GlobalResearch
Center for Research on Globalization

Telecom Companies in Cahoots with Illegal Bush Administration Surveillance Programs

By Tom Burghardt
Global Research, May 27, 2008
Antifascist Calling... 27 May 2008
Region: USA
Theme: Police State & Civil Rights

The hot-button issue of retroactive immunity for telecom companies in cahoots with illegal Bush administration surveillance programs is close to reaching its inevitable dénouement.

But what's gotten little media play throughout the endless months of "debate" are the huge piles of cash that have changed hands to influence congressional Democrats and Republicans.

According to **Glenn Greenwald**:

> Just in the first three months of 2008, recent lobbyist disclosure statements reveal that AT&T spent $5.2 million in lobbyist fees (putting it well ahead of its 2007 pace, when it spent just over $17 million). In the first quarter of 2008, Verizon spent $4.8 million on lobbyist fees, while Comcast spent $2.6 million. So in the first three months of this year, those three telecoms–which would be among the biggest beneficiaries of telecom amnesty (right after the White House)–spent a combined total of almost $13 million on lobbyists. They're on pace to spend more than $50 million on lobbying this year–just those three companies. ("How Telecoms Are Attempting to Buy Amnesty from Congress," Salon, May 24, 2008)

No matter how you squeeze it, that's a lot of corporatist "juice" flowing into campaign coffers.

Until, that is, you consider that "outsourced" government contracts are worth tens of billions of dollars annually to enterprising telecom companies for communications and IT services to a gaggle of shadowy intelligence agencies fighting to "keep America safe"–from lower quarterly earnings!

Ranging from the Central Intelligence Agency (CIA) and Federal Bureau of Investigation (FBI) to the Department of Homeland Security (DHS) and the National Security Agency (NSA), not to mention low profile "partners" such as the National Reconnaissance Office (NRO) or the National Geospatial Intelligence Agency (NGA)–$50 million is chump change.

And what are these corporate pirates seeking from Congress? Why "get-out-of-jail-free-cards," of course!

Behind closed doors, House and Senate negotiators are "are closing in on a deal" with the White House over illegal government domestic spying, ***The Wall Street Journal*** reported Friday.

Touted as a "compromise" and a "major breakthrough" by both Democrats and Republicans, the deal would "would kick the issue to a secret national-security court. Earlier versions of the legislation wanted to grant telecom companies blanket retroactive immunity from lawsuits," Siobhan Gorman avers.

However, according to the **Electronic Frontier Foundation**, a civil liberties group representing plaintiffs in Hepting vs. AT&T, brought by AT&T customers in the wake of revelations of massive domestic spying by the Bush administration and their "private" partners in the telecom industry, the congressional "compromise" is a monumental fraud:

> "The purported immunity 'compromise' announced on Thursday by Senator Bond is a pure sham that's even worse than the original immunity provision passed by the Senate," said EFF Senior Staff Attorney Kevin Bankston. "The stacked-deck immunity determination to be made by the court apparently still doesn't include any meaningful review of the telecoms' conduct or the legality of their cooperation with the NSA, simply a review of whether the companies got a piece of paper saying that the president authorized the surveillance. And the deck would be stacked even more by the proposed transfer to the FISA court–the most conservative and secretive federal court in the nation. Bottom line: it's still immunity, and this so-called compromise concedes nothing." ("EFF Blasts New 'Compromise' Offer on Teleco Immunity," Electronic Frontier Foundation, Press Release, May 23, 2008)

Some "compromise"!

According to the **Federation of American Scientists**, the FISA court,

> ...is responsible for reviewing and approving government applications under the Foreign Intelligence Surveillance Act for domestic electronic surveillance and physical search of suspected foreign intelligence agents or terrorists.

But it does more than that. The Court also reinterprets the terms of the Act in an undisclosed fashion, producing in effect a body of "secret law," a matter discussed at an April 30 hearing of the Senate Judiciary Committee.

> "The FISC has in fact issued... legally significant decisions that remain classified and have not been released to the public," observed Judge John D. Bates, a member of the FIS Court, when he denied an ACLU motion for disclosure of portions of those decisions last December. ("Intel Surveillance Court Gets Two New Judges," Federation of American Scientists, Secrecy News, May 23, 2008)

During the April 30 Senate Judiciary Committee hearing referenced above, John P. Elwood, a DoJ official "disclosed a previously unpublicized method to cloak government activities," according to ***The New York Times***.

In keeping with the Bush administration's penchant for lawless behavior, Elwood acknowledged that the executive branch believed that "the president could ignore or modify existing executive orders that he or other presidents have issued without disclosing the new interpretation," *Times'* reporters Scott Shane and David Johnson wrote.

Conceding nothing that would dispel fears that the administration is operating on the basis of "secret law" beyond the purview of the courts or Congress, the state's "legal stance would let it secretly operate programs that are at odds with public executive orders that to all appearance remain in force," the *Times* reported.

Demonstrating profound contempt for classification rules, Senator Sheldon Whitehouse (D-RI), said the administration's contention that it can "selectively modify" executive orders "turns The Federal Register into a screen of falsehoods behind whose phony regulations lawless programs can operate in secret."

In other words, following dictums laid down by French monarch, the "sun king" Louis XIV, the law is whatever our decider-president and his minions say it is.

While warrantless wiretapping and the subversion of law is bad enough, the question inevitably arises: what *other programs* are being hidden from the American people?

Investigative journalist Christopher Ketcham believes that a "highly classified program with sinister implications" may lie at the heart of Bush administration's refusal to back-down on telecom immunity. Through an as yet-undisclosed "black program," the administration may be "compiling a secret enemies list of citizens who could face detention under martial law."

According to Ketcham, recounting Acting Attorney General James Comey's now infamous 2004 **tussle** with the White House, and the bureaucrat's refusal to reauthorize Bush's illegal programs, Ketcham **writes**,

> Yet in his testimony before the Senate Judiciary Committee, he described how he had grown increasingly uneasy reviewing the Bush administration's various domestic surveillance and spying programs. Much of his testimony centered on an operation so clandestine he wasn't allowed to name it or even describe what it did. ("The Last Roundup," Radar, May/June 2008)

Welcome (once again) to the bizarro world of "Continuity of Government" whose illegally-beating dark heart may dwell in what intelligence insiders have called the ultra-top secret "Main Core" database.

Some months after ***The New York Times*** revealed in December 2005 that the Bush administration had illegally spied on Americans through its so-called "Terrorist Surveillance Program," ***USA TODAY*** reported,

> With access to records of billions of domestic calls, the NSA has gained a secret window into the communications habits of millions of Americans. Customers' names, street addresses and other personal information are not being handed over as part of NSA's domestic program, the sources said. But the phone numbers the NSA collects can easily be cross-checked with other databases to obtain that information. (Leslie Cauley, "NSA has massive database of Americans' phone calls," USA TODAY, May 11, 2006) [emphasis added]

Keep in mind that AT&T, Verizon and BellSouth, the nation's three largest telecommunication providers, are well-positioned to serve as the state's "outsourced" eyes-and-ears. Collectively, the three carriers provide an array of services: local and long-

distance calling, wireless and high-speed broadband internet access, as well as video and cable services.

Once communications information has been "fused" with records gleaned from commercially-available databases–sold, of course, to the state as a "patriotic" duty–NSA "partners" such as Booz Allen Hamilton, IBM, Lockheed Martin, Raytheon, CACI and L-3, can then analyze data such as medical histories, travel itineraries, shopping habits, political affiliations, subscription lists, DVD rentals, etc. In a nanosecond, a unique profile of an individual's "transactional" life has thus been created.

This however, is not without risk to offending spies and data-miners. And given the nature of financial penalties under section 222 of the Communications Act, telecom executives have every reason to sweat. The FCC "can levy fines up to $130,000 per day per violation, with a cap of $1.325 million per violation. The FCC has no hard definition of 'violation.' In practice, that means a single 'violation' could cover one customer or 1 million," Cauley reported.

But the Bush administration's so-called "Terrorist Surveillance Program" may very well be a smokescreen for collecting political data on millions of Americans, a secret "enemies list" far more dangerous to a democratic society than anything conceived by the team of "national security" paranoids assembled by Richard Nixon. Ketcham reports,

> According to a senior government official who served with high-level security clearances in five administrations, "There exists a database of Americans, who, often for the slightest and most trivial reason, are considered unfriendly, and who, in a time of panic, might be incarcerated. The database can identify and locate perceived 'enemies of the state' almost instantaneously." He and other sources tell **Radar** that the database is sometimes referred to by the code name Main Core. One knowledgeable source claims that 8 million Americans are now listed in Main Core as potentially suspect. In the event of a national emergency, these people could be subject to everything from heightened surveillance and tracking to direct questioning and possibly even detention. …
>
> A host of publicly disclosed programs, sources say, now supply data to Main Core. Most notable are the NSA domestic surveillance programs, initiated in the wake of 9/11, typically referred to in press reports as "warrantless wiretapping." In March, a front-page article in the **Wall Street Journal** shed further light onto the extraordinarily invasive scope of the NSA efforts: According to the **Journal**, the government can now electronically monitor "huge volumes of records of domestic e-mails and Internet searches, as well as bank transfers, credit card transactions, travel, and telephone records." Authorities employ "sophisticated software programs" to sift through the data, searching for "suspicious patterns." In effect, the program is a mass catalog of the private lives of Americans. And it's notable that the article hints at the possibility of programs like Main Core. "The [NSA] effort also ties into data from an ad-hoc collection of so-called black programs whose existence is undisclosed," the **Journal** reported, quoting unnamed officials. "Many of the programs in various agencies began years before the 9/11 attacks but have since been given greater reach."

As disturbing as Ketcham's report is, consider this: the ACLU's "**Watch List Counter**" documents that the FBI's Terrorist Screening Center currently lists (as of 5/26/08) 975,883 (!) individuals as potential "threats" to "national security." What are the criteria for inclusion? No one knows and the FBI and DHS aren't saying.

It is of course absurd to believe there are nearly a million U.S. sympathizers of the Afghan-Arab database of disposable intelligence assets, aka al-Qaeda, roaming the streets of American cities. However, if history is any guide to present state surveillance activities, a database like Main Core, *if it exists*, would include dissidents and activists of all stripes, ranging from socialists and communists, anarchists, tax protestors, gun owners, lawyers and professors, "illegal" migrants, publishers and journalists, or just plain folk caught in the government's data driftnet.

But over and above the question of telecom immunity for law-breaking communication corporations looms the issue of intelligence outsourcing as a lucrative business arrangement with the state, the ubiquitous "public-private partnership" in political repression that affect all our lives. As investigative journalist Tim Shorrock documents,

> A second form of cooperation that few Americans are aware of concern the role of the telecom giants as **contractors** for the Intelligence Community. As commercial communications and encryption technologies advanced in the years leading up to 2001, AT&T, Verizon and the other major carriers were hired by the government to build classified communications networks for the NSA and Pentagon. That alliance spawned new institutions where the government could carry out a dialogue with these companies. Many industry executives, for example, hold leading positions in a secretive agency called the National Security Telecommunications Advisory Committee, a group of business leaders who meet regularly with President Bush, Vice President Cheney, and senior officials in the Intelligence Community to discuss critical issues affecting the national telecommunications system. …

That broad alliance between the NSA and the government on one hand and the telecommunications and IT industries on the other is the fundamental issue at stake in the national debate that erupted around FISA in 2007 and 2008. That debate was about far more than a few telecom companies cooperating with the government. (*Spies for Hire: The Secret World of Intelligence Outsourcing*, New York: Simon & Schuster, 2008, pp. 307, 308)

In this context, the political economy of telecom immunity should be considered a shield for government "black" programs that could be quickly rolled-out during a "national emergency." That congressional leaders–Democrats and Republicans–would grant their corporate benefactors nearly unlimited power to spy on Americans, or worse, is an indication that elite consensus has been reached in favor of maintaining an all-encompassing surveillance state.

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****.*

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