## President Obama's Data Harvesting Program:

# NSA as Pollster, PRISM as MISO

by John Stanton

It is way too soon to bet the house fortune on the reliability of reports by the Washington Post (Washington, DC) and The Guardian (United Kingdom) on President Obama's data harvesting program, known for the moment as <u>PRISM</u>.

With the hot pursuit of mainstream media reporters underway by the US Department of Justice (Associated Press, for example); a US Corporate-State show trial of Bradley Manning, Julian Assange/Wikileaks (Obama has already stated they are guilty); the extraordinary cyberwar/hacking accusations against the Chinese government; and the shrill sound of <u>cyber quackery</u> from the Defense Science Board and its legion of security contractors, caution all around is the order of the day.

Indeed, the membership of President Obama's National Security Telecommunications Advisory Committee (NTSAC) reflects the close proximity of the President to critical cyber/telecom/ISP leaders who likely get advanced warning of the incoming nukes. Some of the NSTAC members include Verizon Business Group, Raytheon, AT&T, Vonage, Intelsat, Avaya, Microsoft and Lockheed Martin. And they did not know that their networks, switches, routers, and packets were being violated? Of interest is the presence of FireEye, a cybersecurity firm. One of FireEye's Board members is Robert Lentz who has an excellent DOD/NSA pedigree. "Robert has served as a member of the board of directors since March 2010. He has served as the president of Cyber Security Strategies since October 2009. He served as the deputy assistant secretary of defense for cyber, identity, and information assurance in the Office of the Assistant Secretary of Defense, Networks and Information Integration/Chief Information Officer from November 2007 to October 2009. Since November 2000, he has also served as the chief information security officer for the U.S. Department of Defense. He previously worked at the National Security Agency from 1975 to 2000, where he served in the first National Computer Security Center."

The US national security machinery has stated time and again that the Internet and World Wide Web are fair game for military information support operations (MISO) and that means shaping the consciousness of individuals, organizations and governments to the benefit of America's national interests. Viewed in this manner, it is possible to argue that PRISM would have a chilling effect on not only whistleblowers and their media handlers, but perhaps on practitioners of industrial espionage whether they are French, Chinese or Israeli's.

The calculated pursuit of mainstream media by President Obama, the publicizing by the US corporatenational security machinery of PRISM, Stuxnet—and the takedown of BitCoin websites; and the entry of Cyber Command into the daily lives of Americans seems to suggest that a new order is afoot, or at least that the US Corporate State is trying to recover/wrest control of the US historical-current-future narrative from independent internal and foreign news/information sources. Obama seems to have taken US presidential paranoia to new levels. President Obama's national security aides and political handlers appear to have adopted the John Haldeman—John Erlichman philosophy and practice of protecting Obama. According to the Telegraph, UK, "Vali Nasr, a university professor who was seconded in 2009 to work with Richard Holbrooke, Mr Obama's special envoy to Afghanistan and Pakistan, records his profound disillusion at how a "Berlin Wall" of domestic-focused advisers was erected to protect Mr Obama. "The president had a truly disturbing habit of funneling major foreign policy decisions through a small cabal of relatively inexperienced White House advisers whose turf was strictly politics," reports The Telegraph.

## **Intelligence Agencies as Pollsters**

Would it surprise anyone of some eager Obama aides decided to use data mined through a program like PRISM to figure out what American citizens are thinking? Forget Gallup and Pew. With the thoughts, pictures, video, travel records and expenditures of tens of millions of Americans harvested and interpreted by various machine programs and human analysts in the NSA, CIA, and DIA, who needs commercial pollsters. Talk about sample size! And thanks to many US Court decisions, data gathering is largely legal.

And would it not be a matter of national security for the President of the United States to know what Americans are thinking as the USA remains in a state of emergency since 911. Moreover the American nation is still at war and just steps away from lighting up Iran, Syria and Iraq (again). For the global carnage to proceed as planned, the US Corporate State must control the flow of information as it did in World War II (1939-1945).

Obama "is the boss" has a need for "the info" as Doctor Evil so eloquently put it the movie Austin Powers. PRISM data must be in his hands, particularly given that Obama can say with a straight face "civil liberties improve with this type of surveillance." US Senators must have the info too. Senators like Diane Feinstein, John McCain and Lindsey Graham are "happy" to be monitored and, well, why not all of us. All four of these characters know that American's will collectively shrug their shoulders and forget about the matter by immersing themselves in the celebrity breakdown of the day.

Perhaps the most unsettling aspect of US government data harvesting and analysis programs is that the all of the work is researched, developed, tested and deployed by for-profit companies like those belonging to NSTAC. According to the Defense Security Service (DSS), "U.S. industry develops and produces the majority of our nation's defense technology – much of which is classified – and thus plays a significant role in creating and protecting the information that is vital to our nation's security... DSS has Industrial Security oversight and assistance responsibility for over 13,000 cleared facilities participating in the National Industrial Security Program and estimates that there are over 11 million classified documents in the hands of U.S. industry." DSS, always understaffed but extraordinarily dedicated, do their best to keep US industry within a tolerable degree of greed.

#### All PRISM's are Not Created Equal

Email, voice, video capture would seem to rely on some sort of read-module within a switch. Analyzing it all—separating wheat and chafe—would appear to require some sort of autonomous machine language. Perhaps some of these PRISM's are tangentially related to the NSA's PRISM.

Over at Cryptome, a document from the US Department of Homeland Security (DHS) describes Protect, Respond, Inform, Secure, and Monitor (PRISM). According to DHS PRISM is composed of two primary components: Contora and ESRI ArcIMS. Additional and optional components include Message 911, Ensco Sentry, and Lunar Eye. These components have been tightly integrated into a single end-user application that provides a messaging, alerting, geo-referenced mapping, asset tracking, CBRN sensing, and public warning system. Lunar Eye is a GPS tracking suite.

A USAF "communications" dictionary shortens Programmable-Reconfigurable-Integrated-Switch and Multiplex to PRISM.

Alcatel-Lucent's product PRISM/GORI manages SMS (text) messages. A sample of DOD's DTIC search engine returns when PRISM is entered follows: MITRE's PRISM is a software program used to request intelligence collection on moving vehicles, aircraft, people and animals; PaRallel Inference SysteM-PRISM—a connectionist inference for developing machine language and autonomous network management programs; and RDTE Budget Note--PRISM to MAJIIC Interoperability Assessment: assessed that Planning Tool for Resource, Integration, Synchronization and Management (PRISM) and the interface to NATO Multi-Sensor Aerospace-Ground Joint ISR Interoperability Coalition (MAJIIC) was functional and ready for operations by demonstrating automated interoperability and exchange of intelligence requirements.

## What's the Big Deal?

David Bromwich at the Huffington Post sums it up best, "Even now, government aides are most concerned about "the magnitude of the leak." The question that troubles them is not, How did we come to this? but rather, Shall we prosecute the whistleblower? The pattern is so galling and tedious, and its harms so invisible to all but a few, that we may be tempted to relax and wait for the next election. But remember again the language of the court order. On an ongoing daily basis. All call detail records. Including local telephone calls. The next president will inherit this. No names, no records of words (not yet), no inculpating or exculpating evidence (just "signatures"), but still: these are outlines of the communicative behavior of upward of a million persons, with similarly compelling orders out to the other telecoms. The aim is to capture by index the whole of the U.S. population. The amazing and routine FISA order is a blind command for the opening of a thousand eyes. The plainest rebuke to such procedures comes from the language of the fourth amendment itself."

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.

"By what right are the addressed envelopes of the spoken communications of 280 million citizens plucked from the air by government and filed away? Supported by whose oath and what affirmation? There is a simple force to the words of the fourth amendment after all. It says: we do not live by secret laws, and we will not abide by general warrants. And to the comfort offered by senators Chambliss, Graham, and Feinstein, who ask us to sleep well and sleep long, there is a simple reply. In what country do they think they are living, and under what constitution?"

John Stanton is a Virginia based writer specializing in national security matters. His latest book is Cyber Noodles (cyber security), Orphan Nukes and the Failure of the US National Security State. Reach him at cioran123@yahoo.com