GlobalResearch
Center for Research on Globalization

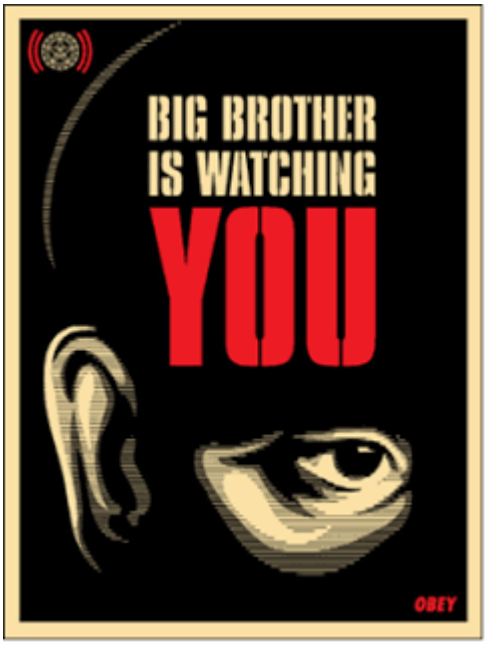
New Documents Shed Light on NSA's Dragnet Surveillance

By Tom Burghardt
Global Research, July 01, 2013
Antifascist Calling

Region: USA
Theme: Intelligence, Police State & Civil Rights

With the Obama administration in full damage control mode over revelations of blanket surveillance of global electronic communications, new documents published by The Guardian, including the draft of a 2009 report by the NSA's Inspector General marked Top Secret and a Secret 2007 Justice Department memo prepared for then US Attorney General Michael Mukasey, show that "a federal judge sitting on the secret surveillance panel called the Fisa court would approve a bulk collection order for internet metadata 'every 90 days'."

An unnamed "senior administration official" confirmed the existence of a Bush-era surveillance program which gobbled-up "vast amounts of records detailing the email and internet usage of Americans," but claimed, without evidence, that "it ended in 2001," according to *The Guardian*.



Early last month, the British newspaper began publishing documents provided by former NSA contractor Edward Snowden, including a Top Secret FISA court order to Verizon Business Services, which requires the firm "on an ongoing, daily basis" to hand over information on all telephone calls within its system.

The Wall Street Journal reported that the NSA's "monitoring of Americans includes customer records from the three major phone networks as well as emails and Web searches, and the agency also has cataloged credit-card transactions." The secret state's spying initiative "also encompasses phone-call data from AT&T Inc. and Sprint Nextel Corp., records from Internet-service providers and purchase information."

Days later, *The Washington Post* revealed that the Bush administration's "warrantless wiretapping" program known as STELLAR WIND, had been succeeded by four "collection programs" two of which, MAINWAY and MARINA, "process trillions of 'metadata' records for storage and analysis."

Additional programs, the *Post* reported, operating "on a much smaller scale, are aimed at content," one of which "intercepts telephone calls and routes the spoken words to a system called NUCLEON."

Although the news outlets principally responsible for bringing these stories to light, principally *The Guardian*, *Washington Post*, *South China Morning Post*, and now *Der Spiegel*, have not (as yet) published complete sets of NSA documents, and their reporting has barely scratched the surface of content-siphoning deep packet inspection (DPI) programs for internet and telephone surveillance (indeed, PRISM may be a subset of larger and more pernicious programs that collect, analyze and store everything), what we *have* learned so far is deeply troubling and pose grave threats to civil liberties.

New PRISM Slides, More Questions

Filling in some of the blanks, on June 29 *The Washington Post* published four additional PRISM slides from the 41-slide deck provided to *The Guardian* and *Post* by Edward Snowden.

Confirming what civil libertarians, journalists and political analysts have long maintained, NSA can and probably does "acquire" anything an individual analyst might request as Snowden averred. This includes, according to new information provided by the *Post*: chats, email, file transfers, internet telephone, login/ID, metadata, photos, social networking, stored data in the cloud, video, video conferencing.

If *that* isn't a surveillance dragnet, then words fail.

Recall, that previous reporting disclosed that major US internet and high tech firms, Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL and Apple gave NSA "direct access" to their systems.

"The program," according to *The Guardian*, "facilitates extensive, in-depth surveillance on live communications and stored information. The law allows for the targeting of any customers of participating firms who live outside the US, or those Americans whose communications include people outside the US."

"It also opens the possibility of communications made entirely within the US being collected without warrants," a near probability in this writer's opinion.

In a report that appeared the same day, *The Washington Post* disclosed that NSA and the FBI "are tapping directly into the central servers of nine leading U.S. Internet companies, extracting audio and video chats, photographs, e-mails, documents, and connection logs that enable analysts to track foreign targets," and that the agency "s accustomed to corporate partnerships that help it divert data traffic or sidestep barriers."

Although the firms all denied that they hand over customer data to the government, their self-serving claims are undercut by evidence that NSA-cleared company personnel, including "collection managers," send "content tasking instructions directly to equipment installed at company-controlled locations," rather than directly to company servers.

"Under Prism," the *Associated Press* reported, "the delivery process varied by company."

"Google, for instance, says it makes secure file transfers. Others use contractors or have set up stand-alone systems. Some have set up user interfaces making it easier for the government, according to a security expert familiar with the process."

"With Prism," AP reported, "the government gets a user's entire email inbox. Every email, including contacts with American citizens, becomes government property."

"Once the NSA has an inbox, it can search its huge archives for information about everyone with whom the target communicated. All those people can be investigated, too."

The slides published June 29 shed some light on how the process works. We learn for example that when an analyst "tasks" PRISM for information on a new "target," it is automatically passed on to a supervisor who "who reviews the 'selectors' or search terms. The supervisor must endorse the analyst's 'reasonable belief,' defined as 51 percent confidence, that the specified target is a foreign national who is overseas at the time of collection."

Tasking orders can be sent to multiple sources, "for example, to a private company and to an NSA access point that taps into the Internet's main gateway switches." (for background see: Mark Klein, *Wiring Up the Big Brother Machine*, Klein's affidavit in EFF's lawsuit, *Hepting v. AT&T* and his groundbreaking 2006 piece for *Wired Magazine*).

The FBI "uses government equipment on private company property to retrieve matching information from a participating company, such as Microsoft or Yahoo and pass it without further review to the NSA." (see Verizon whistleblower Babak Pasdar's affidavit on how FBI "tasking" is accomplished via its Quantico circuit).

"For stored communications, but not for live surveillance" we're informed that the Bureau's Electronic Communications Surveillance Unit (ECSU) "consults its own databases to make sure the selectors do not match known Americans."

If this is what the Bureau is now claiming, it is disingenuous at best. In fact, as *Antifascist Calling* reported back in 2009, the FBI's Investigative Data Warehouse (IDW), a virtual Library of Babel, is a content management and data mining system with the ability to access and analyze aggregated data from some fifty hitherto separate datasets. That the Bureau would feel compelled to "minimize" domestic information it provides to a "sister" agency beggars belief.

In fact, one of the new PRISM slides reveal that from "the FBI's interception unit on the premises of private companies, the information is passed to one or more 'customers' at the NSA, CIA or FBI."

"Depending on the company," Barton Gellman and Todd Lindeman report, "a tasking may return e-mails, attachments, address books, calendars, files stored in the cloud, text or audio or video chats and 'metadata' that identify the locations, devices used and other information about a target."

Elapsed times from "tasking to response" from the above-named firms or other "partners" such as banks, credit card companies, etc. range from "minutes to hours." An unnamed

“senior intelligence official” told the *Post*, “Much as we might wish otherwise, the latency is not zero.”

“After communications information is acquired,” the data is “processed and analyzed by specialized systems that handle voice, text, video and ‘digital network information’ that includes the locations and unique device signatures of targets.”

We also learn how some of these code named systems function.

For example, PRINTURA is described as a tool “which automates the traffic flow.” The *Post* reports that “the same FBI-run equipment sends the search results to the NSA.” Once it is received, in bulk, “PRINTURA sorts and dispatches the data stream through a complex sequence of systems that extract and process voice, text, video and metadata.”

Once dispatched from PRINTURA, described as a “librarian and traffic cop,” SCISSORS and Protocol Exploitation “sort data types for analysis in NUCLEON (voice), PINWALE (video), MAINWAY (call records) and MARINA (internet records).”

While the *Post* claims that “systems identified as FALLOUT and CONVEYANCE appear to be the final filtering to reduce the intake of information about Americans,” information provided by NSA whistleblower William Binney dispute such assertions.

In fact, Binney told investigative journalist James Bamford for his *Wired Magazine* piece on NSA’s giant Utah Data Center, that the agency “could have installed its tapping gear at the nation’s cable landing stations–the more than two dozen sites on the periphery of the US where fiber-optic cables come ashore. If it had taken that route, the NSA would have been able to limit its eavesdropping to just international communications, which at the time was all that was allowed under US law.”

“Instead,” the former cofounder of the agency’s Signals Intelligence Automation Research Center (SARC) told Bamford that NSA “chose to put the wiretapping rooms at key junction points throughout the country–large, windowless buildings known as switches–thus gaining access to not just international communications but also to most of the domestic traffic flowing through the US.”

“The network of intercept stations goes far beyond the single room in an AT&T building in San Francisco exposed by a whistle-blower in 2006. ‘I think there’s 10 to 20 of them,’ Binney says. ‘That’s not just San Francisco; they have them in the middle of the country and also on the East Coast’.”

In other words, NSA’s network of “secret rooms” were installed at key junctures that would facilitate, not “minimize” wholesale domestic surveillance.

Expanding on just how intrusive NSA “collection” programs are, Binney told *The New Yorker* in a Jane Mayer piece on the Obama regime’s prosecution of NSA whistleblower Thomas Drake, that a surveillance program he helped design as SARC director, ThinThread, was “bastardized” after 9/11 and “stripped of privacy controls” that would filter out Americans’ communications.

“‘It was my brainchild,’ Binney told Mayer. “‘But they removed the protections, the anonymization process. When you remove that, you can target anyone.’ He said that although he was not ‘read in’ to the new secret surveillance program, ‘my people were

brought in, and they told me, ‘Can you believe they’re doing this? They’re getting billing records on US citizens! They’re putting pen registers’–logs of dialed phone numbers–‘on everyone in the country!'”

And they continue to do so today without one iota of oversight from a thoroughly compromised Congress.

New Programs Exposed

The programs described above all evolved from the Bush administration’s so-called President’s Surveillance Program, PSP, which has continued under Obama. As *Antifascist Calling* reported in 2009, citing a declassified 38-page report by inspectors general of the CIA, NSA, the Departments of Defense, Justice and the Office of the Director of National Intelligence, the report failed to disclose what these programs actually do, claiming they are “too sensitive” for an “unclassified setting.”

Shrouded beneath impenetrable layers of secrecy and deceit, these undisclosed programs lie at the dark heart of the state’s war against the American people.

For example, the DOJ’s Office of the Inspector General described FBI participation in the PSP as that of a “passive recipient of intelligence collected under the program.” Recent revelations by Edward Snowden expose such statements as bald-faced lies. And when the OIG claimed that Bureau efforts “to improve cooperation with the NSA to enhance the usefulness of PSP-derived information to FBI agents,” that too, is a craven misrepresentation given what we now know about the key role the FBI plays in NSA’s PRISM program.

However, the unclassified version of NSA’s Inspector General’s report on the PSP published by *The Guardian* paints a far-different picture.

A close reading of the document reveals that a federal judge sitting on the FISA would approve a bulk collection order for metadata “every 90 days,” as long as it “involved” the “communications with at least one communicant outside the United States or for which no communicant was known to be a citizen of the United States”.

“Eventually,” Glenn Greenwald and Spencer Ackerman reported, the agency “gained authority to ‘analyze communications metadata associated with United States persons and persons believed to be in the United States’.”

Although the administration now claims that specific program ended in 2011, online collection of data on Americans continues today.

Last week *The Guardian* reported that NSA’s Special Source Operations (SSO) directorate running PRISM is collecting and analyzing “significant amounts of data from US communications systems in the course of monitoring foreign targets.”

“The NSA,” Greenwald and Ackerman disclosed, “called it the ‘One-End Foreign (1EF) solution’.”

That program, code named EVIL OLIVE, was intended to broaden “the scope” of what it is able to surveil and relied, “legally, on ‘FAA Authority’, a reference to the 2008 Fisa Amendments Act that relaxed surveillance restrictions.”

"This new system, SSO stated in December, enables vastly increased collection by the NSA of internet traffic. 'The 1EF solution is allowing more than 75% of the traffic to pass through the filter,' the SSO December document reads. 'This milestone not only opened the aperture of the access but allowed the possibility for more traffic to be identified, selected and forwarded to NSA repositories'."

After EVIL OLIVE's "deployment, traffic has literally doubled."

Referencing another NSA collection program, this one code named SHELL TRUMPET, an SSO official wrote that the program had just "processed its One Trillionth metadata record."

"Explaining that the five-year old program 'began as a near-real-time metadata analyzer … for a classic collection system', the SSO official noted: 'In its five year history, numerous other systems from across the Agency have come to use ShellTrumpet's processing capabilities for performance monitoring' and other tasks, such as 'direct email tip alerting'," *The Guardian* reported.

These, and hitherto as yet unknown programs, are advancing by leaps and bounds due to technological breakthroughs, the result of tens of billions of taxpayer dollars showered on the agency in wake of the 9/11 provocation. As Greenwald and Ackerman reported, "almost half of those trillion pieces of internet metadata were processed in 2012, the document detailed: 'though it took five years to get to the one trillion mark, almost half of this volume was processed in this calendar year'."

"Another SSO entry," this one dated February 6, 2013, "described ongoing plans to expand metadata collection. A joint surveillance collection operation with an unnamed partner agency yielded a new program 'to query metadata' that was 'turned on in the Fall 2012'."

Two additional programs, code named MOON LIGHT PATH AND SPINNERET, "are planned to be added by September 2013." Curiously enough, this is when NSA's Utah Data Center is slated to "go live."

In fact, these programs and their siblings are useful not simply for harvesting metadata, but for "collecting" and storing all electronic communications, including their content; hence the rather circumspect reference to "direct email tip alerting."

Fully a transatlantic affair, Greenwald and Ackerman noted that another SSO entry dated September 21, 2012 revealed that a program called TRANSIENT THURIBLE is "'a new Government Communications Head Quarters (GCHQ) managed XKeyScore (XKS) Deep Dive was declared operational.' The entry states that GCHQ 'modified' an existing program so the NSA could 'benefit' from what GCHQ harvested."

There is much we do not yet know about these programs, how "collected" data is exploited by government agencies, nor the present and future implications for civil liberties and privacy in the United States and globally. What we do know however, is that the Obama administration, including their national security spokespeople and their media and political apologists are lying.

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

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