GlobalResearch
Center for Research on Globalization

Electronic Surveillance: America's Secret Domestic Spying Apparatus

By Tom Burghardt
Global Research, May 09, 2011
Antifascist Calling... 9 May 2011
Theme: Police State & Civil Rights

by ***Antifascist Calling…***

Despite last week's "termination" of America's *bête noire*, Osama bin Laden, the reputed "emir" and old "new Hitler" of the Afghan-Arab database of disposable Western intelligence assets known as al-Qaeda, ***Secrecy News*** reports an uptick in domestic spying.

Never mind that the administration is engaged in an unprecedented **war on whistleblowers**, or is systematically targeting antiwar and solidarity activists with trumped-up charges connected to the "material support of terrorism," as last Fall's multi-state **raids** on anarchists and socialists in Chicago and Minneapolis attest.

In order to do their best to "keep us safe," Team Obama is busily building upon the criminal legacy bequeathed to the administration by the Bush regime and even asserts the right to assassinate American citizens "without a whiff of due process," as ***Salon's*** Glenn Greenwald points out.

According to a new Justice Department **report** submitted to Congress we learn that "during calendar year 2010, the Government made 1,579 applications to the Foreign Intelligence Surveillance Court (hereinafter 'FISC') for authority to conduct electronic surveillance and/or physical searches" on what U.S. security agencies allege are "for foreign intelligence purposes."

The April 29 missive, released under the Freedom of Information Act, documents the persistence of our internal security apparat's targeting of domestic political opponents, under color of rooting out "terrorists."

Secrecy News analyst Steven Aftergood comments that "this compares to a reported 1,376 applications in 2009. (In 2008, however, the reported figure–2,082–was quite a bit higher.)"

"In 2010," Aftergood writes, "the government made 96 applications for access to business records (and 'tangible things') for foreign intelligence purposes, up from 21 applications in 2009."

Also last year, America's premier domestic intelligence agency, the FBI, "made 24,287 'national security letter' requests for information pertaining to 14,212 different U.S. persons, a substantial increase from the 2009 level of 14,788 NSL requests concerning 6,114 U.S. persons. (In 2008, the number of NSL requests was 24,744, pertaining to 7,225 persons.)"

As I have pointed out many times, national security letters are onerous *lettres de cachet*,

secretive administrative subpoenas with built-in gag orders used by the Bureau to seize records from third-parties such as banks, libraries and telecommunications providers without any judicial process whatsoever, not to mention the expenditure of scarce tax dollars to spy on the American people.

"Money for Nothing…"

With U.S. Attorney General Eric Holder's February **announcement** that the Department of Justice will seek $28.2 billion from Congress in Fiscal Year 2012, a 1.7% increase, the FBI is slated to reap an $8.1 billion windfall.

We're told that the "administration supports critical national security programs within the department, including the FBI and the National Security Division (NSD)."

"The requested national security resources include $122.5 million in program increases for the FBI," including "$48.9 million for the FBI to expand national security related surveillance and enhance its Data Integration and Visualization System, as well as "$18.6 million for the FBI's Computer Intrusion Initiative to increase coverage in detecting cyber intrusions."

Rather ironic, considering that ***ThreatPost*** reported last month that a U.S. Department of Justice **audit** found that the FBI's ability to "investigate cyber intrusions" was less than adequate. The report disclosed that "fully 36% [of field agents] were found to be ill-equipped."

To make matters worse, "FBI field offices do not have sufficient analytical and forensic capabilities to support large scale investigations, the audit revealed." All the more reason then to shower even *more* money on the Bureau!

And with the FBI demanding new authority to peer into our lives, on- and offline, the FY 2012 budget would "address the growing technological gap between law enforcement's electronic surveillance capabilities and the number and variety of communications devices available to the public, $17.0 million in program increases are being requested to bolster the department's electronic surveillance capabilities."

One sure sign that things haven't changed under Obama is the FBI's quest for additional funds for what it is now calling it's Data Integration and Visualization System (DIVS). According to April congressional **testimony** by FBI Director Robert Mueller, DIVS will "prioritize and integrate disparate datasets across the Bureau."

Another in a long line of taxpayer-funded boondoggles, it appears that DIVS is the latest iteration of various failed "case management" and "data integration" programs stood up by the Bureau.

As I **reported** last year, previous failed efforts by the FBI have included the Bureau's Virtual Case File (VCF) project. Overseen by the spooky Science Applications International Corporation (SAIC), VCF cost taxpayers some $170 million dollars before it crashed and burned in 2006.

And when defense and security giant Lockheed Martin took over the case management brief, VCF, now rechristened Sentinel, also enjoyed a similarly expensive and waste-filled fate. A 2009 report by the Department of Justice's Office of the Inspector General (**OIG**) found that despite some $450 million dollars showered on Lockheed Martin and assorted

subcontractors, the Sentinel system "encountered significant challenges."

According to a notice quietly posted in August in the **Federal Register**, "DIVS contains replications and extractions of information maintained by the FBI in other databases. This information is replicated or extracted into DIVS in order to provide an enhanced and integrated view of that information."

Wait a minute! Isn't that what VCF and Sentinel were *supposed* to do? We're told that the "purpose of DIVS is to strengthen and improve the methods by which the FBI searches for and analyzes information in support of its multifaceted mission responsibilities to protect the nation against terrorism and espionage and investigate criminal matters."

(Dirty) Business as Usual

While the FBI and the Justice Department have failed to prosecute corporate criminals responsible for the greatest theft and upward transfer of wealth in history, not to mention the virtual get-out-of-jail-free cards handed out to top executives of the drug-money laundering **Wachovia Bank**, they're rather adept at trampling the rights of the American people.

As the ***San Francisco Bay Guardian*** recently reported, while corporate lawbreakers get a free pass, "San Francisco cops assigned to the FBI's terrorism task force can ignore local police orders and California privacy laws to spy on people without any evidence of a crime."

According to a Memorandum of Understanding obtained by the ACLU, "it effectively puts local officers under the control of the FBI," investigative journalist Sarah Phelan disclosed.

Civil rights attorney Veena Dubal told the *Bay Guardian* that during "the waning months of the Bush administration" the FBI "changed its policies to allow federal authorities to collect intelligence on a person even if the subject is not suspected of a crime. The FBI is now allowed to spy on Americans who have done nothing wrong–and who may be engaged in activities protected by the First Amendment."

"It's the latest sign of a dangerous trend: San Francisco cops are working closely with the feds, often in ways that run counter to city policy," Phelan writes. "And it raises a far-reaching question: With a district attorney who used to be police chief, a civilian commission that isn't getting a straight story from the cops, and a climate of secrecy over San Francisco's intimate relations with outside agencies, who is watching the cops?"

Apparently, no one; and in such a repressive climate the federal government has encouraged the FBI to target anyone deemed a threat to the new corporate order.

Earlier this year, an Electronic Frontier Foundation **report** revealed that the Bureau continues to systematically violate the constitutional guarantees of American citizens and legal residents, and does so with complete impunity.

As I **wrote** at the time, this was rather ironic considering the free passes handed out by U.S. securocrats to actual terrorists who killed thousands of Americans on 9/11, as both **WikiLeaks** and FBI whistleblower **Sibel Edmonds** disclosed.

According to EFF, more than 2,500 documents obtained under the Freedom of Information

Act revealed that:

* From 2001 to 2008, the FBI reported to the IOB approximately 800 violations of laws, Executive Orders, or other regulations governing intelligence investigations, although this number likely significantly under-represents the number of violations that actually occurred.

* From 2001 to 2008, the FBI investigated, at minimum, 7000 potential violations of laws, Executive Orders, or other regulations governing intelligence investigations.

* Based on the proportion of violations reported to the IOB and the FBI's own statements regarding the number of NSL violations that occurred, the actual number of violations that may have occurred from 2001 to 2008 could approach 40,000 possible violations of law, Executive Order, or other regulations governing intelligence investigations. (Electronic Frontier Foundation, *Patterns of Misconduct: FBI Intelligence Violations from 2001-2008*, January 30, 2011)

But FBI lawbreaking didn't stop there. Citing internal documents, EFF revealed that the Bureau also "engaged in a number of flagrant legal violations" that included, "submitting false or inaccurate declarations to courts," "using improper evidence to obtain federal grand jury subpoenas" and "accessing password protected documents without a warrant."

And just last week the civil liberties' watchdogs **reported** that "the U.S. District Court for the Central District of California has revealed the FBI lied to the court about the existence of records requested under the Freedom of Information Act (FOIA), taking the position that FOIA allows it to withhold information from the court whenever it thinks this is in the interest of national security."

The court sharply disagreed and **asserted** that "the Government cannot, under any circumstance, affirmatively mislead the Court."

The Court held, following settled case law that goes all the way back to *Marbury v. Madison* (1803) that "Numerous statutes, rules, and cases reflect the understanding that the Judiciary cannot carry out its essential function if lawyers, parties, or witnesses obscure the facts."

Skewering the FBI, U.S. District Judge Cormac J. Carney wrote that while "The Government contends that the FOIA permits it to provide the Court with the same misinformation it provided to Plaintiffs regarding the existence of other responsive information or else the Government would compromise national security … that argument is indefensible."

Nevertheless, that court and the Ninth Circuit Court of Appeals *still* held that despite the Bureau's obvious attempt to bamboozle the federal judiciary, thus subverting the separation of powers amongst the three co-equal branches of government as stipulated in the U.S. Constitution (Article III), "disclosing the number and nature of the documents the Government possesses could reasonably be expected to compromise national security." (see: ***Islamic Shura Council of S. California v. FBI***.)

In other words, while the Bureau was chastised for withholding relevant documents from the court that might demonstrate their illegal surveillance of organizations and individuals who have *never* been indicted, or even charged, with so-called "terrorism offenses," the "national security" card trumps everything.

Electronic Surveillance

Late last month, EFF staff attorney Jennifer Lynch **reported** the group had "recently received documents from the FBI that reveal details about the depth of the agency's electronic surveillance capabilities and call into question the FBI's controversial effort to push Congress to expand the Communications Assistance to Law Enforcement Act (CALEA) for greater access to communications data."

The documents were obtained under a FOIA request by EFF after a 2007 report published by ***Wired*** disclosed that the FBI had deployed "secret spyware" to track domestic targets.

According to *Wired*, "FBI agent Norman Sanders describes the software as a 'computer and internet protocol address verifier,' or CIPAV."

In a follow-up **piece**, investigative journalist Ryan Singel revealed that the FBI "has quietly built a sophisticated, point-and-click surveillance system that performs instant wiretaps on almost any communications device."

That surveillance system known as DCSNet, or Digital Collection System Network, formerly known as Carnivore, "connects FBI wiretapping rooms to switches controlled by traditional land-line operators, internet-telephony providers and cellular companies," *Wired* reported.

"It is far more intricately woven into the nation's telecom infrastructure than observers suspected," Singel wrote at the time, a point underscored a year later when whistleblower **Babak Pasdar** blew the lid off the close relations amongst America's telecoms and the Bureau's illegal surveillance programs.

As ***Antifascist Calling*** reported at the time, a telecom carrier Pasdar worked for as a security consultant, subsequently named as Verizon by ***The Washington Post***, said the company maintained a high-speed DS-3 digital line that allowed the Bureau and other security agencies "unfettered" access to the carrier's wireless network, including billing records and customer data "transmitted wirelessly."

While Verizon denied the report that the FBI has open access to its network, their mendacious claims were demolished when the secrecy-shredding web site **Cryptome** published the firm's **"Law Enforcement Legal Compliance Guide"** in 2010.

Amongst the "helpful hints" provided to law enforcement by the carrier, Verizon urges state spies to "be specific."

"Do not include wording such as 'any and all records'", we read. "The courts have traditionally ruled that this wording is considered overly broad and burdensome. Request only what is required." On and on it goes…

According to documents obtained by EFF, the technologies discussed by Bureau snoops, when installed on a target's computer, allows the FBI to collect the following:

* IP Address

* Media Access Control (MAC) address

* "Browser environment variables"

* Open communication ports

* List of the programs running

* Operating system type, version, and serial number

* Browser type and version

* Language encoding

* The URL that the target computer was previously connected to

* Registered computer name

* Registered company name

* Currently logged in user name

* Other information that would assist with "identifying computer users, computer software installed, [and] computer hardware installed" (Electronic Frontier Foundation, *New FBI Documents Provide Details on Government's Surveillance Spyware*, April 29, 2011)

According to initial reporting by *Wired*, the FBI may have infiltrated the malicious program onto a target's computer by "pointing to code that would install the spyware by exploiting a vulnerability in the user's browser."

Lynch comments that "although the documents discuss some problems with installing the tool in some cases, other documents note that the agency's Crypto Unit only needs 24-48 hours to prepare deployment."

Once the tool is installed, Bureau snoops aver "it stay[s] persistent on the compromised computer and … every time the computer connects to the Internet, [FBI] will capture the information associated with the PRTT [**Pen Register/Trap & Trace Order**]."

The privacy watchdogs write that the Bureau "has been using the tool in domestic criminal investigations as well as in **FISA cases**, and the FISA Court appears to have questioned the **propriety** of the tool."

This is particularly relevant, and troubling, considering that the FBI and other secret state agencies such as the CIA and NSA already possess formidable surveillance tools in their arsenals and that private security outfits such as HBGary and Palantir–as well as *hundreds of other firms*–are busily concocting ever-more intrusive spyware for their state and private partners, as the massive disclosure of internal HBGary emails and documents by the cyber-guerrilla group **Anonymous** revealed.

With all the hot air from Washington surrounding claims by the FBI and other secret state satrapies that they'll "go dark" unless Congress grants them authority to build secret backdoors into America's communications networks, EFF revealed that documents "show the FBI already has numerous tools available to surveil suspects directly, rather than through each of their communications service providers."

"One heavily redacted **email** notes that the FBI has other tools that 'provide the functionality of the CIPAV [text redacted] as well as provide other useful info that could help

further the case'."

What is clear from the latest document release is that it isn't the FBI that's "going dark" but the right of the American people to free speech and political organizing without the threat that government-sanctioned malware which remains "persistent" on a "compromised computer" becomes one more tool for building "national security" dossiers on dissidents.

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****,* ***The Intelligence Daily****,* ***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.*

Articles by: **Tom Burghardt**
http://antifascist-calling.blogspot.com/