GlobalResearch
Center for Research on Globalization

Violating the Digital Privacy Rights of Americans

Pentagon Stonewalls Corporate Spy Probe

By Tom Burghardt
Global Research, April 10, 2011
Antifascist Calling... 10 April 2011

Region: USA
Theme: Law and Justice, Police State & Civil Rights

When ***Politico*** reported late last month that President Obama quietly received a "transparency" award "in a closed, undisclosed meeting at the White House," I first thought it was an April Fool's gag.

But as with all things Obama, the joke is on us.

Reporter Abby Phillip revealed that during a "secret presentation" which had been "inexplicably postponed" two weeks earlier, His Changeness received high marks from "Gary Bass of OMB Watch, Tom Blanton of the National Security Archive, Danielle Brian of the Project on Government Oversight, Lucy Dalglish of the Reporters Committee for Freedom of the Press, and Patrice McDermott of OpenTheGovernment.org."

Let it be said, these organizations do yeoman's work uncovering official waste, fraud and abuse and have done much to expose state crimes (past and present) committed by the U.S. government.

Nevertheless, in callous disregard for his supporters (which should be an object lesson for those who believe the secret state can be "reformed" from the inside), the White House failed to post the meeting on the president's public schedule and barred photographers and print journalists from recording the august event.

OMB Watch's Gary Bass found it "baffling" that the president wouldn't want to trumpet his award; after all, hadn't Obama promised his would be the most "open" administration in history?

For her part, **OpenTheGovernment.org's** Patrice McDermott expressed "disappointment" that the meeting was held *in camera* and "surprise" when they learned the event was "not on the President's daily calendar."

Caught off-guard by the White House McDermott averred, "Why they decided to close the meeting to the press is not something we understand."

Scarcely a week later, we learned that the administration will soon seek legislation from Congress that would "punish leaks of classified information" and authorize "intelligence agencies to seize the pension benefits of current or former employees who are believed to have committed an unauthorized disclosure of classified information," ***Secrecy News*** revealed.

Given the embarrassing fact that the award was bestowed "in honor of President Obama's

commitment to transparency," even as his administration hounds and prosecutes whistleblowers with a ferocity not seen since the darkest days of Watergate, the question is: why is there *still* such a profound disconnect between the harsh realities of White House policy and its perception management amongst those who should know better?

Digital Privacy? Forgetaboutit!

What other ironies are hiding in plain sight in well-appointed Washington hearing rooms and dark corridors?

CNET News reported that the Justice Department "offered what amounts to a frontal attack on proposals to amend federal law to better protect Americans' privacy."

During hearings last week before the Senate Judiciary Committee, which is rewriting portions of the 1986 Electronic Communications Privacy Act (**ECPA**), Associate Attorney General James A. Baker warned the panel that granting "cloud computing users more privacy protections and to require court approval before tracking Americans' cell phones would hinder police investigations."

Baker **told** the committee "that requiring a search warrant to obtain stored e-mail could have an 'adverse impact' on criminal investigations," CNET reported. And making location information only available with a search warrant, he said, would hinder "the government's ability to obtain important information in investigations of serious crimes."

"As we engage in that discussion," Baker averred, "what we must not do–either intentionally or unintentionally–is unnecessarily hinder the government's ability to effectively and efficiently enforce the criminal law and protect national security."

How obtaining a search warrant to legally investigate crime while protecting the rights of suspects would hinder "the government's ability to access, review, analyze, and act promptly upon the communications of criminals that we acquire lawfully," was side-stepped by the Justice Department.

Coming on the heels of new administration rules that "allow investigators to hold domestic-terror suspects longer than others without giving them a Miranda warning," as ***The Wall Street Journal*** reported, while "significantly expanding exceptions to the instructions that have governed the handling of criminal suspects for more than four decades," weakening already anemic digital privacy rights would grant even more power to those building a National Surveillance State.

Indeed, short of obtaining a search warrant as stipulated in the Fourth Amendment, any and all electronic communications trolled by the secret state, whether or not they are part of an ongoing criminal or national security investigation have *not* been acquired "lawfully."

On this point, the law is clear: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

But as ***Antifascist Calling*** reported in February, the Electronic Frontier Foundation (EFF) released an explosive **report** that documented the lawless, constitution-free zone that

already exists in “new normal” America.

According to EFF, their review of nearly 2,500 pages of previously classified **documents** pried from the FBI through Freedom of Information Act litigation, revealed that Bureau “intelligence investigations have compromised the civil liberties of American citizens far more frequently, and to a greater extent, than was previously assumed.”

In fact, “almost one-fifth involved an FBI violation of the Constitution, the Foreign Intelligence Surveillance Act, or other laws governing criminal investigations or intelligence gathering activities.”

“From 2001 to 2008,” the civil liberties’ watchdogs uncovered evidence that “the FBI engaged in a number of flagrant legal violations.” Amongst the more egregious abuses of democratic norms, EFF revealed that FBI investigators could be criminally charged with “submitting false or inaccurate declarations to courts, using improper evidence to obtain federal grand jury subpoenas” and “accessing password protected documents without a warrant.”

Keep in mind these transgressions occurred in but *one* of 16 agencies which comprise the so-called “Intelligence Community.” It’s anyone’s guess what dirty work is being hatched in darkness by opaque Pentagon satrapies such as the National Security Agency or U.S. Cyber Command, let alone that institutional black hole of crime and corruption, the CIA.

Never one to miss a beat, or offer ever more insidious snooping privileges to the Executive Branch, Senator Charles Grassley (R-IA) said “it’s crucial to ensure we don’t limit (law enforcement’s) ability to obtain information necessary to catch criminals and terrorists who use electronic communication.”

Grassley also suggested that requiring warrants, a thoroughly novel and radical approach to policing in a society that presumably champions the rule of law and the rights of the accused, would lead to “increased burdens on the court system.”

We wouldn’t want *that* would we? Heavens no! Considering how tiresome it must already be for our “overburdened” federal court system and Justice Department busily and conscientiously investigating and prosecuting Bush, now Obama, administration officials for high crimes and misdemeanors.

Launch a preemptive war against a nation that hasn’t attacked us, say Libya, without consulting Congress whom the Constitution alone has granted the power to declare war? Well, there’s an app for that too!, the White House Office of Legal Counsel (**OLC**), which recently declared “that the President had the constitutional authority to direct the use of force in Libya because he could reasonably determine that such use of force was in the national interest.”

Memo to Congress: sit down, shut up and continue doing what you do best–taking **blood money** from the corporate merchants of death who profit from the enterprise.

Pentagon Stonewalls Corporate Spy Probe

Violating the digital privacy and political rights of Americans isn’t the exclusive purview of

the secret state.

As fallout from the HBGary/Palantir/Berico/Team Themis hack by **Anonymous** continues to spread like a radioactive cloud, ***The Tech Herald***, which first broke the story of Bank of America's sleazy project to bring down WikiLeaks by targeting journalists and supporters, reported that the Defense Department is stonewalling Rep. Hank Johnson's (D-GA) request "to review contracts signed with Team Themis."

> "Last week," investigative journalist Steve Ragan disclosed, "Rep. Johnson sent a **letter** to the DOD, as well as the Department of Justice (DOJ) and the Office of the Director of National Intelligence (ODNI), asking that any information regarding contracts signed with Team Themis be returned to his office within 10 business days."

Ragan writes that "Johnson is seeking 'in their entirety,' all past and present contracts held by Team Themis, in addition to a written explanation of what safeguards are in place to restrain federal contractors from using technologies for official use against American citizens. Moreover, he asked for a written explanation of who owns and controls the tools developed by contractors for the government."

> "This last request," The Tech Herald avers, "is important when you consider that the persona management software developed for the U.S. Central Command (USCENTCOM), also known as MetalGear, isn't owned by the government, it's owned by developer Ntrepid."

Such contracts are worth millions and niche security outfits like Team Themis are viewed by the Pentagon as key players in the development of surveillance tools in Washington's endless "War on Terror."

Last week, the secrecy-shredding web site **Public Intelligence** published two additional HBGary documents that provided new details on the close, and profitable, conjunction amongst opaque corporate entities and the Pentagon.

The first is the **HBGary SRA International 'Memory Grabber' Forensics Tool White Paper**, which describes a system for obtaining "memory access to a running and password protected laptop through the use of a small PC Card inserted into the PCMCIA slot of the laptop."

We're told that "law enforcement agents and Special Operations personnel need a tool that provides memory access to a running laptop in the field enabling the timely capture of volatile information."

Such a device would be of particular interest to Border Patrol agents who might seize the laptop of a dissident returning from an overseas peace conference, or a journalist who may have had the temerity to probe too deeply into state-sanctioned crimes.

Last week, the 9th U.S. Circuit Court of Appeals ruled in a 2-1 decision that "authorities may seize laptops, cameras and other digital devices at the U.S. border without a warrant, and scour through them for days hundreds of miles away," ***Wired*** reported.

Unsurprisingly, "under the Obama administration, law enforcement agents have aggressively used this power to search travelers' laptops, sometimes copying the hard drive before returning the computer to its owner."

The second document, **HBGary DARPA Cyber Insider Threat (CINDER) Proposal**, details a bid by the dodgy firm to secure a piece of the Defense Advanced Research Project Agency's "Insider Threat" pie.

> "Like a lie detector detects physical changes in the body based on sensitivities to specific questions," HBGary avers, "we believe there are physical changes in the body that are represented in observable behavioral changes when committing actions someone knows is wrong."
>
> "Our solution," disgraced former HBGary Federal CEO Aaron Barr wrote, "is to develop a paranoia-meter to measure these observables."

Before being run to ground by Anonymous, Barr and HBGary CEO Greg Hoglund claimed they had developed a system, a "full functional rootkit on every host or on targeted hosts that can have complete control over the operating environment."

We're told that "the rootkit loads as a stealth kernel-mode base implant," and "will collect select file access, process execution with parameters, email communications, keyboard activity with a time/date stamp, network/TDI activity (and the actual network data if appropriate), and IM traffic. If detailed surveillance is required, it can be enabled to capture screenshots and construct a video stream. All traces of the rootkit installation will be removed after the initial deployment (event log, etc)."

But as we have seen, projects such as this can just as easily migrate into the private sector and be deployed by corporations to spy on employees who might have an unfavorable view of shady practices, such as robo-signing tens of thousands of fraudulent foreclosure notices to cash-strapped homeowners, and then **do something** about it.

Johnson, in his letter to ODNI Director James Clapper is determined to discover whether Team Themis "violated the law and/or their federal contracts by conspiring to use technologies developed for U.S. intelligence and counterterrorism purposes against American citizens and organizations on behalf of private actors."

In the best traditions of DOD stonewalling and cover-up, the Department's CIO Teri Takai and deputy CMO Elizabeth McGrath both said they were not familiar with "that company" [HBGary] but, as Ragan reported, Takai said "she would have her office look into things and make sure that 'we get back to you…'"

When hell freezes over!

*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**, an independent research and media group of writers, scholars, journalists and activists based in Montreal, he is a Contributing Editor with **Cyrano's Journal Today**. His articles can be read on **Dissident Voice**, **The Intelligence Daily**, Pacific Free Press, **Uncommon Thought Journal**, and the whistleblowing website **WikiLeaks**. He is the editor of Police State America: U.S. Military "Civil Disturbance" Planning, distributed by **AK Press** and has contributed to the new book*

*from **Global Research**, The Global Economic Crisis: The Great Depression of the XXI Century.*

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