Democracy Going Dark: The Electronic Police State

The FBI's Multi-Billion "High-Tech Surveillance" Program

By Tom Burghardt
Global Research, May 21, 2009
Antifascist Calling... 21 May 2009

Region: USA
Theme: Police State & Civil Rights

The Federal Bureau of Investigation's **budget request** for Fiscal Year 2010 reveals that America's political police intend to greatly expand their high-tech surveillance capabilities.

According to ***ABC News***, the FBI is seeking additional funds for the development of "a new 'Advanced Electronic Surveillance' program which is being funded at $233.9 million for 2010. The program has 133 employees, 15 of whom are agents."

Known as "Going Dark," the program is designed to beef up the Bureau's already formidable electronic surveillance, intelligence collection and evidence gathering capabilities "as well as those of the greater Intelligence Community," *ABC* reports. An FBI spokesperson told the network:

> "The term 'Going Dark' does not refer to a specific capability, but is a program name for the part of the FBI, Operational Technology Division's (OTD) lawful interception program which is shared with other law enforcement agencies."
>
> "The term applies to the research and development of new tools, technical support and training initiatives." (Jason Ryan, "DOJ Budget Details High-Tech Crime Fighting Tools," ABC News, May 9, 2009)

Led by Assistant Director Marcus C. Thomas, OTD **describes** the office as supporting "the FBI's investigative and intelligence-gathering efforts–and those of our federal, state, and local law enforcement/intelligence partners–with a wide range of sophisticated technological equipment, examination tools and capabilities, training, and specialized experience. You won't hear about our work on the evening news because of its highly sensitive nature, but you will continue to hear about the fruits of our labor…"

According to OTD's **website**, the Division possesses "seven core capabilities": Digital Forensics; Electronic Surveillance; Physical Surveillance; Special Technology and Applications; Tactical Communications; Tactical Operations and finally, Technical Support/Coordination.

Under the heading "Electronic Surveillance," OTD deploys "tools and techniques for performing lawfully-authorized intercepts of wired and wireless telecommunications and data network communications technologies; enhancing unintelligible audio; and working with the communications industry as well as regulatory and legislative bodies to ensure that our continuing ability to conduct electronic surveillance will not be impaired as technology evolves."

But as we have seen throughout the entire course of the so-called “war on terror,” systemic constitutional breeches by the FBI–from their abuse of **National Security Letters**, the proliferation of corporate-dominated **Fusion Centers** to the infiltration of **provocateurs** into antiwar and other dissident groups–the only thing “impaired” by an out-of-control domestic spy agency have been the civil liberties of Americans.

Communications Backdoor Provided by Telecom Grifters

While the Bureau claims that it performs “lawfully-authorized intercepts” in partnership with the “communications industry,” also known as telecommunications’ **grifters**, the available evidence suggests otherwise.

As *Antifascist Calling* **reported** last year, security consultant and whistleblower Babak Pasdar, in a sworn **affidavit** to the Government Accountability Project (**GAP**), provided startling details about the collusive–and **profitable** alliance–between the FBI and America’s wireless carriers.

Pasdar furnished evidence that FBI agents have instantly transferred data along a high-speed computer circuit to a Bureau technology office in Quantico, Virginia. The so-called Quantico Circuit was provided to the FBI by Verizon, ***The Washington Post*** revealed.

According to published reports, the company maintains a 45 megabit/second DS-3 digital line that allowed the FBI and other security agencies virtually “unfettered access” to the carrier’s wireless network, including billing records and customer data “transferred wirelessly.” Verizon and other telecom giants have supplied FBI technical specialists with real-time access to customer data.

“The circuit was tied to the organization’s core network,” Pasdar wrote. Such access would expose customers’ voice calls, data packets, even their physical movements and geolocation to uncontrolled–and illegal–surveillance.

In April, *Wired* obtained **documents** from the FBI under a Freedom of Information Act request. Those files demonstrate how the Bureau’s “geek squad” routinely hack into wireless, cellular and computer networks.

Although the FBI released 152 heavily-redacted pages, they withheld another 623, claiming a full release would reveal a “sensitive investigative technique.” Nevertheless, *Wired* discovered that the FBI is deploying spyware called a “computer internet protocol address verifier,” or CIPAV, designed to infiltrate a target’s computer and gather a wide range of information, “which it sends to an FBI server in eastern Virginia.” While the documents do not detail CIPAV’s capabilities, an FBI affidavit from a 2007 case indicate it gathers and reports,

> a computer’s IP address; MAC address; open ports; a list of running programs; the operating system type, version and serial number; preferred internet browser and version; the computer’s registered owner and registered company name; the current logged-in user name and the last-visited URL.
>
> After sending the information to the FBI, the CIPAV settles into a silent “pen register” mode, in which it lurks on the target computer and monitors its internet use, logging the IP address of every server to which the machine connects. (Kevin Poulsen, “FBI Spyware Has Been Snaring Extortionists,

Hackers for Years," Wired, April 16, 2009)

"Going Dark" is ostensibly designed to help the Bureau deal with technological changes and methods to intercept Voice Over Internet Protocol (VOIP) phone calls facilitated by programs such as Skype. But a tool that can seamlessly target hackers and cyber-criminals can just as easily be deployed against political opponents.

The FBI also intends to continue their use of automated link- and behavioral analysis derived from data mining as investigative tools. As a subset of applied mathematics, social network theory and its derivatives, link- and behavioral analysis, purport to uncover hidden relationships amongst social groups and networks. Over time, it has become an invasive tool deployed by private- and state intelligence agencies against political activists, most recently, as *Antifascist Calling* reported in February, against protest groups organizing against the **Republican National Convention**.

These methods raise very troubling civil liberties' and privacy concerns. The Electronic Privacy Information Coalition (**EPIC**) filed a Freedom of Information Act **request**, demanding that the General Services Administration (**GSA**) turn over agency records "concerning agreements the GSA negotiated between federal agencies and social networking services, including Flickr, YouTube, Vimeo, Blip.tv, and Facebook."

With the proliferation of social networking sites, applications allow users to easily share information about themselves with others. But as EPIC points out, "Many online services relay information about online associations as users create new relationships. While government agencies may use social networking, cloud computing, and Internet services to create greater transparency on their activities, it remains unclear if there are data collection, use, and sharing limitations."

And with "information discoverability" all the rage amongst spooky security agencies ranging from the FBI to the NSA, "connecting the dots," particularly when it comes to dissident Americans, "is gaining increasing attention from homeland security officials and experts in their ongoing attempt to corral anti-terrorism information that resides across federal, state and local jurisdictions," *Federal Computer Week* **reports**.

Will an agreement between Facebook and the FBI facilitate "dot connecting" or will it serve as a new, insidious means to widen the surveillance net, building ever-more intrusive electronic case files on dissident Americans?

The Electronic Police State

As *Antifascist Calling* **reported** earlier this month, citing the Electronic Frontier Foundation's (**EFF**) **dossier** on the FBI's Investigative Data Warehouse (IDW), the office had "transitioned to the operations and maintenance phase during FY 2008" and now possesses some "997,368,450 unique searchable documents," ready for data mining.

But as study after study has revealed, most recently the comprehensive **examination** of various programs by the National Research Council, automated data mining is "likely to generate huge numbers of false leads."

Because the mountainous volumes of data "mined" for "actionable intelligence" are drawn from dozens of disparate sources on terrorism or criminal suspects, "they have an enormous potential for privacy violations because they will inevitably force targeted individuals to explain and justify their mental and emotional states."

EFF documented that the Bureau's Telephone Application (TA) "provides a central repository for telephone data obtained from investigations." TA allegedly functions as an "investigative tool … for all telephone data collected during the course of FBI investigations. Included are pen register data, toll records, trap/trace, tape-edits, dialed digits, airnet (pager intercepts), cellular activity, push-to-talk, and corresponding subscriber information."

Additionally, the civil liberties' group revealed that "records obtained through National Security Letters are placed in the Telephone Application, as well as the IDW by way of the ACS [Automated Case] system." It would appear that "Going Dark" will serve as a research subsystem feeding the insatiable appetite of the Investigative Data Warehouse.

In fact, these programs are part and parcel of what the security **website** *Cryptohippie* refers to as the **Electronic Police State**. Far from keeping us safe from all manner of dastardly plots hatched by criminals and/or terrorists, *Cryptohippie* avers:

> An electronic police state is quiet, even unseen. All of its legal actions are supported by abundant evidence. It looks pristine.
>
> An electronic police state is characterized by this:
>
> **State use of electronic technologies to record, organize, search and distribute forensic evidence against its citizens.**
>
> The two crucial facts about the information gathered under an electronic police state are these:
>
> 1. It is criminal evidence, ready for use in a trial.
>
> 2. It is gathered universally and silently, and only later organized for use in prosecutions.
>
> In an Electronic Police State, 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. ("The Electronic Police State, 2008 National Rankings," Cryptohippie, no date)

Unfortunately, this is not the stuff of paranoid fantasies, but American reality in the year 2009; one unlikely to change in the foreseeable future.

In addition to "Going Dark," the FBI is busily constructing what *ABC News* refers to as the "development of the Biometric Technology Center, a Joint Justice, FBI and DoD program." At a cost of $97.6 million, the center will function as a research and development arm of the Bureau's Biometric Center of Excellence (**BCOE**), one which will eventually "be a vast database of personal data including fingerprints, iris scans and DNA which the FBI calls the Next Generation Identification (NGI)."

The program is closely tied with technology under development by West Virginia

University's Center for Identification Technology Research (**CITeR**). As the FBI's "lead academic partner in biometrics research" according to a Bureau **press release**, CITeR provides "biometrics research support to the FBI and its law enforcement and national security partners and serve as the FBI liaison to the academic community of biometric researchers nationwide."

Indeed, CITeR director Lawrence A. Hornak, "a visionary of the Big Brother school of technology" told ***The Register***, he awaits the day "when devices will be able to 'recognize us and adapt to us'." The "long-term goal," Hornak declared, is the "ubiquitous use of biometrics."

But as *The Register* pointed out when the program was publicly rolled-out, "civil libertarians and privacy advocates are not amused."

> They claim that the project presents nightmare scenarios of stolen biometric information being used for ever-more outlandish forms of identity theft, which would be nearly impossible to correct. Correcting an inaccurate credit report is already an insulting and hair-raising experience in America, and critics contend that the use of biometrics would make correcting inaccurate credit reports or criminal histories nearly impossible. Besides, they argue, the US government does not exactly have a sterling record when it comes to database security–what happens when, as seems inevitable, the database is hacked and this intimate and allegedly indisputable data is compromised? …
>
> Databases usually become less accurate, rather than more, the older and bigger they get, because there's very little incentive for the humans that maintain them to go back and correct old, inaccurate information rather than simply piling on new information. Data entry typically trumps data accuracy. Furthermore, the facial recognition technology in its current iteration is woefully inaccurate, with recognition rates as low as 10 per cent at night. All in all, there is ample reason for skepticism–not that it will make much of a difference. (Burke Hansen, "FBI preps $1bn biometric database," The Register, December 24, 2007)

But WVU's CITeR isn't the only partner lining-up to feed at the FBI's trough. *ABC* reports that the Bureau "has awarded the NGI contract to Lockheed Martin to update and maintain the database which is expected to come online in 2010. After being fully deployed the NGI contract could cost up to $1 billion."

However, *Federal Computer Week* **reported** in 2008 that although the initial contract will "consist of a base year," the potential for "nine option years" means that "the value of the multiyear contract … could be higher." You can bet it will!

Additional firms on Lockheed Martin's "team" as subcontractors include IBM, Accenture, BAE Systems, Global Science & Technology, Innovative Management & Technology Services and Platinum Solutions. In other words, NGI is yet another in a gigantic herd of cash cows enriching the Military-Industrial-Security Complex.

Democracy "Going Dark"

The "vast apparatus of domestic spying" described by the ***World Socialist Web Site***, greatly expanded under the criminal Bush regime is a permanent feature of the capitalist state; one that will continue to target political dissent during a period of profound economic crisis.

That the Obama administration, purportedly representing fundamental change from the previous government, has embraced the felonious methods of the Bush crime family and its *capo tutti capo*, Richard Cheney, should surprise no one. Like their Republican colleagues, the Democrats are equally complicit in the antidemocratic programs of repression assembled under the mendacious banner of the "global war on terror."

From warrantless wiretapping to the suppression of information under cover of state secrets, and from the waging of imperialist wars of conquest to torture, the militarist mind-set driving capitalist elites at warp speed towards an abyss of their own creation, are signs that new political provocations are being prepared by America's permanent "shadow government"–the military-intelligence-corporate apparatus.

***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**, an independent research and media group of writers, scholars, journalists and activists based in Montreal, his articles can be read on **Dissident Voice**, **The Intelligence Daily**, **Pacific Free Press** and the whistleblowing website **Wikileaks**. He is the editor of Police State America: U.S. Military "Civil Disturbance" Planning, distributed by **AK Press**.*

The original source of this article is Antifascist Calling...

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

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

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

For media inquiries: publications@globalresearch.ca