"MANAGING" DATA AND DISSENT IN AMERICA

Posted on April 5, 2010 by Keghart

Category: Opinions

By Tom Burghardt, GlobalResearch.ca ,5 April 2010

Repression doesn't come cheap, just ask the FBI.

As the securitization of daily life increase at near exponential rates (all to keep us "safe," mind you) the dark contours of an American police state, like a pilot's last glimpse of an icy peak before a plane crash, wobbles into view.

By Tom Burghardt, GlobalResearch.ca ,5 April 2010

Repression doesn't come cheap, just ask the FBI.

As the securitization of daily life increase at near exponential rates (all to keep us "safe," mind you) the dark contours of an American police state, like a pilot's last glimpse of an icy peak before a plane crash, wobbles into view.

In the main, such programs include, but are by no means limited to the following: electronic surveillance (call records, internet usage, social media); covert hacking by state operatives; GPS tracking; CCTV cameras linked-in to state databases; "smart" cards; RFID chipped commodities and the spooky "internet of things;" biometrics, and yes, the Pentagon has just stood up a Biometrics Identity Management Agency (BIMA); data-mining; watch listing; on and on it goes.

Pity our poor political minders, snowed-under by a blizzard of data-sets crying out for proper "management"! Or, as sycophantic armchair warrior and New York Times columnist, Thomas Friedman, would have it, "The hidden hand of the market will never work without a hidden fist--McDonald's cannot flourish without McDonnell Douglas, the designer of the F-15."

So true; yet neither can an aggregate of repressive police and intelligence agencies function without an army of corporate grifters who guide that "hidden hand" and not-so-hidden fist into highly profitable safe harbors. Call it Big Brother meets market fundamentalism.

And so, the heat is on as America's premier political police agency struggles to "modernize" their case file management system.

The FBI's Case Management "Problem"

When circumstances (a massive up-tick in illegal spying since 9/11 courtesy of the USA Patriot Act) forced the Bureau to store a treasure trove of tittle-tattle of "national security interest" on decidedly low-tech storage devices, FBI agents and their all-too-willing helpers from giant telecommunications firms such as AT&T took to scribbling "leads" on post-it notes.

Communications Analysis Unit (CAU) eager-beavers did so in order to speed-up the process of obtaining dodgy "exigent letters" that smoothed over the wrinkles (your rights!) as the Bureau issued tens of thousands of National Security Letters (NSLs).

The secretive lettres de cachet demanded everything: emails, internet searches, call records, bank statements, credit card purchases, travel itineraries, medical histories, educational résumés, even video rentals and books borrowed from public libraries. The contents of such shady administrative warrants cannot be disclosed by their recipients under penalty of stiff fines or even imprisonment.

While such extra-legal missives are supposedly issued only in cases of dire "emergency," the banal, ubiquitous nature of surveillance in post-Constitutional, "new normal" regimes such as the United States, all but guarantee that extraordinary "states of exception" are standard rules of the game in our managed democracy.

As the Justice Department's Office of the Inspector General revealed in a heavily-redacted report in January, with all semblance of a legal process out the window, the FBI were caught with their hands in the proverbial cookie jar, repeatedly violating the Electronic Communications Privacy Act.

Fear not, Obama administration legal eagles cobbled together a new theory justifying the practice and have created, yet another, accountability free zone for agents who violated the rules.

Neatly, seamlessly and silently Obama's Office of Legal Counsel (John Yoo and Judge Bybee's old stomping grounds) granted them, wait!, retroactive immunity for such lawbreaking. The trouble is, the OLC's ruling is classified so we haven't a clue what it entails or how far-reaching is its purview. So much for the new era of "openness" and "transparency."

But I digress...

The New York Times reported March 18, that work on parts of the Bureau's cracker-jack case management program known as Sentinel has been "temporarily" suspended.

While the "overhaul" was supposed "to be completed this fall,"Times journalist Eric Lichtblau disclosed that the system will not be ready for prime time until "next year at the earliest."

Overall, American taxpayers have shelled-out some $451 million to an endless parade of contractors, Lockheed Martin being the latest. Delays are expected to cost "at least $30 million in cost overruns on a project considered vital to national security" Lichtblau wrote, citing Congressional "officials."

But problems have plagued the project since its inception. Lockheed Martin, No. 1 on Washington Technology's "2009 Top 100" list of Prime Federal Contractors, secured some $14,983,515,367 in defense-related contracts last year and was brought on-board to revamp the troubled case management project.

This is all the more ironic considering that the defense giant was hailed as Sentinel's savior, after an earlier incarnation of the program known as Virtual Case File (VCF), overseen by the spooky Science Applications International Corporation (SAIC), crashed and burned in 2006.

No slouches themselves when it comes to raking-in taxpayer boodle, SAIC is No. 7 on the

Washington Technology list, pulling in some $4,811,194,880 in 2009, largely as a result of the firm's close political connections to the Defense Department and the secret state.

SAIC's work on VCF began in June 2001 and was expected to be completed in 36 months. However, after shelling out some $170 million over four years the Bureau concluded the system wouldn't work. Published reports fail to mention whether or not SAIC was forced to hand the loot back to cash-strapped taxpayers. Probably not.

Open-Ended Contracts: Hitting the Corporatist "Sweet Spot"

As with all things having to do with protecting their national security constituency from lean quarterly reports to shareholders, congressional grifters and secret state agencies alike are adept at showering giant defense and security corporations with multiyear, multibillion dollar contracts.

After all, high-end CEO salaries and lucrative remunerations for top executives in the form of handsome bonuses are based, not on a firm's actual performance but rather, on the critical up-tick in the share price; just ask Lehman Brothers or other outstanding corporate citizens such as Goldman Sachs. Or SAIC itself, for that matter!

Unfortunately, effective oversight is not the forte of a plethora of congressional committees; nor are crisp, objective evaluations, better known as due diligence, conducted by outside auditors before scarce federal resources, which could be used for quaint things such as health care, education or other reality-based programs, pour into any number of virtual black holes.

Take VCF as an example.

In a post-mortem of the SAIC program, The Washington Post revealed back in 2006, that after spending months writing 730,000 lines of computer code, corporate officers proclaimed VCF's roll-out "only weeks away."

The trouble was, software problem reports, or SPRs, "numbered in the hundreds." Worse for SAIC, as engineers continued running tests, systemic problems were multiplying quicker than proverbial rabbits.

As Post journalists Dan Eggen and Griff Witte disclosed, citing an unreleased audit of the program hushed-up by the Bureau, because "of an open-ended contract with few safeguards, SAIC reaped more than $100 million as the project became bigger and more complicated, even though its software never worked properly."

Despite evidence that the system was failing badly, SAIC "continued to meet the bureau's requests, accepting payments despite clear signs that the FBI's approach to the project was badly flawed."

Auditors discovered that the "system delivered by SAIC was so incomplete and unusable that it left the FBI with little choice but to scuttle the effort altogether."

David Kay, a former SAIC senior vice president and Bushist chief weapons inspector in Iraq tasked with finding nonexistent "weapons of mass destruction," told the Post even though top executives at the firm were aware the project was going "awry," they didn't insist on changes "because the bureau continued to pay the bills as the work piled up."

"From the documents that define the system at the highest level, down through the software design and into the source code itself," Aerospace, the independent firm that conducted the secretive FBI audit, "discovered evidence of incompleteness, lack of follow-through, failure to optimize and missing documentation."

Even more damning, a report by computer experts from the National Research Council and SAIC insider, Matthew Patton, removed from the program by top executives after posting critical remarks on VCF in an on-line forum, found that the firm "kept 200 programmers on staff doing 'make work'," when a "couple of dozen would have been enough."

SAIC's attitude, according to Patton, was that "it's other people's money, so they'll burn it every which way they want to."

As a cash cow, VCF was a superlative program; however, the IT security specialist told the Post: "Would the product actually work? Would it help agents do their jobs? I don't think anyone on the SAIC side cared about that."

Why would they? After all, $170 million buys much in the way of designer golf bags, pricey Hawaiian getaways or other necessities useful for navigating the dangerous shoals of America's "war on terror"!

As investigative journalist Tim Shorrock detailed in his essential book, Spies For Hire and for CorpWatch, SAIC "stands like a private colossus across the whole intelligence industry." Shorrock writes, "of SAIC's 42,000 employees, more than 20,000 hold U.S. government security clearances, making it, with Lockheed Martin, one of the largest private intelligence services in the world."

As the journalist revealed, while SAIC "is deeply involved in the operations of all the major collection agencies, particularly the NSA, NGA and CIA," failure also seems to come with the corporate territory.

"For example" Shorrock wrote, the firm "managed one of the NSA's largest efforts in recent years, the $3 billion Project Trailblazer, which attempted (and failed) to create actionable intelligence from the cacophony of telephone calls, fax messages, and emails that the NSA picks up every day. Launched in 2001, Trailblazer experienced hundreds of millions of dollars in cost overruns and NSA cancelled it in 2005."

Is there a pattern here?

No matter. Washington Technology reported March 31, that SAIC's fourth quarter revenues and overall gains for fiscal year 2010 were "$2.68 billion, a 7 percent increase, up from $2.52 billion in the fourth quarter of fiscal 2009, the company announced. Full-year revenues were $10.85 billion, up 8 percent from fiscal 2009. Fiscal 2010 ended Jan. 31."

"We are pleased to complete the fiscal year with improved operating margin, earnings per share and cash generation," Walt Havenstein, SAIC's chief executive officer said in a corporate press release.

"We enter fiscal year 2011 with our portfolio of capabilities well aligned with national priorities, emphasizing areas such as intelligence, surveillance, and reconnaissance (ISR), cybersecurity, logistics, energy, and health technology to fuel our growth and shareholder value prospects," Havenstein added.

If by "national priorities" SAIC's head honcho means the continued bleed-out of taxpayer funds into corporate coffers, then, by all means, 2010 was a banner year!

Which brings us full-circle to Lockheed Martin and Sentinel.

DOJ Inspector General: "Significant Challenges"

The Department of Justice Office of the Inspector General (OIG) disclosed in a redacted December 2009 report that the Lockheed Martin system "encountered significant challenges." As of August 2009, "the FBI and Lockheed Martin agreed to revise the project's schedule, increase Lockheed Martin's cost to develop Phase 2 to $155 million, and update the remaining costs for Phases 3 and 4."

Sound familiar?

"Consequently" the OIG reported, "the overall project completion date has been extended to September 2010, 3 months later than we previously reported and 9 months later than originally planned." In a new report released in late March, Department of Justice auditors revised their previous analysis. It wasn't a pretty picture.

According to the OIG, "As of March 2010, the FBI does not have official cost or schedule estimates for completing Sentinel. The remaining budget, schedule, and work to be performed on Sentinel are currently being renegotiated between the FBI and Lockheed Martin. While the FBI does not yet have official estimates, FBI officials have acknowledged that the project will cost more than its latest revised estimate of $451 million and will likely not be completed until 2011." That can only be music to Lockheed Martin's ears!

As the Times reported, work on the project has ground to a halt. This was confirmed by the OIG. "On March 3, 2010, because of significant issues regarding Phase 2 Segment 4's usability, performance, and quality delivered by Lockheed Martin, the FBI issued a partial stop-work order to Lockheed Martin for portions of Phase 3 and all of Phase 4."

The latest set-back to taxpayers mean that the Bureau's "stop-work order returned Phase 2 Segment 4 of the project from operations and maintenance activities to the development phase."

In other words, after four years and nearly $500 million, its back to the drawing board!

After beating out their rivals for work on a program considerably more costly than SAIC's failed VCF, the OIG revealed that multiple issues and problems plague the system designed by the defense giant.

"First, there were significant problems with the usability of electronic forms that were developed for Sentinel." The forms are supposedly the heart of the system and the tools through which FBI repressors "manage" case-related information deployed across the Bureau, particularly when agents add or subtract data gleaned from the FBI's massive Investigative Data Warehouse (IDW).

Last year, Antifascist Calling reported on the Bureau's spooky "Library of Babel," IDW, that does yeoman's work as a virtual Department of Precrime.

A massive project, IDW already holds more than a billion unique, searchable records on American citizens and legal residents that the Electronic Frontier Foundation (EFF) said would be used to "data-mine ... using unproven science in an attempt to predict future crimes from past behavior."

The IDW is one of the data-mining projects that Sentinel will directly tap into, allowing the migration of data currently held in the FBI's antiquated Automated Case Support (ACS) system.

The OIG report revealed, "there were 26 critical issues related to the functionality of Sentinel that required resolution before deployment" and that "Lockheed Martin had deviated from accepted systems engineering processes in developing the software code for Sentinel."

According to a review of the program by the shadowy MITRE Corporation, more than 10,000 "inefficiencies" in the software code may collectively result in the diminished performance of the "product."

Do these problems pose a "challenge" to either the Bureau or Lockheed Martin executives? Hardly! The OIG disclosed that "FBI officials have stated that in order to meet any increased funding requirements, the FBI plans to request congressional approval to redistribute funds from other FBI information technology programs to Sentinel."

How's that for creative accounting!

Repression: A Game the Whole Corporate "Family" Can Play

With their fingers into everything from missile design and satellite surveillance technology to domestic spying or that latest craze consuming Washington, "cybersecurity," Lockheed Martin is, as they say, a "player."

On the domestic spy game front, Lockheed Martin were one of the contractors who supplied intelligence analysts for the Counterintelligence Field Activity office (CIFA), the secretive Rumsfeld-era initiative that spied on antiwar activists and other Pentagon policy critics.

CIFA was tasked with tracking "logical combinations of keywords and personalities" used to estimate current or future threats. When CIFA was shuttered after public outcry, its functions were taken over by the Defense Intelligence Agency, where Lockheed Martin runs a bidding consortium.

But as with CIFA, the DIA's Defense Counterintelligence and Human Intelligence Center, relies heavily on the unproven "science" of data-mining and its offshoot, link analysis.

Data-mining by corporate and secret state agencies such as the FBI seek to uncover "hidden patterns" and "subtle relationships" within disparate data-sets in order to "infer rules that allow for the prediction of future results," according to a 2004 Government Accountability Office (GAO) report.

Sentinel will undoubtedly deploy data-mining techniques insofar as they are applicable to "managing" alleged foreign "terrorism plots," but also domestic dissidents identified as national security "risks."

Although the Sentinel program has apparently hit a brick wall in terms of operability, it is also clear that the FBI and other national security agencies, will continue their quixotic quest for technophilic "silver bullets" to "manage" domestic dissent.

That such endeavors are illusory, as with the Pentagon's "Revolution in Military Affairs" that promised always-on "persistent area surveillance" of the "battlespace," the deployment of high-priced sensor technologies and data-mining algorithms assure securocrats that "total information awareness" is only a keystroke away.

While "situational awareness" may be an illusive commodity, when it comes to data storage and the indexing of alleged national security threats, systems such as Sentinel or the Investigative Data Warehouse, as well as the broader application of predictive data-mining to map so-called terrorist "nodes" expand the operation and intensification of the "surveillance society" ever-deeper into social life.

As Tim Shorrock revealed in CorpWatch, in 2004 and 2005 Lockheed Martin "acquired the government IT unit of Affiliated Computer Services Inc., inheriting several contracts with defense intelligence agencies and Sytex, a $425 million Philadelphia-based company that held contracts with the Pentagon's Northern Command and the NSA/Army Intelligence and Security Command. By 2007 the company employed 52,000 IT specialists with security clearances, and intelligence made up nearly 40 percent of its annual business, company executives said."

According to Shorrock, one of the firm's "most important intelligence-related acquisitions took place in the 1990s, when the conglomerate bought Betac Corporation. Betac was one of the companies the government hired during the late 1980s to provide communications technology for the secret Continuity of Government program the Reagan administration created to keep the U.S. government functioning in the event of a nuclear attack."

As readers are aware, secretive Continuity of Government programs went into effect after the 9/11 attacks. Details on these programs have never been revealed, although investigative journalists have discovered that some portions of COG have to do with the national security indexing of American citizens in a massive, classified database known as Main Core.

As investigative journalist Christopher Ketcham revealed in 2008, one "well-informed source--a former military operative regularly briefed by members of the intelligence community--says this particular program has roots going back at least to the 1980s and was set up with help from the Defense Intelligence Agency. He has been told that the program utilizes software that makes predictive judgments of targets' behavior and tracks their circle of associations with 'social network analysis' and artificial intelligence modeling tools."

Ketcham's source told him that "'the more data you have on a particular target, the better can predict what the target will do, where the target will go, who it will turn to for help,' he says. 'Main Core is the table of contents for all the illegal information that the U.S. government has on specific targets.' An intelligence expert who has been briefed by high-level contacts in the Department of Homeland Security confirms that a database of this sort exists, but adds that 'it is less a mega-database than a way to search numerous other agency databases at the same time'."

Shorrock writes that "Under a 1982 presidential directive, the outbreak of war could trigger the proclamation of martial law nationwide, giving the military the authority to use its domestic database to round up citizens and residents considered threats to national security. The Federal Emergency Management Agency (FEMA) and the Army were to carry out the emergency measures for domestic security."

And one of the "biggest winners" was Betac Corporation, "a consulting firm composed of former intelligence and communications specialists from the Pentagon. Betac was one of the largest government contractors of its day and, with TRW and Lockheed itself, dominated the intelligence contracting industry from the mid-1980s until the late 1990s."

"Its first project for the Continuity of Government plan," Shorrock reveals, "was a sole-source contract to devise and maintain security for the system. Between 1983 and 1985, the contract expanded from $316,000 to nearly $3 million, and by 1988 Betac had multiple COG contracts worth $22 million. Betac was eventually sold to ACS Government Solutions Group and is now a unit of Lockheed Martin."

While it is de rigueur, particularly since the rise of the Obama administration, to deride critics who point out the perils of an out-of-control national security state armed with meta-databases such as Main Core and secretive COG programs as "conspiracy theorists," such "whistling past the graveyard" is done at great peril to an open and transparent democratic system of governance based on accountability and the rule of law.