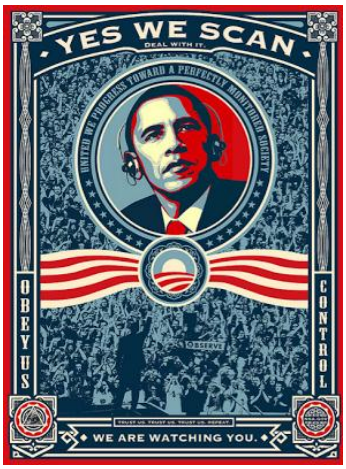
http://www.globalresearch.ca/the-obama-regime-what-the-nsa-revelations-tell-us-about-americas-police-state/5339151

The Obama Regime: What the NSA Revelations Tell Us about America's Police State

By Tom Burghardt
June 15, 2013

Ongoing revelations by *The Guardian* and *The Washington Post* of massive, illegal secret state surveillance of the American people along with advanced plans for waging offensive cyberwarfare on a global scale, including inside the US, underscores what *Antifascist Calling* has reported throughout the five years of our existence: that democracy and democratic institutions in the United States are dead letters.

Last week, *Guardian* investigative journalist Glenn Greenwald revealed that NSA "is currently collecting the telephone records of millions of US customers of Verizon, one of America's largest telecoms providers, under a top secret court order issued in April."



That order from the FISA court "requires Verizon on an 'ongoing, daily basis' to give the NSA information on all telephone calls in its systems, both within the US and between the US and other countries."

"The document shows for the first time that under the Obama administration the communication records of millions of US citizens are being collected indiscriminately and in bulk–regardless of whether they are suspected of any wrongdoing."

The latest revelations track directly back to what *USA Today* reported in 2006:

"The National Security Agency has been secretly collecting the phone call records of tens of millions of Americans, using data provided by AT&T, Verizon and BellSouth," and that secretive NSA program "reaches into homes and businesses across the nation by amassing information about the calls of ordinary Americans–most of whom aren't suspected of any crime."

"'It's the largest database ever assembled in the world,' said one person, who, like the others who agreed to talk about the NSA's activities, declined to be identified by name or affiliation. The agency's goal is 'to create a database of every call ever made' within the nation's borders," *USA Today* disclosed.

Mission accomplished!

The publication of the FISA order confirms what whistleblowers such as former AT&T technician Mark Klein, Babak Pasdar, as well as NSA insiders William Binney, Russell Tice and Thomas Drake have been warning for years: the architecture of an American police state is not only in place but fully functioning.

According to Binney, just one Narus STA 6400 "traffic analyzer" installed in one of AT&T's "secret rooms" exposed by Klein (there are upwards of 20 scattered across the United States) can can analyze 1,250,000 1,000-character emails every second, or some 100 billion emails a day.

While the Obama administration and their coterie of media flacks argue that these programs are "legal," we would do well to recall that in 2009, *The New York Times* reported that NSA "intercepted private e-mail messages and phone calls of Americans in recent months on a scale that went beyond the broad legal limits established by Congress last year."

Although Justice Department and intelligence officials described NSA's massive communications' dragnet as simple "overcollection" that was "unintentional," documents published so far expose such statements for what they are: lies.

Babak Pasdar's Verizon Disclosure

More than five years ago I wrote that "a new FISA whistleblower has stepped forward with information about a major wireless provider apparently granting the state unrestricted access to all of their customers' voice communications and electronic data via a so-called 'Quantico Circuit'."

That whistleblower, Babak Pasdar, the CEO of Bat Blue, revealed in a 2008 affidavit filed with the Government Accountability Project (GAP) that Verizon maintained a high-speed DS-3

digital line that allowed the FBI, the agency which oversees the "Quantico Circuit," virtually "unfettered" access to Verizon's wireless network, including billing records and customer data "transmitted wirelessly."

A year prior to Pasdar's disclosure, *Wired Magazine* revealed that the FBI was deploying malware which it described as a "computer and internet protocol address verifier," or CIPAV, to spy on selected targets.

Wired disclosed, citing a court affidavit filed in US District Court in the Western District of Washington, that "the spyware program gathers a wide range of information, including the computer's IP address; MAC address; open ports; a list of running programs; the operating system type, version and serial number; preferred internet browser and version; the computer's registered owner and registered company name; the current logged-in user name and the last-visited URL."

Compare *Wired's* description of CIPAV with what we have learned about the NSA's black program, PRISM, from *The Guardian* and *The Washington Post*.

According to Glenn Greenwald and Ewen MacAskill's reporting in *The Guardian*: "The program facilitates extensive, in-depth surveillance on live communications and stored information." Additionally, one "chart prepared by the NSA, contained within the top-secret document obtained by the Guardian, underscores the breadth of the data it is able to obtain: email, video and voice chat, videos, photos, voice-over-IP (Skype, for example) chats, file transfers, social networking details, and more."

"Once that data is gathered," *Wired* reported in 2007, "the CIPAV begins secretly monitoring the computer's internet use, logging every IP address to which the machine connects," and sends that data "to a central FBI server located somewhere in eastern Virginia."

"The server's precise location wasn't specified, but previous FBI internet surveillance technology–notably its Carnivore packet-sniffing hardware–was developed and run out of the bureau's technology laboratory at the FBI Academy in Quantico, Virginia."

According to Pasdar, with such access the FBI and the NSA are allowed to listen in and record all conversations en-masse; collect and record mobile phone data en-masse; obtain the data that a subscriber accessed from their mobile phone, including internet access, email and web queries; trend individual call patterns and call behavior; identify inbound and outbound callers; track all inbound and outbound calls and trace the user's physical location.

And as we learned last week from *The Guardian* and *The Washington Post*, the secret state's technical capabilities have evolved by whole orders of magnitude since initial stories of secret government surveillance were first reported nearly eight years ago by *The New York Times*.

For example, under NSA's internet-tapping PRISM program the *Guardian* and *Post* revealed that "nine leading US Internet companies," have given over access to their central servers to the FBI and NSA, thereby enabling high-tech spooks to extract "audio and video chats, photographs, e-mails, documents, and connection logs."

So pervasive, and intrusive, are these programs, that the whistleblower who revealed their existence, who we now know is former CIA technical specialist Edward Snowden, who had "firsthand experience with these systems, and horror at their capabilities," are what led him "to

provide PowerPoint slides about PRISM and supporting materials to *The Washington Post* in order to expose what he believes to be a gross intrusion on privacy. 'They quite literally can watch your ideas form as you type'," the officer said."

Hints of the frightening capabilities of these, and other as yet unknown programs, had been revealed years earlier.

When Pasdar was in the process of migrating Verizon servers and installing a newer and more secure set of firewalls, the security specialist discovered an unnamed "third party" had installed the above-mentioned DS-3 line, a "45 megabit per second circuit that supports data and voice communications."

Stunned when he learned that Verizon officials insisted the circuit should "not have any access control" and "should not be firewalled," Pasdar was told in no uncertain terms that the "owners" of the DS-3 line specified that no record of its existence should ever be made.

"'Everything at the least SHOULD be logged,' I emphasized."

"I don't think that is what they want."

A top project manager who drove out to the site warned Pasdar to "forget about the circuit" and "move on" with the migration. He was further warned that if he "couldn't do that then he would get someone who could."

When the manager left, Pasdar asked one of his Verizon colleagues, "Is that what I think it is?"

"What do you think?", he replied.

"I shifted the focus. 'Forgetting about who it is, don't you think it is unusual for some third party to have completely open access to your systems like this? You guys are even firewalling your internal offices, and they are part of your own company!'"

His colleague replied, "Dude, that's what they want."

"I didn't bother asking who 'they' were this time. 'They' now had a surrogate face,'" top manager dubbed "DS" by Pasdar. "They told me that 'they' went all the way to the top [of Verizon], which is why the once uncertain DS could now be so sure and emphatic."

Disturbed that Verizon was turning over access of their communications infrastructure to secret government agencies, Pasdar wrote: "For the balance of the evening and for some time to come I thought about all the systems to which this circuit had complete and possibly unfettered access. The circuit was tied to the organization's core network. It had access to the billing system, text messaging, fraud detection, web site, and pretty much all the systems in the data center without apparent restrictions."

"What really struck me," Pasdar noted, "was that it seemed no one was logging any of the activity across this circuit. And if they were, the logging system was so abysmal that they wouldn't capture enough information to build any type of a picture of what had transpired. Who knew what was being sent across the circuit and who was sending it? To my knowledge no historical logs of the communications traversing the 'Quantico Circuit' exists."

The security consultant affirmed that government snoops "may be able to access the billing system to find information on a particular person. This information may include their billing

address, phone number(s), as well as the numbers and information of other people on the plan. Other information could also include any previous numbers that the person or others on their plan called, and the outside numbers who have called the people on the plan."

And once the Electronic Security Number (ESN) of any plan member's phone has been identified, well, the sky's the limit!

"With the ESN information and access to the fraud detection systems, a third party can locate or track any particular mobile device. The person's call patterns and location can be trended and analyzed."

"With the ESN," Pasdar averred, "the third party could tap into any and all data being transmitted from any particular mobile device. This would include Internet usage, e-mails, web, file transfers, text messages and access to any remote applications."

"It would also be possible in real-time to tap into any conversation on any mobile phone supported by the carrier at any point."

While the major firms identified by *Guardian* and *Post* reporters in the PRISM disclosures deny that NSA has built backdoors into their systems, *The New York Times* revealed although Twitter declined to make it easier for the government to spy on their users, "other companies were more compliant, according to people briefed on the negotiations. They opened discussions with national security officials about developing technical methods to more efficiently and securely share the personal data of foreign users in response to lawful government requests. And in some cases, they changed their computer systems to do so."

According to the *Times*, the "companies that negotiated with the government include Google, which owns YouTube; Microsoft, which owns Hotmail and Skype; Yahoo; Facebook; AOL; Apple; and Paltalk, according to one of the people briefed on the discussions," the same tech giants called out by the PRISM revelations.

"In at least two cases, at Google and Facebook," reporter Claire Cain Miller disclosed, "one of the plans discussed was to build separate, secure portals, like a digital version of the secure physical rooms that have long existed for classified information, in some instances on company servers. Through these online rooms, the government would request data, companies would deposit it and the government would retrieve it, people briefed on the discussions said."

So much for their non-denial denials!

More pertinently however, the "digital version of the secure physical rooms" described by the *Times* track directly back to what whistleblower Mark Klein told *Wired*, along with supporting documents in 2006, about AT&T's secret Room 641A housed in San Francisco.

Klein revealed: "In 2003 AT&T built 'secret rooms' hidden deep in the bowels of its central offices in various cities, housing computer gear for a government spy operation which taps into the company's popular WorldNet service and the entire internet. These installations enable the government to look at every individual message on the internet and analyze exactly what people are doing. Documents showing the hardwire installation in San Francisco suggest that there are similar locations being installed in numerous other cities."

And as with the "separate, secure portals" described by the *Times*, AT&T's "secret rooms" are staffed with NSA-cleared corporate employees of the tech giants.

Klein informed us:

"The normal work force of unionized technicians in the office are forbidden to enter the 'secret room,' which has a special combination lock on the main door. The telltale sign of an illicit government spy operation is the fact that *only people with security clearance from the National Security Agency can enter this room*." (emphasis in original)

How Extensive Is the Surveillance? Well, Boundless!

Back in 2008, *The Wall Street Journal* reported that NSA "now monitors huge volumes of records of domestic emails and Internet searches as well as bank transfers, credit-card transactions, travel and telephone records. The NSA receives this so-called 'transactional' data from other agencies or private companies, and its sophisticated software programs analyze the various transactions for suspicious patterns."

With the Verizon and PRISM disclosures, we now know who those "private companies" are: major US high tech and telecommunications giants.

Journalist Siobhan Gorman revealed that the NSA's "enterprise involves a cluster of powerful intelligence-gathering programs, all of which sparked civil-liberties complaints when they came to light. They include a Federal Bureau of Investigation program to track telecommunications data once known as Carnivore, now called the Digital Collection System, and a U.S. arrangement with the world's main international banking clearinghouse to track money movements."

"The effort also ties into data from an ad-hoc collection of so-called 'black programs' whose existence is undisclosed, the current and former officials say."

Amongst the "black programs" disclosed by *The Guardian*, we learned last week that through the NSA's top secret Boundless Informant program the agency "has developed a powerful tool for recording and analysing where its intelligence comes from, raising questions about its repeated assurances to Congress that it cannot keep track of all the surveillance it performs on American communications."

As Glenn Greenwald and Ewen MacAskill disclosed, the "Boundless Informant documents show the agency collecting almost 3 billion pieces of intelligence from US computer networks over a 30-day period ending in March 2013. One document says it is designed to give NSA officials answers to questions like, 'What type of coverage do we have on country X' in 'near real-time by asking the SIGINT [signals intelligence] infrastructure'."

Like their Bushist predecessors, the Obama regime claims the security apparatus is "not listening in" to the phone calls of Americans, asserting instead they are "merely" harvesting metadata, the digital footprints and signatures of electronic devices.

But as the Electronic Frontier Foundation (EFF) points out: "Metadata provides enough context to know some of the most intimate details of your lives. And the government has given no assurances that this data will never be correlated with other easily obtained data. They may start out with just a phone number, but a reverse telephone directory is not hard to find. Given the

public positions the government has taken on location information, it would be no surprise if they include location information demands in Section 215 orders for metadata."

Conservative estimates since the 9/11 provocation have revealed that the NSA phone database now contains upwards of 1.9 trillion call-detail records under a program code name MARINA and that a similar database for email and web queries also exists, PINWALE.

The FISA court order signed in April by Judge Roger Vinson directs Verizon to hand over to the NSA "on an ongoing daily basis thereafter for the duration of this order, unless otherwise directed by the Court, an electronic copy of the following tangible things: all call detail records or 'telephony metadata' created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls."

One can only assume that other carriers such as AT&T and Sprint have been issued similar orders by the FISA court.

According to the Order,

"Telephony metadata includes comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (ISMI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call."

While the order specifies that "telephony metadata" does not include the "substantive content of any communication" or "the name, address, or financial information of a subscriber or customer," that information, should an individual come in for "special handling" by the secret state, call and internet content is fully-retrievable, courtesy of US high-tech firms, under the MARINA, PINWALE and PRISM programs.

As the heroic whistleblower Edward Snowden told *The Guardian* last Sunday: "The NSA has built an infrastructure that allows it to intercept almost everything. With this capability, the vast majority of human communications are automatically ingested without targeting. If I wanted to see your emails or your wife's phone, all I have to do is use intercepts. I can get your emails, passwords, phone records, credit cards."

"What they're doing," Snowden said, poses "an existential threat to democracy."

If what the Bush and now, Obama regimes are doing is not Orwellian blanket surveillance of the American people, then words fail.