Wiretaps “R” Us: Is the FBI Tracking Your Cellphone?

By Tom Burghardt
Global Research, June 14, 2008
Antifascist Calling... 14 June 2008

Region: USA
Theme: Police State & Civil Rights

Under broad powers handed the Federal Bureau of Investigation by Congress in 2001 after it passed the Orwellian USA Patriot Act, the rights of ordinary citizens have progressively been stripped away by America’s national security state.

With a history of domestic counterinsurgency operations against the **left**, and despite bruising attacks after **9/11** on its (undeserved) reputation as the nation’s premier “crime fighting agency,” the FBI nevertheless, remains a formidable organization when it comes to repressing dissent.

In this light, a disturbing report showcased Wednesday by ***Wired***, highlights the grave dangers posed to individual rights and freedoms when secretive and largely unaccountable federal bureaucracies are handed nearly unlimited powers. Ryan Singel writes:

Does the FBI track cellphone users’ physical movements without a warrant? Does the Bureau store recordings of innocent Americans caught up in wiretaps in a searchable database? Does the FBI’s wiretap equipment store information like voicemail passwords and bank account numbers without legal authorization to do so? (“Secret Spy Court Repeatedly Questions FBI Wiretap Network,” *Wired*, June 11, 2008)

According to Singel, during a series of inquiries in 2005-2006 the secretive Foreign Intelligence Surveillance Court repeatedly questioned the legality of Bureau electronic surveillance operations that targeted Americans. These revelations came to light in newly declassified documents obtained by the Electronic Frontier Foundation (**EFF**).

The spy court inquired whether the FBI was using so-called “pen register” orders to “collect digits dialed after a call is made, potentially including voicemail passwords and account numbers entered into bank-by-phone applications,” Singel writes.

Title 18 of the United States Code, as amended by the USA Patriot Act, defines a pen register and/or a trap and trace device as

...a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business.

Under existing federal statutes, the FBI can compel a telecom carrier to turn over records of whom a "target" has called simply by claiming the information is relevant to an on-going investigation. However, under interpretations of existing case law, *Wired* reports that "so-called 'post-cut-through dialed digits' count as the content of a communication, and thus to collect that information, the FBI would need to get a full-blown wiretapping warrant based on probable cause."

Coming on the heels of revelations of the FBI's abuse of so-called **National Security Letters** to obtain electronic and financial records during "terrorism investigations," the documents outline a systematic pattern by the Bureau to skirt the law. *Wired* reports,

Among other things, the declassified documents reveal that lawyers in the FBI's Office of General Counsel and the Justice Department's Office of Intelligence Policy Review queried FBI technology officials in late July 2006 about cellphone tracking. The attorneys asked whether the FBI was obtaining and storing real-time cellphone-location data from carriers under a "pen register" court order that's normally limited to records of who a person called or was called by.

You read that right: *real-time cellphone-location data from carriers*.

In 2006, Foreign Intelligence Surveillance Court judge Coleen Kollar-Kottely ordered the FBI to **report** how its phone wiretapping network known as Digital Collection System, handled information it obtained illegally and whether it stored them in its centralized data-mining repository known as Telephone Application. *Wired* further reports that FBI **documents** show that

the majority of FBI offices surveyed internally were collecting that information without full-blown wiretap orders, especially in classified investigations. The documents also indicate that the information was being uploaded to the FBI's central repository for wiretap recordings and phone records, where analysts can data-mine the records for decades.

According to EFF attorney Kevin Bankston, this demonstrates that FBI offices had reconfigured their "digit-recording software, DCS 3000, to collect more than the law allows."

In other words, despite prohibitions on the FBI's ability to spy on Americans, the Bureau is storing illegally-obtained data in a centralized data-mining "warehouse" for indefinite retrieval purposes, say, during a "state of national emergency" when the "usual suspects" can be "disappeared" under **Continuity of Government** plans already in place.

Lest there be any question that federal surveillance programs are concerned with far more than wiretapping alleged terrorists, National Security Presidential Directive 59/Homeland Security Presidential Directive 24 (**NSPD 59/HSPD 24**), "Biometrics for Identification and Screening to Enhance National Security," should clear up any lingering doubts.

Signed June 5, 2008 by President Bush,

This directive establishes a framework to ensure that Federal executive departments and agencies (agencies) use mutually compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information of individuals in a lawful and appropriate manner, while respecting their information privacy and other legal rights under United States law.

The executive branch has developed an integrated screening capability to protect the Nation against "known and suspected terrorists" (KSTs). The executive branch shall build upon this success, in accordance with this directive, by enhancing its capability to collect, store, use, analyze, and share biometrics to identify and screen KSTs and ***other persons who may pose a threat to national security****.* [emphasis added]

As analyst **Michel Chossudovsky** points out in a scathing critique of Bush's directive,

NSPD 59 goes far beyond the issue of biometric identification, it recommends the collection and storage of "associated biographic" information, meaning information on the private lives of US citizens, in minute detail, all of which will be "accomplished within the law." …

The directive uses 9/11 as an all encompassing justification to wage a witch hunt against dissenting citizens, establishing at the same time an atmosphere of fear and intimidation across the land. It also calls for the integration of various data banks as well as inter-agency cooperation in the sharing of information, with a view to eventually centralizing the information on American citizens. ("'Big Brother' Presidential Directive: 'Biometrics for Identification and Screening to Enhance National Security'," *Global Research*, June 11, 2008)

In other words, in addition to "known and suspected terrorists," presumably al-Qaeda and their minions, additional "potential threats" to the capitalist order are named: domestic "radical groups" and "disgruntled employees."

One needn't be a "conspiracy buff" to recognize–cooly and rationally–that the national security surveillance state under construction since before 9/11, can trace its lineage back to domestic counterinsurgency operations such as the FBI's COINTELPRO or "civil disturbance" contingency plans such as **NORTHCOM's** contemporaneous **"Garden Plot"** and **"Cable Splicer"** projects.

Cellphone and internet tracking, now ubiquitous after the USA Patriot Act, are but two of the repressive bricks shoring-up the decaying edifice of the corporatist American empire. In this light, it would be a fatal mistake to hope for ameliorating the erosion of our rights by relying on the Democratic party, or to believe that "change" in the form of an Obama presidency will somehow, magically perhaps, reverse ruling class consensus on this score.

Over the past decade, the Democrats and their "progressive" critics have stood idly by–or joined in the assault on democracy–as the sinister Bush regime hijacked a national election, launched an illegal war, systematically tortured prisoners, covered-up their criminal negligence, or worse, in the 9/11 attacks, while shredding the Bill of Rights.

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****.*

Become a Member of Global Research

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