GlobalResearch
Center for Research on Globalization

NSA Spying and Intelligence Collection: A Giant Blackmail Machine and "Warrantless Wiretapping" Program

Bipartisan Consensus that seeks to Criminalize the leak and not the Illegality of the Programs Exposed

By Tom Burghardt
Global Research, June 24, 2013
Antifascist Calling…

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

Despite a stream of mendacious twaddle from President Obama, congressional grifters and spook agency mouthpieces like Office of the Director of National Intelligence head James Clapper, FBI Director Robert Mueller and NSA chief General Keith Alexander, it turns out our guardians are listening in to America's, and most of the world's, telephone conversations after all.

In the wake of the Boston Marathon bombing, former FBI counter-terrorism agent Tim Clemente was asked by CNN whether there's a way that investigators "can get the phone companies" to cough up audio of a particular conversation.

Clemente responded: "No, there is a way. We certainly have ways in national security investigations to find out exactly what was said in that conversation. It's not necessarily something that the FBI is going to want to present in court, but it may help lead the investigation and/or lead to questioning of her [the alleged bomber's wife]. We certainly can find that out."

CNN's incredulous reply: "So they can actually get that? People are saying, look, that is incredible."

Clemente: "No, welcome to America. All of that stuff is being captured as we speak whether we know it or like it or not."

When questioned the next day whether he would confirm his previous statements, Clemente told CNN, "I'm talking about all digital communications are–there's a way to look at digital communications in the past. I can't go into detail of how that's done or what's done. But I can tell you that no digital communication is secure. So these communications will be found out. The conversation will be known."

While there was scant media follow-up to Clemente's assertions, recent revelations of NSA dragnet spying have confirmed what analysts, researchers and whistleblowers have been saying for years: the secret state has the technological wherewithal to digitally record the content of all electronic communications, including telephone calls, and store them in massive cloud computing server farms in the event they're needed for future "reference."

And as it turns out, according to Internet Archive founder, computer engineer Brewster

Kahle, who has wide experience storing large amounts of data, the cost of doing so is incredibly cheap.

A spreadsheet created by Kahle estimates it would cost the government a mere $27 million to "store all phonecalls made in a year in the 'cloud'." To do so would require less than 5,000 square feet of space and $2 million in electricity costs to store the estimated 272 petabytes of data generated annually in the United States!

A Giant Blackmail Machine

Recent disclosures by NSA whistleblower Edward Snowden have done much to dispel remaining myths (government spying is "focused," "legal," etc.) surrounding the secret state's privacy-killing surveillance programs.

It now seems likely that NSA is hoovering up far more than the "telephony metadata" revealed by *The Guardian's* publication of the secret FISA Court Order to Verizon Business Services.

Following-up on PRISM program reporting, *The Washington Post* disclosed June 15 that the Bush administration's "warrantless wiretapping" program STELLAR WIND "was succeeded by four major lines of intelligence collection in the territorial United States, together capable of spanning the full range of modern telecommunications, according to the interviews and documents."

"Two of the four collection programs, one each for telephony and the Internet," Barton Gellman reported, "process trillions of 'metadata' records for storage and analysis in systems called MAINWAY and MARINA, respectively."

According to the *Post*, "Metadata includes highly revealing information about the times, places, devices and participants in electronic communication, but not its contents. The bulk collection of telephone call records from Verizon Business Services, disclosed this month by the British newspaper the Guardian, is one source of raw intelligence for MAINWAY."

Dropping a bombshell, although withholding supporting documents, Gellman reports that the "other two types of collection, which operate on a much smaller scale, are aimed at content. One of them intercepts telephone calls and routes the spoken words to a system called NUCLEON."

> "MARINA and the collection tools that feed it are probably the least known of the NSA's domestic operations," the Post averred. "Yet they probably capture information about more American citizens than any other, because the volume of e-mail, chats and other Internet communications far exceeds the volume of standard telephone calls."
>
> "The NSA calls Internet metadata 'digital network information.' Sophisticated analysis of those records can reveal unknown associates of known terrorism suspects. Depending on the methods applied, it can also expose medical conditions, political or religious affiliations, confidential business negotiations and extramarital affairs."

In other words, it seems likely that harvested data gleaned from phone calls, emails, video chats and credit card records are being used in ways that are as old as the spy game itself:

political and economic *blackmail*.

Indeed, NSA whistleblower Russ Tice, the principal source for *The New York Times* exposé of illegal Bush administration spy programs, told Sibel Edmonds' *Boiling Frogs Post* podcast that the secret state has ordered surveillance on a wide range of groups and individuals, including antiwar activists, high-ranking military officials, lawmakers and diplomats.

According to Tice:

> "Okay. They went after–and I know this because I had my hands literally on the paperwork for these sort of things–they went after high-ranking military officers; they went after members of Congress, both Senate and the House, especially on the intelligence committees and on the armed services committees and some of the–and judicial. But they went after other ones, too. They went after lawyers and law firms. All kinds of–heaps of lawyers and law firms. They went after judges. One of the judges is now sitting on the Supreme Court that I had his wiretap information in my hand. Two are former FISA court judges. They went after State Department officials. They went after people in the executive service that were part of the White House–their own people. They went after antiwar groups. They went after US international–US companies that that do international business, you know, business around the world. They went after US banking firms and financial firms that do international business. They went after NGOs that–like the Red Cross, people like that that go overseas and do humanitarian work. They went after a few antiwar and civil rights groups. So, you know, don't tell me that there's no abuse, because I've had this stuff in my hand and looked at it."
>
> "Here's the big one," Tice told hosts Sibel Edmonds and Peter B. Collins, "this was in summer of 2004, one of the papers that I held in my hand was to wiretap a bunch of numbers associated with a 40-something-year-old wannabe senator for Illinois. You wouldn't happen to know where that guy lives right now would you? It's a big white house in Washington, D.C. That's who they went after, and that's the president of the United States now."

Other political targets revealed by Tice included *all nine* Supreme Court justices, Senate Intelligence Committee head Dianne Feinstein (D-CA), Sen. John McCain (R-AZ), House Minority leader Nancy Pelosi (D-CA) and ousted CIA director General David Petraeus, who allegedly resigned over a sex scandal.

Is it any wonder then, that House and Senate leaders driving the "oversight" clown car are the ones now braying loudest for Ed Snowden's head!

Like ECHELON, Only on Steroids

A new series of disclosures published by *The Guardian*, based on the Snowden files but, like the *Post*, without public disclosure of the actual documents, we learned that Britain's Government Communications Headquarters (GCHQ) "has secretly gained access to the network of cables which carry the world's phone calls and internet traffic and has started to process vast streams of sensitive personal information which it is sharing with its American partner, the National Security Agency (NSA)."

"The sheer scale of the agency's ambition is reflected in the titles of its two principal components: Mastering the Internet and Global Telecoms Exploitation, aimed at scooping up as much online and telephone traffic as possible," *The Guardian* reported.

Britain's "Mastering the Internet" scheme was first reported by *The Register* and *The Sunday Times* back in 2009; *Antifascist Calling* published an analysis of NSA's key role in the GCHQ program; a few months later, citing documents posted by WikiLeaks, *AFC* commented on the cozy relations amongst private intelligence contractors, the European Union and the secret state.

The architecture of these highly intrusive, illegal programs was created decades ago however, in intelligence-sharing arrangements in the English speaking world under the rubric of NSA's global surveillance network known as ECHELON.

As one of the "Five Eyes" partner agencies of the Cold War-era UKUSA Security Agreement (US, UK, Canada, Australia and New Zealand) exposed by journalists Duncan Campbell and Nicky Hager in their ECHELON investigations, GCHQ, through a contemporary operation code named TEMPORA, has tapped into and stored vast quantities of data gleaned from fiber optic cables passing through the UK.

"This includes recordings of phone calls, the content of email messages, entries on Facebook and the history of any internet user's access to websites–all of which is deemed legal, even though the warrant system was supposed to limit interception to a specified range of targets," *The Guardian* reported.

But as we know from Campbell and Hager's reporting, while intelligence and law enforcement officials in Britain and the United States are required to obtain an *individualized* warrant to target a suspect's communications in their own nation, *no such restrictions apply* should one of the five "partner agencies" spy on another country's citizens. One must assume this arrangement continues today.

"The documents reveal that by last year GCHQ was handling 600m 'telephone events' each day," *The Guardian* disclosed, and "had tapped more than 200 fibre-optic cables and was able to process data from at least 46 of them at a time."

That GCHQ did so on the basis of "secret agreements with commercial companies, described in one document as 'intercept partners'," should come as now surprise to readers of this blog.

According to Snowden documents "seen" but not published by *The Guardian*, "some companies have been paid for the cost of their co-operation and GCHQ went to great lengths to keep their names secret. They were assigned 'sensitive relationship teams' and staff were urged in one internal guidance paper to disguise the origin of 'special source' material in their reports for fear that the role of the companies as intercept partners would cause 'high-level political fallout'."

"It's not just a US problem. The UK has a huge dog in this fight," Snowden told *The Guardian*. "They [GCHQ] are worse than the US."

The latest revelations have certainly raised eyebrows in Hong Kong and China, long accused by US political hacks of waging "aggressive cyberwarfare" against US defense and financial networks.

On Sunday, the *South China Morning Post* disclosed that "US spies are hacking into Chinese mobile phone companies to steal text messages and attacking the servers at Tsinghua University," according to documents provided to the *Post* by Edward Snowden.

The *Post* revealed that the US is "hacking" computers "at the Hong Kong headquarters of Pacnet, which owns one of the most extensive submarine cable networks in the region."

"Pacnet," the Hong Kong newspaper explained, "recently signed major deals with the mainland's top mobile phone companies, owns more than 46,000 kilometres of fibre-optic cables. The cables connect its regional data centres across the Asia-Pacific region, including Hong Kong, the mainland, Japan, South Korea, Singapore and Taiwan. It also has offices in the US."

Talk about the (US) pot calling the (Chinese) kettle black!

NSA Data Fed to Main Core Security Index?

As sinister as these programs are, is there another component which taps "into data from an ad-hoc collection of so-called 'black programs' whose existence is undisclosed," as alluded to by *The Wall Street Journal* five years ago?

In a recent interview with the conservative web site, *The Daily Caller*, former NSA technical director and whistleblower William Binney said while he doesn't think "they're recording all of it," what they do however, "is take their target list, which is somewhere on the order of 500,000 to a million people. They look through these phone numbers and they target those and that's what they record."

"500,000 to a million people"? Who are they? Foreign citizens, Americans? If the latter, is Binney's statement confirmation of reporting by journalists Christopher Ketchum and Tim Shorrock about the existence of a secret "Continuity of Government" database of "suspect" Americans known as Main Core?

"One knowledgeable source claims that 8 million Americans are now listed in Main Core as potentially suspect," Ketchum reported. "In the event of a national emergency, these people could be subject to everything from heightened surveillance and tracking to direct questioning and possibly even detention."

As we now know, US government intelligence agencies including the CIA, DHS, the FBI, military outfits such as US Northern Command and the 70-odd "public-private" fusion centers scattered across the country have spied on antiwar activists, Ron Paul supporters, anarchists, socialists, gun rights' proponents and, as revealed by journalist Beau Hodai in his troubling report, *Dissent or Terror*, Occupy Wall Street.

Did all the data secretly scooped up on law-abiding Americans exercising their constitutionally protected right to free speech wind up in the government's ultra-secret Main Core security index?

> "Another well-informed source–a former military operative regularly briefed by members of the intelligence community" told Ketchum: "'The more data you have on a particular target, the better [the software] can predict what the target will do, where the target will go, who it will turn to for help,' he says. 'Main Core is the table of contents for all the illegal information that the U.S. government has [compiled] on specific targets.' An intelligence expert who has been briefed by high-level contacts in the Department of Homeland Security confirms that a database of this sort exists, but adds that 'it is less a mega-database than a way to search numerous other agency databases at the same time'."

> A few months after Ketchum's report appeared, Shorrock informed us that during an interview with financial consultant Norman Bailey, who headed "a special unit within the Office of the Director of National Intelligence focused on financial intelligence on Cuba and Venezuela–the NSA has been using its vast powers with signals intelligence to track financial transactions around the world since the early 1980s."

"After 9/11," Bailey told Shorrock, NSA signals intelligence intercept capabilities were "instantly seen within the US government as a critical tool in the war on terror–and apparently was deployed by the Bush administration inside the United States."

"In September 2001," Shorrock disclosed, "a contemporary version of the [Reagan era] Continuity of Government program was put into play in the hours after the 9/11 terrorist attacks, when Vice President Cheney and senior members of Congress were dispersed to 'undisclosed locations' to maintain government functions."

"It was during this emergency period," Shorrock wrote, "that President Bush may have authorized the NSA to begin actively using the Main Core database for domestic surveillance."

"If Main Core does exist, says Philip Giraldi, a former CIA counterterrorism officer and an outspoken critic of the agency, the Department of Homeland Security (DHS) is its likely home," Ketchum averred.

> "'If a master list is being compiled, it would have to be in a place where there are no legal issues'–the CIA and FBI would be restricted by oversight and accountability laws–'so I suspect it is at DHS, which as far as I know operates with no such restraints'."
>
> "Giraldi notes that DHS already maintains a central list of suspected terrorists and has been freely adding people who pose no reasonable threat to domestic security. 'It's clear that DHS has the mandate for controlling and owning master lists. The process is not transparent, and the criteria for getting on the list are not clear.' Giraldi continues, 'I am certain that the content of such a master list [as Main Core] would not be carefully vetted, and there would be many names on it for many reasons–quite likely, including the two of us'."

While we don't know whether Binney is referring to the NSA component of Main Core, or some other highly illegal, hitherto unknown program, his statements seem to confirm Gellman's reporting in *The Washington Post* that "spoken words" are routed "to a system called NUCLEON." Again, without publishing supporting documentation supplied by Edward Snowden, the picture is far from clear.

Recent revelations however, building on scandals surrounding the interception of the sensitive communications of Associated Press and Fox News reporters, along with President Obama's Nixonian obsession with stopping "leaks" as part of the administration's war on whistleblowers, it should be clear by now that the police state Rubicon has *already* been crossed.

In 1976, during Senate hearings into earlier government lawbreaking, Senator Frank Church warned: "The National Security Agency's capability at any time could be turned around on the American people, and no American would have any privacy left, such is the capability to

monitor everything: telephone conversations, telegrams, it doesn't matter. There would be no place to hide. If a dictator ever took over, the NSA could enable it to impose total tyranny, and there would be no way to fight back."

"I don't want to see this country ever go across the bridge," Senator Church cautioned. "I know the capacity that is there to make tyranny total in America, and we must see to it that this agency and all agencies that possess this technology operate within the law and under proper supervision, so that we never cross over that abyss. That is the abyss from which there is no return."

What should also be clear, is that the *bipartisan consensus* that seeks to criminalize the leak and not the illegality of the programs exposed, reflects the profound fear in elite Washington circles of the American people. As opposition to endless war and austerity continues to percolate below the surface, it is only a matter of time before the breaking point is reached.

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