

## US Government Spying on Americans, Lawsuits Against Telecom Partners

As Whistleblower Prosecutions Rise, Government Withholds Spy Doc, Fears Lawsuits Against Telecom Partners

By <u>Tom Burghardt</u> Global Research, May 15, 2011 <u>Antifascist Calling...</u> 15 May 2011 Region: <u>USA</u> Theme: <u>Police State & Civil Rights</u>

With Obama's Justice Department threatening to classify previously *unclassified* material during the upcoming trial of accused NSA whistleblower Thomas A. Drake, <u>Secrecy News</u> reports that prosecutors <u>claim</u> they can do so because "NSA possesses a statutory privilege that protects against the disclosure of information relating to its activities."

Never mind that security apparatchiks have carried out multiyear, illegal driftnet surveillance operations against the American people, or that the broad outlines of these illicit programs have been known for almost six years when they were first reported by <u>The</u> <u>New York Times</u>. Despite these inconvenient truths, our "transparency" president's minions are now asserting the right to erase well-known facts from the public record to win a conviction in a high-profile case.

And with a federal <u>Grand Jury</u> now meeting in Alexandria, Virginia to criminally investigate the <u>WikiLeaks</u> organization and its founder, Julian Assange, to determine whether they can be charged with violations of the draconian Espionage Act, the administration is pulling out all the stops by targeting individuals who expose government crimes and corruption.

Accused of leaking information that uncovered high-level corruption at the Pentagon's electronic intelligence satrapy, Drake is charged with serving as a source for a series of articles published by <u>The Baltimore Sun</u> that provided rich details on cosy relations between NSA officials and Science Applications International Corporation (SAIC).

According to investigative journalist Siobhan Gorman, three years and \$1.2 billion after choosing SAIC as the primary contractor for a failed digital communications project called Trailblazer, "SAIC did not provide computer experts with the technical or management skills to complete the project."

In subsequent reporting, the <u>Sun</u> revealed that "six years after it was launched, the Trailblazer program consists of little more than blueprints on a wall."

Drake's revelations of high-level cronyism at the agency which cost taxpayers billions of dollars were further amplified by other reporters. Writing for <u>CorpWatch</u>, investigative journalist Tim Shorrock disclosed that NSA "is the company's largest single customer, and SAIC is the NSA's largest contractor."

Shorrock tells us that "the company's penchant for hiring former intelligence officials played

an important role in its advancement."

According to CorpWatch, "the story of William Black, Jr." is emblematic of the clubby, goodold-boy networks that constellate the National Security State. "In 1997," Shorrock writes, "the 40-year NSA veteran was hired as an SAIC vice president 'for the sole purpose of soliciting NSA business,' according to a published account. Three years later, after NSA initially funded Trailblazer, Black went back to the agency to manage the program; within a year, SAIC won the master contract for the program."

Hardly surprising, given the fact that the so-called revolving door ushering former top intelligence officials into corporate board rooms is a tale oft-told, as the curriculum vitae of former NSA- and Director of National Intelligence, John Michael "Mike" McConnell, readily attests. After his two-year stint as President Bush's DNI (2007-2009), McConnell returned to his perch at the ultra-spooky Booz Allen Hamilton security firm as Senior Vice President where he currently manages that firm's cybersecurity portfolio.

Peddling his expertise as an intelligence insider, McConnell is one of the chief tricksters hawking the so-called "cyber threat," the latest front to have emerged from the highly-profitable "War on Terror."

Last year, in a widely-cited <u>Washington Post</u> op-ed, McConnell claimed that the United States needs "to reengineer the Internet to make attribution, geolocation, intelligence analysis and impact assessment-who did it, from where, why and what was the result-more manageable."

What should interest readers here, is the fact that while the Obama administration wages war on whistleblowers like Thomas Drake, Bradley Manning and others, who expose waste, fraud, abuse and war crimes, the architects and perpetrators of those offenses, high-level corporate and government officials, escape justice and continue to operate with impunity.

In the Drake case, *Secrecy News* analyst Steven Aftergood writes, "The NSA Act ... has never been used to exclude information in a criminal case."

That the administration has chosen to do so with Drake serves as an unmistakable warning that the federal government will crush anyone who challenges crimes perpetrated by the secret state.

Aftergood told <u>NPR</u> last week that the Obama regime's surge of whistleblower prosecutions is "a worrisome development."

"Leaks serve a very valuable function as a kind of safety valve," he said. "They help us to get out the information that otherwise would be stuck."

And with Congress, spearheaded by right-wing Democratic Senator Dianne Feinstein, chairwoman of the powerful Senate Intelligence Committee, seeking to go even further to persecute whistleblowers, the government is poised to choke-off what little remains of democratic oversight, thus ensuring that information remains "stuck."

As FBI whistleblower Sibel Edmonds <u>points out</u>, "every time when I think things couldn't possibly get any worse, I'm proven wrong and they actually do get worse."

"Our so called representatives," Edmonds writes, "are planning to increase the federal government's unchecked powers by giving them the right to strip national security whistleblowers of their pensions."

According to the National Whistleblowers Center (<u>NWC</u>), under <u>Section 403</u> of the Intelligence Authorization Act, "the head of an employee's agency can simply accuse a whistleblower of leaking classified information and that whistleblower can automatically be stripped of their federal pension, even after they retire."

So draconian is this proposal that once stripped of their pensions, whistleblowers would be barred from accessing the federal courts to challenge their administrative punishment.

"Instead," NWC avers, "they will be forced to use the DNI's administrative procedures to try to defend themselves. In other words, the DNI will be the prosecutor, the judge and the jury to strip pensions from public servants."

## Shielding Telecoms ... from their Customers

Meanwhile across the Potomac, the <u>ACLU</u> reported last week that in response to their lawsuit challenging the constitutionality of the repulsive FISA Amendments Act and their Freedom of Information Act request "to learn more about the government's interpretation and implementation" of FAA, "the government released a few hundred pages of heavily redacted documents."

As readers recall, the FAA was a piece of legislative detritus passed by a Democraticcontrolled Congress in 2008 that authorized the secret state's driftnet surveillance of American's communications while providing retroactive immunity to NSA's private partners in the telecommunications' industry.

Just so we understand what it is Congress shielded, AT&T whistleblower Mark Klein described how the firm and the NSA physically split and then copied global communications traffic flowing into their offices and then passed it along to the Agency. In his self-published book, Klein wrote:

What screams out at you when examining this physical arrangement is that the NSA was vacuuming up everything flowing in the Internet stream: e-mail, web browsing, Voice-Over-Internet phone calls, pictures, streaming video, you name it. The splitter has no intelligence at all, it just makes a blind copy. There could not possibly be a legal warrant for this, since according to the 4th Amendment warrants have to be specific, "particularly describing the place to be searched, and the persons or things to be seized." ...

This was a massive blind copying of the communications of millions of people, foreign and domestic, randomly mixed together. From a legal standpoint, it does not matter what they claim to throw away later in the their secret rooms, the violation has already occurred at the splitter. (Mark Klein, *Wiring Up the Big Brother Machine... And Fighting It*, Charleston, South Carolina: BookSurge, 2009, pp. 38-39.)

"Two weeks ago," ACLU National Security Project staffer Alexander Abdo wrote, "as part of our FOIA lawsuit over those documents, the government gave us several declarations attempting to justify the redaction of the documents."

In the course of examining the documents, ACLU researchers "came across this

unexpectedly honest explanation from the FBI of why the government doesn't want us to know which 'electronic communication service providers' participate in its dragnet surveillance program." On page 32 we are enlightened by the following nugget:

In this case, the FBI withheld the identities of the electronic communication service providers that have provided information, or are listed as potentially required to provide information, to the FBI as part of its national security and criminal investigations under authority granted by Section 702 of the FAA. Exemption (b)(4)-1, cited in conjunction with (b)(7)(D)-1, has been asserted because disclosure of the identities of electronic communication service providers would cause substantial harm to their competitive position. Specifically, these businesses would be substantially harmed if their customers knew that they were furnishing information to the FBI. The stigma of working with the FBI would cause customers to cancel the companies' services and file civil actions to prevent further disclosure of subscriber information. Therefore, the FBI has properly withheld this information pursuant to Exemption (b)(4), in conjunction with (b)(7)(D)-1. (Declaration of David M. Hardy, Federal Bureau of Investigation, in *American Civil Liberties Union, et al v. Office of the Director of National Intelligence, et al*, Civil Action No. 10-CV-4419 (RJS), April 25, 2011)

Got that?

While the federal government illegally spies on us, those who are sworn to uphold the Constitution and protect our rights are engaged in a massive swindle designed by Congress to shield private lawbreakers whose "competitive position" might be compromised should their filthy corporate practices be exposed.

Public *harm*, private *profit*; it doesn't get any clearer than this!

Tom Burghardt is a researcher and activist based in the San Francisco Bay Area. In addition to publishing in Covert Action Quarterly and <u>Global Research</u>, an independent research and media group of writers, scholars, journalists and activists based in Montreal, he is a Contributing Editor with <u>Cyrano's Journal Today</u>. His articles can be read on <u>Dissident Voice</u>, <u>The Intelligence Daily</u>, <u>Pacific Free Press</u>, <u>Uncommon Thought Journal</u>, and the whistleblowing website <u>WikiLeaks</u>. He is the editor of Police State America: U.S. Military "Civil Disturbance" Planning, distributed by <u>AK Press</u> and has contributed to the new book from <u>Global Research</u>, The Global Economic Crisis: The Great Depression of the XXI Century.

The original source of this article is <u>Antifascist Calling...</u> Copyright © <u>Tom Burghardt</u>, <u>Antifascist Calling...</u>, 2011

## **Comment on Global Research Articles on our Facebook page**

## **Become a Member of Global Research**

Articles by: <u>Tom Burghardt</u> http://antifascist-calling.blogspot.co m/ **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: <a href="mailto:publications@globalresearch.ca">publications@globalresearch.ca</a>

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