GlobalResearch
Center for Research on Globalization

Spying on Americans: “Business as Usual” under Obama

NSA "engaged in 'overcollection' of domestic communications"

By Tom Burghardt
Global Research, April 19, 2009
Antifascist Calling... 19 April 2009

Region: USA
Theme: Police State & Civil Rights

New evidence that the National Security Agency (NSA) continues to systematically spy on Americans emerged on Thursday.

In an explosive **report**, *The New York Times* revealed that the agency “intercepted private e-mail messages and phone calls of Americans in recent months on a scale that went beyond the broad legal limits established by Congress last year.”

According to investigative journalists Eric Lichtblau and James Risen, “several intelligence officials” told the paper that the ultra-spooky NSA “had been engaged in ‘overcollection’ of domestic communications of Americans.”

As numerous critics have charged, the NSA’s driftnet surveillance of electronic communications would dramatically escalate precisely *because* of Congress’ passage of the shameful FISA Amendments Act (FAA) last summer.

When revelations that domestic spying have increased since Obama’s January inauguration are coupled with the Justice Department’s aggressive moves to suppress litigation that would hold former and present officials accountable, claims of “overcollection” by the agency become a code word for *business as usual*.

The *Times* points out that “classified government briefings have been held in recent weeks in response to a brewing controversy that some officials worry could damage the credibility of legitimate intelligence-gathering efforts.”

But as *The Wall Street Journal* **reported** last year, “the spy agency now monitors huge volumes of records of domestic emails and Internet searches as well as bank transfers, credit-card transactions, travel and telephone records.”

Acting in concert with private corporations, “transactional data” such as credit card purchases, bank transactions and travel itineraries are sold to NSA by corporate freebooters. Once this information is obtained, it is then fed into data mining programs, including NSA’s own Terrorist Surveillance Program or the FBI’s Digital Collection System formerly known as Carnivore in a quixotic search for “suspicious patterns.” As the *Journal* revealed:

The effort also ties into data from an ad-hoc collection of so-called “black programs” whose existence is undisclosed, the current and former officials say. Many of the programs in various agencies began years before the 9/11 attacks but have since been given greater

reach. Among them, current and former intelligence officials say, is a longstanding Treasury Department program to collect individual financial data including wire transfers and credit-card transactions. (Siobhan Gorman, "NSA Domestic Spying Grows as Agency Sweeps Up Data," *The Wall Street Journal*, March 10, 2008)

As investigative journalist Christopher Ketchum **reported** last year in the now-defunct *Radar Magazine*, one such "black program" may be its ultra top secret Main Core database, "a secret enemies list of citizens who could face detention under martial law."

Ketchum revealed that as many as "8 million Americans are now listed in Main Core as potentially suspect" and, in the event of a national emergency, "could be subject to everything from heightened surveillance and tracking to direct questioning and even detention."

According to investigative journalist Tim Shorrock, the author of the essential *Spies for Hire*, Main Core "reportedly collects and stores–without warrants or court orders–the names and detailed data of Americans considered to be threats to national security." A creature of so-called Continuity of Government **programs** that came on-line during the 1980s Iran-Contra affair, Main Core evolved from Inslaw's Prosecutors' Management Information System or PROMIS, a software program that can quickly sift through multiple databases.

William Hamilton, the president of Insalw, Inc. told Shorrock that Justice Department officials "appropriated" or stole, the software from Inslaw. "Hamilton claims that Reagan officials gave PROMIS to the NSA and the CIA, which then adapted the software–and its outstanding ability to search other databases–to manage intelligence operations and track financial transactions." According to *Salon*,

Through a former senior Justice Department official with more than 25 years of government experience, *Salon* has learned of a high-level former national security official who reportedly has firsthand knowledge of the U.S. government's use of Main Core. The official worked as a senior intelligence analyst for a large domestic law enforcement agency inside the Bush White House. He would not agree to an interview. But according to the former Justice Department official, the former intelligence analyst told her that while stationed at the White House after the 9/11 attacks, one day he accidentally walked into a restricted room and came across a computer system that was logged on to what he recognized to be the Main Core database. When she mentioned the specific name of the top-secret system during their conversation, she recalled, "he turned white as a sheet." (Tim Shorrock, "Exposing Bush's Historic Abuse of Power," *Salon*, July 23, 2008)

Typically, Obama's Justice Department, much like their predecessors in the criminal Bush regime, told *The New York Times* "there had been problems with the N.S.A. surveillance operation, but said they had been resolved."

In other words, move along!

Unsurprisingly, the NSA claimed that its "intelligence operations, including programs for collection and analysis, are in strict accordance with U.S. laws and regulations." True enough as far as it goes (which isn't very far!), since laws rubber-stamped by a compliant Congress have given the security and intelligence apparatus carte blanche to systematically rob us of our rights under color of "national security."

One would think that with revelations that the agency attempted to wiretap a member of Congress without court approval would light a fire under our representatives. You'd be wrong, however. Describing the virtual love-fest amongst congressional clock-punchers and spooks as a "contentious three-year debate," the *Times* avers:

Congress gave the N.S.A. broad new authority to collect, without court-approved warrants, vast streams of international phone and e-mail traffic as it passed through American telecommunications gateways. The targets of the eavesdropping had to be "reasonably believed" to be outside the United States. Under the new legislation, however, the N.S.A. still needed court approval to monitor the purely domestic communications of Americans who came under suspicion.

In recent weeks, the eavesdropping agency notified members of the Congressional intelligence committees that it had encountered operational and legal problems in complying with the new wiretapping law, Congressional officials said. (Eric Lichtblau and James Risen, "N.S.A.'s Intercepts Exceed Limits Set by Congress," *The New York Times*, April 16, 2009)

An agency official, anonymously of course, had the temerity to claim that the "overcollection" problem led the NSA to "inadvertently" target groups of American citizens, and that snooping, cataloguing and data mining private communications was merely a glitch best left to professionals to resolve!

But as the American Civil Liberties Union argued in an April 16 **press release**, Congress bears responsibility for its failure to curb aggressive spies-gone-wild and cites the FAA's passage as the primary culprit. Jameel Jaffer, the Director of the ACLU's National Security Project said:

> "These revelations are as alarming as they are predictable. The FAA set virtually no limits on the government's eavesdropping authority, but it appears that the NSA has disregarded even what minimal limits existed. The new law should have ensured that the government's surveillance powers would be subject to meaningful judicial oversight. Instead the new law allowed the NSA to operate without the safeguards that the Constitution requires. The Bush administration argued that the law was necessary to protect national security, but in fact the law implicates all kinds of communications that have nothing to do with terrorism or criminal activity of any kind. The law was ill-advised, and today's report only underscores that the law should be struck down as unconstitutional." ("NSA Spies on Americans Outside the Law," American Civil Liberties Union, Press Release, April 16, 2009)

As I **pointed out** last September,

> The FAA, a piece of Bushist legislative flotsam, was overwhelmingly approved by both houses of Congress and signed into law in July by president Bush. While the reputed "opposition" party, the Democrats, managed a few bleats against immunity provisions for lawbreaking corporate grifters, they quickly fell into line and passed this disgraceful statute. …
>
> The FAA gives the Bush–and future administrations–virtually unlimited power to intercept the emails and phone calls of American citizens and legal residents. Indeed, the new law hands the state the authority to conduct intrusive spying

> operations “without ever telling a court who it intends to spy on, what phone lines and email addresses it intends to monitor, where its surveillance targets are located, why it’s conducting the surveillance or whether it suspects any party to the communication of wrongdoing,” according to the ACLU. (“As ACLU Challenges FISA Law in Federal Court, Justice Department Moves to Immunize Spying Telecoms,” Antifascist Calling, September 17, 2009)

Well, that “future administration” is now the current regime. Isn’t “change” wonderful!

As I **reported** April 12 the Obama administration, drawing a page from the Bush/Cheney playbook, moved to squash the Electronic Frontier Foundation’s landmark ***Jewell v. NSA*** lawsuit, on the grounds of the state secrets privilege and the government’s alleged “sovereign immunity.”

Given these latest revelations, you’d think that NSA’s wings would be clipped by administration officials. You’d be wrong. On April 17, *The New York Times* **reported** that the “National Security Agency has been campaigning to lead the government’s rapidly growing cybersecurity programs, raising privacy and civil liberties concerns among some officials who fear that the move could give the spy agency too much control over government computer networks.”

One official, Rod Beckstrom, resigned in March as director of the Department of Homeland Security’s National Cyber Security Center citing “N.S.A.’s push for a greater role in guarding the government’s computer systems” as a reason for his resignation.

Beckstrom told the *Times*, “I have very serious concerns about the concentration of too much power in one agency. Power over information is so important, and it is so difficult to monitor, that we need to have checks and balances.”

While the Senate Intelligence Committee plans a “closed hearing on the issue soon,” and promises that “we will make sure we get the facts,” I wouldn’t hold my breath.

NSA has powerful allies in the Obama administration. Although agency officials declined to comment on the controversy, Obama’s Director of National Intelligence, Dennis C. Blair, a former admiral with extensive ties to the corporate security industry, recently told Congress he believed NSA should be given the lead in cybersecurity, arguing the agency has the computer “wizards” with the requisite skills.

And so it goes…

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****, 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****.*

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

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