GlobalResearch
Center for Research on Globalization

Big Brother FBI

Data-Mining Programs Resurrect "Total Information Awareness"

By Tom Burghardt
Global Research, October 08, 2009
Antifascist Calling 4 October 2009
Region: USA
Theme: Intelligence

Like a vampire rising from it's grave each night to feed on the privacy rights of Americans, the Federal Bureau of Investigation is moving forward with programs that drain the life blood from our constitutional liberties.

From the wholesale use of informants and provocateurs to stifle political dissent, to Wi-Fi hacking and viral computer spyware to follow our every move, the FBI has turned massive data-mining of personal information into a growth industry. In the process they are building the surveillance state long been dreamed of by American securocrats.

A chilling new report by investigative journalist Ryan Singel provides startling details of how the FBI's National Security Branch Analysis Center (NSAC) is quietly morphing into the Total Information Awareness (TIA) system of convicted Iran-Contra felon, Admiral John M. Poindexter. According to documents obtained by Wired:

> A fast-growing FBI data-mining system billed as a tool for hunting terrorists is being used in hacker and domestic criminal investigations, and now contains tens of thousands of records from private corporate databases, including car-rental companies, large hotel chains and at least one national department store. (Ryan Singel, "FBI's Data-Mining System Sifts Airline, Hotel, Car-Rental Records," Wired, September 23, 2009)

Among the latest revelations of out-of-control secret state spookery, *Wired* disclosed that personal details on customers have been provided to the Bureau by the Wyndham Worldwide hotel chain "which includes Ramada Inn, Days Inn, Super 8, Howard Johnson and Hawthorn Suites." Additional records were obtained from the Avis rental car company and Sears department stores.

Singel reports that the Bureau is planning a massive expansion of NSAC, one that would enlarge the scope, and mission, of the Foreign Terrorist Tracking Task Force (FTTTF) and the file-crunching, privacy-killing Investigative Data Warehouse (IDW).

"Among the items on its wish list," Singel writes, "is the database of the Airlines Reporting Corporation–a company that runs a backend system for travel agencies and airlines." If federal snoops should obtain ARC's data-sets, the FBI would have unlimited access to "billions of American's itineraries, as well as the information they give to travel agencies, such as date of birth, credit card numbers, names of friends and family, e-mail addresses, meal preferences and health information."

The publication reports that the system "is both a meta-search engine–querying many data

sources at once–and a tool that performs pattern and link analysis." Internal FBI documents reveal that despite growing criticism of the alleged "science" of data-mining, including a stinging 2008 report by the prestigious National Research Council, for all intents and purposes the Bureau will transform NSAC into a low-key version of Adm. Poindexter's Information Awareness Office. An internal FBI document provides a preview of the direction NSAC will take.

> According to the General Accounting Office (GAO) May 2004 report on federal data mining efforts, the GAO defined data mining as "the application of database technology–to uncover hidden patterns and subtle relationships in data and to infer rules that allow for the prediction of future results" (GAO-05-866, Data Mining p. 4). There are a number of security and privacy issues that government and private industry must address when contemplating the use of technology and data in these ways. While the current activities and efforts of the IDW and FTTTF programs do not provide NSB [National Security Branch] users with the full level of data mining services as defined above it is the intention of the NSAC to pursue and refine these capabilities where permitted by statute and policy. The implementation and responsible utilization of these services will advance the FBI's ability to address national security threats in a timely fashion, uncover previously unknown patterns and trends and empower agents and analysts to better "hunt between the cases" to find those persons, places or things of investigative and intelligence interest. (Federal Bureau of Investigation, "Fiscal Year (FY) 2008, Internal Planning & Budget Review, Program Narrative for Enhancements/Increases," p. 5, emphasis added)

Unsurprisingly, in their quest for increased funding FBI officials failed to mention that the 2004 GAO report raised significant and troubling questions glossed over by securocrats. To wit, GAO investigators averred:

> Privacy concerns about mined or analyzed personal data also include concerns about the quality and accuracy of the mined data; the use of the data for other than the original purpose for which the data were collected without the consent of the individual; the protection of the data against unauthorized access, modification, or disclosure; and the right of individuals to know about the collection of personal information, how to access that information, and how to request a correction of inaccurate information. (General Accounting Office, Data Mining: Federal Efforts Cover a Wide Range of Uses, GAO-04-548, May 2004)

Despite these concerns, an FBI budget document released to Wired baldly states:

> The NSAC will provide subject-based "link analysis" through utilization of the FBI's collection data sets, combined with public records on predicated subjects. Link analysis uses these data sets to find links between subjects, suspects, and addresses or other pieces of relevant information, and other persons, places, and things. This technique is currently being used on a limited basis by the FBI; the NSAC will provide improved processes and greater access to this technique to all NSB components. The NSAC will also pursue "pattern analysis" as part of its service to the NSB. "Pattern analysis" queries take a predictive model or pattern of behavior and search for that pattern in data sets. The FBI's efforts to define predictive models and patterns of behavior should improve efforts to identify "sleeper cells." Information produced through data exploitation will be processed by analysts who are experts in the use of this information and used

> to produce products that comply with requirements for the proper handling of the information. (Federal Bureau of Investigation, "National Security Branch Analytical Capabilities," November 12, 2008)

Four years after the GAO report cited the potential for abuse inherent in such techniques, The National Research Council's exhaustive study criticized the alleged ability of data-miners to discover hidden "patterns" and "trends" among disparate data-sets "precisely because so little is known about what patterns indicate terrorist activity; as a result, they are likely to generate huge numbers of false leads."

False leads that may very well land an innocent person on a terrorist watch-list or as a subject of a wide-ranging and unwarranted national security investigation. But as with all things relating to "counterterrorism," the guilt or innocence of the average citizen is a trifling matter while moves to "empower agents" to "find those persons, places or things of investigative and intelligence interest," is the paramount goal. "Justice" under such a system becomes another preemptive "tool" subject to the whims of our political masters.

The use of federal dollars for such a dubious and questionable enterprise has already had real-world consequences for political activists. Just ask RNC Welcoming Committee activists currently under indictment in Minnesota for their role in organizing legal protests against the far-right Republican National Convention last year in St. Paul.

As Antifascist Calling revealed earlier this year, one private security outfit, the now-defunct Highway Watch which worked closely with the FBI, used "social network theory" and "link analysis," and cited the group's legal political organizing, including "increased membership via the internet" and "public appearances at various locations across the US," as a significant factor that rendered the group a "legitimate" target for heightened surveillance and COINTELPRO-style disruption.

Singel also disclosed that NSAC shared data "with the Pentagon's controversial Counter-Intelligence Field Activity office, a secretive domestic-spying unit which collected data on peace groups, including the Quakers, until it was shut down in 2008. But the FBI told lawmakers it would be careful in its interactions with that group."

As journalists and congressional investigators subsequently revealed however, CIFA's dark heart–the office's mammoth databases–were off-loaded to other secret state security agencies, including the FBI.

CIFA: Closed Down or Farmed Out?

When CIFA ran aground after a series of media disclosures beginning in 2004, some critics believed that was the end of that. "From the beginning of its existence," investigative journalist Tim Shorrock revealed in Spies For Hire, "CIFA had extensive authority to conduct domestic counterintelligence."

Indeed, one CIFA official "was the deputy director of the FBI's multiagency Foreign Terrorist Tracking Task Force," Shorrock wrote, "and other CIFA officials were assigned to more than one hundred regional Joint Terrorism Task Forces where they served with other personnel from the Pentagon, as well as the FBI, state and local police, and the Department of Homeland Security."

Several investigative reports in Antifascist Calling have documented the close interconnections among Pentagon spy agencies, the FBI, DHS, private contractors, local and state police in what have come to be known as fusion centers, which rely heavily on extensive data-mining operations.

Their role as clearinghouses for domestic intelligence will expand even further under President Obama's purported "change" administration.

Federal Computer Week revealed September 30, that DHS "is establishing a new office to coordinate its intelligence-sharing efforts in state and local intelligence fusion centers."

According to the publication, a "new Joint Fusion Center Program Management Office will be part of DHS' Office of Intelligence and Analysis, [DHS Secretary Janet] Napolitano told the Senate Homeland Security and Governmental Affairs Committee. Napolitano said she strongly supports the centers."

Though little reported by the corporate media, domestic spying had become big business with some very powerful constituencies.

Take CIFA, for example. Ostensibly a Defense Department agency, the secretive office which once had a multi-billion dollar budget at its disposal, was a veritable cash cow for enterprising security grifters. Much has been made of the corrupt contracts forged by disgraced Pentagon contractor Mitchell Wade and his MZM corporation, caught up in the "Duke" Cunningham scandal that landed the San Diego Republican congressman an eight-year federal prison term in 2006. Untouched however, by the outcry over domestic Pentagon spying were top-flight defense and security firms who lent their considerable resources–at a steep price–to the office.

Among the corporations who contracted out analysts and operatives to CIFA were heavy hitters such as Lockheed Martin, Carlyle Group subsidiary U.S. Investigations Services, Analex, Inc., an intelligence contractor owned by the U.K.'s QinetiQ, ManTech International, the Harris Corporation, SRA International, as well as General Dynamics, CACI International and the Science Applications International Corporation (SAIC). All told, these corporations reap tens of billions of dollars annually in federal largesse.

As Shorrock revealed, by 2006 CIFA "had four hundred full-time employees and eight hundred to nine hundred contractors working for it." Many were military intelligence and security analysts who jumped ship to land lucrative six-figure contracts in the burgeoning homeland security market, as the whistleblowing web site Wikileaks revealed in July when they published a massive 1525-page file on just one fusion center.

Information illegally obtained on American citizens by CIFA came to reside in the office's Threat And Local Observation Notice (TALON) system and a related database known as CORNERSTONE.

In 2007, the National Security Archive published Pentagon documents outlining U.S. Northern Command's (USNORTHCOM) extensive surveillance activities that targeted legal political protests organized by antiwar activists. In April 2007, Undersecretary of Defense for Intelligence, Lt. General James Clapper, "reviewed the results of the TALON program" and concluded "he did not believe they merit continuing the program as currently constituted."

Despite revelations that CIFA and USNORTHCOM had illegally conducted prohibited activities

in violation of the Posse Comitatus Act, which restricts the military from carrying out domestic law enforcement, not a single operative or program manager was brought to book. According to The National Security Archive:

> In June 2007, the Department of Defense Inspector General released the results of his review of the TALON reporting program. Its findings included the observation that CIFA and the Northern Command "legally gathered and maintained U.S. person information on individuals or organizations involved in domestic protests and demonstrations against DOD"–information gathered for law enforcement and force protection purposes as permitted by Defense Department directive (5200.27) on the "Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense." However, CIFA did not comply with the 90-day retention review policy specified by that directive and the CORNERSTONE database did not have the capability to identify TALON reports with U.S. person information, to identify reports requiring a 90-day retention review, or allow analysts to edit or delete the TALON reports.
>
> In August the Defense Department announced that it would shut down the CORNERSTONE database on September 17, with information subsequently collected on potential terror or security threats to Defense Department facilities or personnel being sent to an FBI data base known as GUARDIAN. A department spokesman said the database was being terminated because "the analytical value had declined," not due to public criticism, and that the Pentagon was hoping to establish a new system–not necessarily a database–to "streamline" threat reporting, according to a statement released by the Department's public affairs office. (Jeffrey Richelson, "The Pentagon's Counterspies: The Counterintelligence Field Activity," The National Security Archive, September 17, 2007)

Last year Antifascist Calling reported that when CIFA was shut down, that organization's TALON database was off-loaded to the Defense Intelligence Agency's Defense Counterintelligence and Human Intelligence Center and the FBI's GUARDIAN database that resides in the Bureau's Investigative Data Warehouse (IDW).

The IDW is a massive repository for data-mining. As I reported in May, citing the Electronic Frontier Foundation's revelations, the IDW possesses something on the order of 1.5 billion searchable files. In comparison, the entire Library of Congress contains 138 million unique documents.

EFF has called the IDW "the FBI's single largest repository of operational and intelligence information."

In 2005, FBI Section Chief Michael Morehart said that "IDW is a centralized, web-enabled, closed system repository for intelligence and investigative data." Unidentified FBI agents have described it as "one-stop shopping" for FBI agents and an "uber-Google." According to the Bureau, "[t]he IDW system provides data storage, database management, search, information presentation, and security services."

As the Wired investigation reveals, NSAC intends to expand these data-mining capabilities. Currently, NSAC employs "103 full-time employees and contractors, and the FBI was seeking budget approval for another 71 employees, plus more than $8 million for outside contractors to help analyze its growing pool of private and public data." Long-term, according to a planning document, the FBI "wants to expand the center to 439 people."

While John Poindexter's Total Information Awareness program may have disappeared along with the Bush administration, it's toxic heart lives on in the National Security Branch Analysis Center.

TIA, IDW, NSAC: What's in an Acronym? Plenty!

When the Pentagon's Defense Advanced Research Project Agency (DARPA) stood up the Information Awareness Office in 2002, the office's stated mission was to gather as much information on American citizens as possible and store it in a centralized, meta-database for perusal by secret state agencies.

Information included in the massive data-sets by IAO included internet activity, credit card purchase histories, airline ticket purchases and travel itineraries, rental car records, medical histories, educational transcripts, driver's licenses, social security numbers, utility bills, tax returns, indeed any searchable record imaginable.

As Wired reported, these are the data-sets that NSAC plans to exploit.

When Congress killed the DARPA program in 2004, most critics believed that was the end of the Pentagon's leap back into domestic intelligence. However, as we have since learned, the data-mining portion of the program was farmed out to a host of state agencies, including the National Security Agency, the Defense Intelligence Agency and the FBI.

Needless to say, private sector involvement–and lucrative contracts–for TIA projects included usual suspects such as Booz Allen Hamilton, Lockheed Martin, Raytheon, The Analysis Group and SAIC, as well as a number of low-key firms such as 21st Century Technologies, Inc., Evolving Logic, Global InfoTech, Inc., and the Orwellian-sounding Fund For Peace.

These firms, and many more, are current NSAC contractors; to all intents and purposes TIA now resides deep inside the Bureau's Investigative Data Warehouse and NSAC's Foreign Terrorist Tracking Task Force.

While the FBI claims that unlike TIA, NSAC is not "open-ended" and that a "mission is usually begun with a list of names or personal identifiers that have arisen during a threat assessment, preliminary or full investigation," Wired reports that "the FBI's pre-crime intentions are much wider that the bureau acknowledged."

This will inevitably change–and not for the better–as NSAC expands its brief and secures an ever-growing mountain of data at an exponential rate. In this endeavor, they will be aided by the U.S. Senate.

With three provisions of the draconian Patriot Act set to expire at years' end, the Senate Judiciary Committee, chaired by Sen. Patrick Leahy (D-VI) and Sen. Dianne Feinstein (D-CA), a member of the committee and chairwoman of the powerful Senate Intelligence Committee, stripped-away privacy protections to proposed legislation that would extend the provisions.

Caving-in to pressure from the FBI which claims that protecting Americans' privacy rights from out-of-control spooks would jeopardize "ongoing" terror investigations, Leahy gutted the safeguards he had espoused just last week!

Claiming that his own proposal might hinder open-ended "terror" investigations Leahy said at the hearing, "I'm trying to introduce balances on both sides." The original amendment would have curtailed Bureau fishing expeditions and would have required an actual connection of investigated parties to terrorism or foreign espionage.

Leahy was referring to Section 215 of the Patriot Act that allows the secretive Foreign Intelligence Surveillance Court (FISC) to authorize broad warrants for nearly any type of record, including those held by banks, libraries, internet service providers, credit card companies, even doctors of "persons of interest."

An amendment offered by Sen. Richard Durbin (D-IL) to repeal the Leahy-Feinstein amendment was defeated in committee by a 4-15 vote. As the Senator from the FBI, Feinstein said that the Bureau did not support Durbin's amendment. "It would end several classified and critical investigations," she said. Or perhaps Durbin's amendment would have lowered the boom on a host of illegal programs across the 16-agency U.S. "Intelligence Community."

As Antifascist Calling reported in July, a 38-page declassified report by inspectors general of the CIA, NSA, Department of Justice, Department of Defense and the Office of National Intelligence collectively called the acknowledged "Terrorist Surveillance Program" and cross-agency top secret "Other Intelligence Activities" the "President's Surveillance Program," PSP.

The IG's report failed to disclose what these programs actually did, and probably still do today under the Obama administration. Shrouded beneath impenetrable layers of secrecy and deceit, these undisclosed programs lie at the dark heart of the state's war against the American people.

The Department of Justice's Office of Inspector General (OIG) described FBI participation in the PSP as that of a passive "recipient of intelligence collected under the program" and efforts by the Bureau "to improve cooperation with the NSA to enhance the usefulness of PSP-derived information to FBI agents."

The OIG goes on to state that "further details about these topics are classified and therefore cannot be discussed here." As The New York Times revealed earlier this year in April and June, the NSA's STELLAR WIND and PINWALE internet and email text intercept programs are giant data-mining meta-databases that sift emails, faxes, and text messages of millions of people in the United States.

Far from being mere passive spectators, the FBI's Investigative Data Warehouse continues to be a major recipient of NSA's STELLAR WIND and PINWALE programs. As Marc Ambinder reported in The Atlantic PINWALE is "an unclassified proprietary term used to refer to advanced data-mining software that the government uses. Contractors who do SIGINT mining work often include a familiarity with Pinwale as a prerequisite for certain jobs."

As the Electronic Frontier Foundation's report on the IDW revealed, the FBI closely worked with SAIC, Convera and Chiliad to develop the project. Indeed, as EFF discovered "The FBI set up an Information Sharing Policy Group (ISPG), chaired by the Executive Assistant Directors of Administration and Intelligence, to review requests to ingest additional datasets into the IDW, in response to Congressional 'privacy concerns that may arise from FBI engaging in 'data mining.' In February 2005, the Counterterrorism Division asked for 8 more

data sources.” The names of the data sources were redacted in three of the eight datasets reviewed by EFF while three came from the Department of Homeland Security.

All of which begs the question: what is the FBI hiding behind it’s reorganization of the FTTTF and IDW into the National Security Branch Analysis Center? What role does the National Security Agency and private contractors play in standing-up NSAC? And why, as EFF disclosed, is the Bureau fearful of including Privacy Impact Assessments (PIAs) that might raise “congressional consciousness levels and expectations” in the context of Bureau “national security systems”?

Indeed, as the American Civil Liberties Union stated, “once again, the FBI has been found to be using invasive ‘counterterrorism’ tools to collect personal information about innocent Americans,” and it “appears that the FBI has continued its habit of gathering bulk amounts of personal information with little or no oversight.”

Not that congressional grifters and their corporate cronies, who have much to gain from billions of federal dollars pumped into these intrusive programs, actually care to explore what becomes of data illegally collected on innocent Americans by NSAC.

The civil liberties watchdog concludes they have “long suspected that the congressional dissent over and public demise of the Pentagon’s TIA program would result in a concealed and more invasive version of the program.”

Plus ça change, plus c’est la même chose. Somewhere near Washington Admiral Poindexter is leaning back in his chair, filling his pipe and smiling…

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