees until a few years ago–the taps in the secret rooms dotting the country are actually powered by highly sophisticated software programs that conduct 'deep packet inspection,' examining Internet traffic as it passes through the 10-gigabit-per-second cables at the speed of light."

"Once a name is entered into the Narus database," Binney said, "all phone calls and other communications to and from that person are automatically routed to the NSA's recorders."

> "'Anybody you want, route to a recorder,' Binney says. 'If your number's in there? Routed and gets recorded.' He adds, 'The Narus device allows you to take it all.' And when Bluffdale is completed, whatever is collected will be routed there for storage and analysis."

Chillingly, Binney "held his thumb and forefinger close together" and told Bamford: "'We are that far from a turnkey totalitarian state'."

Main Core

During World War II, the Roosevelt administration issued Executive Order 9066 which granted the military carte blanche to circumvent the constitutional rights of some 120,000 Japanese-American citizens and led to their mass incarceration in remote, far-flung camps surrounded by barbed wire and armed guards.

Will history repeat, this time under the rubric of America's endless "War on Terror"?

In 2008, investigative journalists Christopher Ketchum reported in the now-defunct *Radar Magazine* and Tim Shorrock, writing in *Salon*, provided details on a frightening "Continuity of Government" database known as Main Core.

According to Ketchum, a senior government official told him that "there exists a database of Americans, who, often for the slightest and most trivial reason, are considered unfriendly, and who, in a time of panic, might be incarcerated. The database can identify and locate perceived 'enemies of the state' almost instantaneously."

That official and other sources told *Radar* that "the database is sometimes referred to by the code name Main Core. One knowledgeable source claims that 8 million Americans are now listed in Main Core as potentially suspect. In the event of a national emergency, these people could be subject to everything from heightened surveillance and tracking to direct questioning and possibly even detention."

For his part, Shorrock revealed that several government officials with above top secret security clearances told him that "Main Core in its current incarnation apparently contains a vast amount of personal data on Americans, including NSA intercepts of bank and credit card transactions and the results of surveillance efforts by the FBI, the CIA and other agencies."

> "One former intelligence official," Shorrock reported, "described Main Core as 'an emergency internal security database system' designed for use by the military in the event of a national catastrophe, a suspension of the Constitution

> or the imposition of martial law. Its name, he says, is derived from the fact that it contains 'copies of the 'main core' or essence of each item of intelligence information on Americans produced by the FBI and the other agencies of the U.S. intelligence community'."

It now appears that Main Core, or some other code-word protected iteration of the secret state's administrative detention database will in all likelihood soon reside at Bluffdale.

While conservative and liberal supporters of the Bush and Obama administrations have derided these reports as the lunatic ravings of "conspiracy theorists," analysts such as Peter Dale Scott have made clear that a decade after the 9/11 attacks, "some aspects of COG remain in effect. COG plans are still authorized by a proclamation of emergency that has been extended each year by presidential authority, most recently by President Obama in September 2009. COG plans are also the probable source for the 1000-page Patriot Act presented to Congress five days after 9/11, and also for the Department of Homeland Security's Project Endgame–a ten-year plan, initiated in September 2001, to expand detention camps, at a cost of $400 million in Fiscal Year 2007 alone."

> "At the same time," Scott wrote, "we have seen the implementation of the plans outlined by [Miami Herald journalist Alfonso] Chardy in 1987: the warrantless detentions that Oliver North had planned for in Rex 1984, the warrantless eavesdropping that is their logical counterpart, and the militarization of the domestic United States under a new military command, NORTHCOM. Through NORTHCOM the U.S. Army now is engaged with local enforcement to control America, in the same way that through CENTCOM it is engaged with local enforcement to control Afghanistan and Iraq."

Indeed, as the *Associated Press* recently disclosed in their multipart investigation into illegal spying by the New York Police Department (NYPD), undercover officers "attended meetings of liberal political organizations and kept intelligence files on activists who planned protests around the U.S., according to interviews and documents that show how police have used counterterrorism tactics to monitor even lawful activities."

A 2008 intelligence report obtained by AP revealed "how, in the name of fighting terrorism, law enforcement agencies around the country have scrutinized groups that legally oppose government policies."

"The FBI for instance," investigative journalists Adam Goldman and Matt Apuzzo averred, "has collected information on anti-war demonstrators. The Maryland state police infiltrated meetings of anti-death penalty groups. Missouri counterterrorism analysts suggested that support for Republican Rep. Ron Paul might indicate support for violent militias–an assertion for which state officials later apologized. And Texas officials urged authorities to monitor lobbying efforts by pro Muslim-groups."

> "The April 2008 memo offers an unusually candid view of how political monitoring fit into the NYPD's larger, post-9/11 intelligence mission. As the AP has reported previously, [David] Cohen's unit has transformed the NYPD into one of the most aggressive domestic intelligence agencies in the United States, one that infiltrated Muslim student groups, monitored their websites and used informants as listening posts inside mosques."

Nor should we forget how the Pentagon's own domestic intelligence unit, the Counterintelligence Field Activity or CIFA, routinely monitored antiwar activists and other dissidents.

As *Antifascist Calling* previously reported, multiple news reports beginning in late 2005 revealed that CIFA with 400 full-time DoD workers and 900 "outsourced" contractor employees and a classified budget, had been authorized to track "potential terrorist threats" against DoD through reports known as Threat and Local Observation Notices (TALON).

Although that office was shuttered in 2008, its domestic security functions were transferred to the Defense Intelligence Agency's Defense Counterintelligence and Human Intelligence Center and the TALON database along with future "threat reports" would now be funneled to an FBI database known as "Guardian."

However, as *SourceWatch* noted, "in accordance with intelligence oversight requirements," even though CIFA was closed down, DoD "will maintain a record copy of the collected data." In other words TALON reports, including data illegally collected on antiwar activists, will continue to exist somewhere deep in the bowels of the Defense Department, more likely than not in a Bluffdale database administered by NSA.

When President Obama signed the National Defense Authorization Act (NDAA) into law on December 31, he did more than simply facilitate multibillion dollar Pentagon boondoggles for the current fiscal year; he set the stage for what journalist Christopher Ketchum called "The Last Roundup," and what James Bamford's source denounced as our approaching "turnkey totalitarian state."

We need not speculate as to *when* an American police state will be fully functional, *it already is.*

Tom Burghardt is a researcher and activist based in the San Francisco Bay Area. In addition to publishing in Covert Action Quarterly and Global Research,, he is a Contributing Editor with Cyrano's Journal Today. His articles can be read on Dissident Voice, Pacific Free Press, Uncommon Thought Journal, and the whistleblowing website WikiLeaks. He is the editor of Police State America: U.S. Military "Civil Disturbance" Planning, distributed by AK Press and has contributed to the new book from Global Research, The Global Economic Crisis: The Great Depression of the XXI Century.
