GlobalResearch
Center for Research on Globalization

Spying on Americans: The FBI's "Quantico Circuit" — Still Spying, Still Lying

By Tom Burghardt
Global Research, April 09, 2008
Antifascist Calling... 9 April 2008

Region: USA
Theme: Police State & Civil Rights

Tuesday's ***Washington Post*** reports that FBI investigators "with the click of a mouse, [can] instantly transfer key data along a computer circuit to an FBI technology office in Quantico."

Last month I **wrote** that evidence of the Bureau's massive spying operations on Americans had been uncovered and "that a new FISA whistleblower has stepped forward with information about a major wireless provider apparently granting the state unrestricted access to all of their customers' voice communications and electronic data via a so-called 'Quantico Circuit'."

According to whistleblower **Babak Pasdar**, a telecom carrier he worked for as a security consultant, subsequently named as Verizon by the *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."

Verizon denied the report that the FBI has open access to its network; a denial belied by documents obtained by the San Francisco-based **Electronic Frontier Foundation** describing the Bureau's Digital Collection System.

When these allegations first surfaced they were stonewalled by major media. Nevertheless, the reports continued and we now have learned that electronic connections between major telecom firms and FBI personnel scattered across the country provide the Bureau with real-time access to who is speaking to whom, the time and duration of each call as well as the locations of those so targeted.

Despite half-hearted protests by Congress, the FBI's budget for these operations have increased significantly. According to *Post* reporter Ellen Nakashima,

> "The bureau says its budget for the collection system increased from $30 million in 2007 to $40 million in 2008. Information lawfully collected by the FBI from telecom firms can be shared with law enforcement and intelligence-gathering partners, including the National Security Agency and the CIA. Likewise, under guidelines approved by the attorney general or a court, some intercept data gathered by intelligence agencies can be shared with law enforcement agencies."(Ellen Nakashima, "FBI Transfers via Telecoms Questioned," The Washington Post, Tuesday, April 8, 2008; A03)

But who's "watching the watchers," or in this case, *the listeners*?

Since 1994, under rules mandated by the Communications Assistance for Law Enforcement Act (CALEA), passed by the "liberal" Clinton administration, federal rules are in place "to make clear a telecommunications carrier's duty to cooperate in the interception of communications for Law Enforcement purposes, and for *other purposes*." [emphasis added]

These rules specify that telecom carriers and manufacturers design their equipment, facilities and services so as to guarantee they have the necessary surveillance capabilities. This onerous piece of legislative flotsam specifies that common carriers, broadband internet access providers and providers of Voice Over Internet Protocol (VOIP) service are designated "telecommunications carriers" under federal law and thus, are capable of interception by the state's "security" bureaucracies. (For an historical analysis of CALEA's civil liberties implications see: "Big Brother in the Wires: Wiretapping in the Digital Age," **ACLU**, March 1, 1998)

The FBI has since created a network of links and electronic hubs for collection purposes amongst the nation's largest telecom carriers and internet providers "and about 40 FBI offices and Quantico, according to interviews and documents describing the agency's Digital Collection System," according to the *Washington Post*.

These revelations mirror those of AT&T whistleblower Mark Klein, who revealed that the super secretive National Security Agency had been given access by AT&T management to install "splitters" for the Agency hard-wired to an NSA "secure" room in the company's central office in San Francisco. According to **Klein**,

> "In short, an exact copy of all internet traffic that flowed through critical AT&T cables–emails, documents, pictures, web browsing, Voice over-internet phone conservations, everything–was being diverted to equipment inside the secret room. In addition the documents reveal the technological gear used in their secret project, including a highly sophisticated search component capable of quickly sifting through huge amounts of digital data (including text, voice and images) in real time according to pre-programmed criteria.
>
> It's important to understand that the internet links which were connected to the splitter contained not just foreign communications but vast amounts of domestic traffic, all mixed together. Furthermore, the splitter has no selective abilities–it's just a dumb device which copies everything to the secret room. And the links going through the splitter are AT&T's physical connections to many other internet providers (e.g., Sprint, Qwest, Global Crossing, Cable & Wireless, and the critical West Coast Internet Exchange Point known as Mae West). Since these networks are interconnected, the government surveillance affects not only AT&T customers but everyone else–millions of Americans.
>
> I also discovered in my conversations with other technicians that other "secret rooms" were established in Seattle, San Jose, Los Angeles and San Diego. One of the documents I obtained also mentions Atlanta, and the clear inference in the logic of this setup, and the language of the documents, is that there are other such rooms across the country to complete the coverage–possibly 15 to 20 or more." (Mark Klein, "Reject Amnesty for Telecoms," Electronic Frontier Foundation)

As a key networking hub of the national security state's electronic driftnet, the "Quantico circuit" enables the FBI and their CIA and NSA partners in crime to literally target any one or

any group with highly-intrusive and silent monitoring of all electronic communications. Under the Bush administration's repressive "public-private" police state architecture, privacy rights join Geneva Convention prohibitions against torture as yet another "quaint" notion, a "phantom of lost liberty," in the memorable phrase uttered by former U.S. Attorney General John Ashcroft in 2001.

While the Bureau claims that the content of a phone call or e-mail must be authorized by a court order showing "probable cause," as with other abusive FBI practices such as the issuance of so-called "national security letters" to obtain financial or other private records, the legal bar undoubtedly is set very low.

These latest revelations of FBI abuse of Fourth Amendment protections, follow on the heels of new initiatives undertaken by the Department of Homeland Security to utilize U.S. spy satellites for domestic "law enforcement and counterterrorism" investigations.

According to **Nick Juliano**,

> "DHS plans to create a new office that would expand law enforcement and other civilian agencies' access to data gathered by powerful intelligence and military satellites orbiting the earth. The National Applications Office [NAO] will oversee who can access such satellite data, which is typically used to monitor climate change and track hurricane damage, among other uses.
>
> DHS still has not laid out legal frameworks or standard operating procedures for the office, according to a letter from three members of the House Homeland Security Committee." (Nick Juliano, "DHS Ignores Civil Liberties in Domestic Spy Satellite Plan, Lawmakers Say," The Raw Story, Monday, April 7, 2008)

First floated last August, then delayed over civil liberties concerns, DHS is now moving full speed ahead with the project. In a letter to DHS Secretary Michael Chertoff, Reps. Bennie G. Thompson, Jane Harman and Christopher P. Carney wrote, "merely mentioning Posse Comitatus and other laws in the NAO Charter does not provide needed assurances that the Department will not transform NAO into a domestic spying platform."

Tepid protests by congressional Democrats who have systematically enabled these repressive measures by granting unlimited budgetary increases to Bushist spymasters, will have virtually no effect on an administration hell-bent on turning the entire country into a "free spy zone."

Tom Burghardt is a researcher and activist based in the San Francisco Bay Area. In addition to publishing in Covert Action Quarterly, Love & Rage and Antifa Forum, 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...
Copyright © Tom Burghardt, Antifascist Calling..., 2008

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

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca