

The NSA: Is It American, or British?

by Edward Spannaus

June 24—Recent revelations, based on NSA documents disclosed by whistleblower Edward Snowden, showing the extent of collaboration between the U.S. National Security Agency (NSA), and Her Majesty’s General Communications Headquarters (GCHQ), raise again the question of British control over vital U.S. intelligence functions, and whether the British, as well as the NSA, are targeting U.S. citizens.

Taken together with the issue of Anglo-Dutch domination of the U.S. and global financial system, the more fundamental question to be posed, is whether the United States can claim to still be a sovereign nation, when it functions as a junior partner of the British imperial faction—“perfidous Albion”—which remains steadfast in its determination to destroy the United States as a constitutional republic.

And what does this say about those so-called U.S. presidents—specifically, George W. Bush and Barack Obama—who implement this imperial policy?

A secondary question is, how can there be any official oversight of such an operation, which is controlled, in large part, from abroad? On top of the fact that an estimated 70% of all U.S. intelligence is privatized, i.e., contracted out to private contractors such as Booz Allen Hamilton—and probably an even higher percentage for the NSA—the massive interconnections between NSA and GCHQ, and the fact that so much of NSA’s data collection comes from, and goes to, GCHQ, makes a mockery of any claim that the NSA

spying program is subject to strict Congressional and court oversight.

‘Special Relationship’

Ten days before the London *Guardian* started publishing documents obtained from Snowden showing the vast scope of GCHQ telecommunications snooping and sharing with the NSA, the *Guardian’s* Defence and Security Blog published a blockbuster piece by Richard Norton-Taylor and Nick Hopkins, titled “Intelligence-gathering by British state out of control.” It begins:

“Among all the uncertainties and denials over the interception of communications by GCHQ and America’s National Security Agency some things should be crystal clear.

“The bilateral relationship between GCHQ and the NSA is uniquely special. It is the core of the ‘special relationship.’ The two agencies are truly intertwined.”

That statement in itself should immediately ring a bell with anyone who has read *EIR’s* chronology of the development of the Bush-Cheney-Obama surveillance dragnet in our June 14, 1013 issue. The third entry under “The British-U.S. Arrangement” noted the 1947 signing of the U.K.-U.S.A. Security Agreement (UKUSA), which, we noted, “represented President Harry Truman’s treasonous policy of establishing an Anglo-American ‘special relationship’—a repudiation of FDR’s policy.”¹

1. *EIR*, June 14, 2013.



Creative Commons/Tom Blackwell

Menwith Hill, in North Yorkshire, the NSA's largest listening post outside the U.S., consists of a satellite station for monitoring foreign military traffic, and is plugged into Britain's telecommunications network.

As Norton-Taylor and Hopkins explain: “There are NSA liaison officers assigned to GCHQ in Cheltenham, and GHQC officers at the NSA’s headquarters in Fort Meade, Maryland.” They note that the “RAF base” known as Menwith Hill, in North Yorkshire, is the NSA’s largest listening post outside the U.S., consisting of a satellite station for monitoring foreign military traffic, but also plugged into Britain’s telecommunications network.

They cite a 1994 GCHQ staff manual which discussed the importance of GCHQ’s contribution to the alliance with its partners, and stated: “This may entail on occasion the applying of UK resources to the meeting of US requirements.” This, of course, has been going on for a long time: Norton-Taylor and Hopkins recall that in the late 1960s, GCHQ had cooperated in the illegal eavesdropping on U.S. civil rights and anti-war activists. “With the help of a US-funded GCHQ listening station at Bude on North Cornwall, the two agencies did each other’s dirty work, getting around their domestic laws by spying on each other’s citizens.”

Always ritualistically denied, this U.S.-British arrangement, using each other to spy on their own citizens, has been going on for decades. *EIR* reported some of the ways this worked, in an April 2000 report on the

“Echelon” controversy.² One loophole, described by *Puzzle Palace* author James Bamford and others, works as follows:

The Foreign Intelligence Surveillance Act (FISA), passed in 1978, speaks of “acquisition,” which is undefined in the statute. To fill this gap, the NSA has defined it as “interception by the National Security Agency through electronic means of a communication.” Thus, information acquired by Britain’s GCHQ, or one of the other UKUSA parties, and then passed to U.S. agencies, is *not* covered under the act.

We also noted that a U.S. Justice Department report in 1976 had reported that “CGHQ-acquired” data was given to the NSA for use in its MINARET program of U.S. domestic surveillance; this was then passed on to other U.S. agencies such as the FBI.

Norton-Taylor and Hopkins give another example of GCHQ cooperating with the NSA in a 2002-03 Bush Administration-Tony Blair “dirty tricks” campaign of

2. Patrick Radden Keefe, *Chatter: Dispatches from the Secret World of Global Eavesdropping* (2005).

bugging the homes and offices of UN diplomats from the “swing states,” whose support was needed if the U.S. and Britain were to be able to ram through a UN Security Council resolution authorizing the invasion of Iraq. This was revealed by a GCHQ whistleblower named Katherine Gun, against whom criminal charges were brought, and later dropped, so that evidence of the illegal spying would not come out in a courtroom.

According to Bamford, the NSA tasked Britain and the other members of the UKUSA, or “Five Eyes” alliance—Canada, Australia, and New Zealand—with eavesdropping on the diplomats. (Under the post-war UKUSA agreement, the parties divided the world among themselves, at least for purposes of surveillance.)

Norton-Taylor and Hopkins make an obvious point

Senators Challenge Value of NSA Surveillance Programs

This statement was released on June 19, 2013.

Washington, D.C.—U.S. Senators Ron Wyden (D-Ore.) and Mark Udall (D-Colo.) issued the following statement, responding to comments made by members of the Intelligence Community about the value of certain NSA surveillance programs. Both Senators sit on the Senate Intelligence Committee.

“Over the past few days the Intelligence Community has made new assertions about the value of recently declassified NSA surveillance programs. In addition to the concerns that we have about the impact of large-scale collection on the civil liberties of ordinary Americans, we are also concerned that the Foreign Intelligence Surveillance Act (FISA) Section 702 collection program (which allows collection of phone or internet communications, and involves the PRISM computer system) and the bulk phone records collection program operating under Section 215 of the USA PATRIOT ACT are being conflated in a way that exaggerates the value and usefulness of the bulk phone records collection program.

“Based on the evidence that we have seen, it appears that multiple terrorist plots have been disrupted at least in part because of information obtained under section 702 of FISA. However, it appears that the bulk phone records collection program under section 215 of the USA Patriot Act played little or no role in most of these disruptions. Saying that “these programs” have disrupted “dozens of potential terrorist plots” is misleading if the bulk phone records collec-

tion program is actually providing little or no unique value.

“The Intelligence Community notes that the massive collection of phone records under Section 215 has provided some relevant information in a few terrorism cases, but it is still unclear to us why agencies investigating terrorism do not simply obtain this information directly from phone companies using a regular court order. If the NSA is only reviewing those records that meet a “reasonable suspicion” standard, then there is no reason it shouldn’t be able to get court orders for the records it actually needs. Making a few hundred of these requests per year would clearly not overwhelm the FISA Court. And the law already allows the government to issue emergency authorizations to get these records quickly in urgent circumstances. The NSA’s five-year retention period for phone records is longer than the retention period used by some phone companies, but the NSA still has not provided us with any examples of instances where it relied on its bulk collection authority to review records that the relevant phone company no longer possessed.

“In fact, we have yet to see any evidence that the bulk phone records collection program has provided any otherwise unobtainable intelligence. It may be more convenient for the NSA to collect this data in bulk, rather than directing specific queries to the various phone companies, but in our judgment convenience alone does not justify the collection of the personal information of huge numbers of ordinary Americans if the same or more information can be obtained using less intrusive methods.

“If there is additional evidence for the usefulness of the bulk phone records collection program that we have not yet seen, we would welcome the opportunity to review it.”

about oversight of GCHQ and NSA in Britain, which is equally valid for the U.S.: “Ministers and commissioners (former senior judges) appointed to monitor GCHQ’s activities cannot possibly know the content or the quantity, of all the data the agency collects on a daily basis.” (Which reminds us of what former NSA employee and whistleblower William Binney has said regarding Congressional oversight, that Congress is being given “techno-babble . . . even when they get briefings, they still don’t understand.”)

Tempora: A Joint GCHQ-NSA Project

Further indication of the vast scope of “sensitive personal information” being obtained by GCHQ and shared with the NSA, came on June 21, as the *Guardian* published another round of stories, based on additional NSA documents disclosed by Edward Snowden.

In early June, the first set of Snowden documents showed that the NSA had obtained direct access to Internet data by tapping directly into the servers of Internet giants such as Microsoft, Google, Yahoo, etc., through a program identified as PRISM, which reportedly began in 2007 under the Bush-Cheney Administration.

Around the same time, in 2007, according to the *Guardian*, GCHQ launched a top-secret project called “Mastering the Internet,” to determine how to better process the vast amounts of data it was collecting every day. As part of this, one experimental project was run out of the GCHQ station at Bude in Cornwall. (Bamford, in his 2008 book *The Shadow Factory*, says that the NSA actually helped to finance and build the Bude station in the 1960s.) By 2010, this was being referred to in official documents as a “joint GCHQ/NSA research initiative.”

One of its core programs for storing and analyzing this data, is known as “Tempora.” It processes up to 600 million “telephone events” a day, and 39 million gigabytes of Internet traffic. This includes, according to the *Guardian*, “voice recording, the content of emails”—in



NSA Director Keith Alexander, who has lied repeatedly about even the existence of the NSA surveillance program, asked, during a June 2008 visit to Menwith Hill: “Why can’t we collect all signals all the time? Sounds like a good summer project for Menwith.”

other words, *content* as well as metadata.

Another *Guardian* story published the same day shed some light on the source of all this data that the CGHQ and NSA are attempting to process. At some point, probably around 2007-08, GCHQ tapped into the trans-Atlantic fiber-optic cables that carry streams of telecommunications data from the U.S. to Europe. Under Tempora, all of this product is shared with the NSA.

Not only are there 300 analysts from GCHQ, and 250 from NSA, who are assigned to sift through the data, but, the *Guardian* reports, 850,000 NSA employees and private contractors with top-secret clearances, have access to the GCHQ database.

No wonder NSA Director Gen. Keith Alexander, during a June 2008 visit to Menwith Hill, was prompted to ask: “Why can’t we collect all signals all the time? Sounds like a good summer project for Menwith.”

Yes, this is the same Alexander, who, after having been caught lying about the very existence of these programs, has repeatedly declared, in his most solemn tone, that NSA cannot access the content of Americans’ communications without a court order, and who assures us that NSA surveillance programs are subject to the most stringent oversight from all three branches of the

U.S. government. Not to mention President Obama's frequent claim, that "Nobody is listening to the content of people's phone calls."

U.K.: 'Worse Than the U.S.'

By 2010, two years into the program, the U.K. had regained its predominant position among the "Five Eyes" UKUSA alliance, able to boast that it had the "biggest Internet access" of the five partners, and that it was now producing "larger amounts of metadata than the NSA."

By 2011, GCHQ had attached taps to more than 200 Internet links, each carrying data at 10 gigabits a second. "This is a massive amount of data!" an internal GCHQ slide show gushed. In the Summer of 2011, GCHQ brought NSA analysts into the trials of the Tempora program at Bude, and in the Fall of 2011, the program was fully launched and shared with the NSA—with the implication that NSA was now relegated to the status of a junior partner to the British.

And for what purpose? It has little to do with catching terrorists: That little fairy tale is only designed for the gullible. The 1994 Intelligence Services Act, the current charter for GCHQ, mandates the agency to work "in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's government in the United Kingdom; in the interests of the economic well being of the United Kingdom; or in support of the prevention and detection of serious crime."

The "economic well being" clause of this mandate is clearly taken quite seriously. In mid-June, the *Guardian* revealed that the GCHQ—with the assistance of the NSA—was listening in on diplomats at the April 2009 meeting of the G20 group of nations, and again at a meeting of finance ministers five months later. GCHQ and NSA went so far as to set up a fake "Internet cafe" where they could eavesdrop on diplomats' discussions and e-mails. British Prime Minister Gordon Brown was reported to be interested in gathering intelligence on reactions to his plans to use public funds to bail out collapsing British banks.

Is this what the NSA is involved in, under the guise of detecting terrorism?

The *Guardian* reports that some of the Snowden documents indicate that key elements of the Tempora filtering process were designed by the NSA. And, it asks, why did the NSA not just attach probes to the North American end of the trans-Atlantic cables? "In-

stead, the NSA has exported its computer programs and 250 of its analysts to operate the system from the UK."

"Initial inquiries by the *Guardian* have failed to explain why this has happened, but US legislators are likely to want to check whether the NSA has sought to bypass legal or policy requirements which restrict its activity in the US. This will be particularly sensitive if it is confirmed that Tempora is also analysing internal U.S. traffic."

The *Guardian* also notes that its interviews with both a U.K. source, and with Snowden, raise a number of questions, including whether the Tempora program: "Allows the NSA to engage in bulk intercepts of internal US traffic which would be forbidden on its own territory."

The result of all this? "GCHQ and the NSA are consequently able to access and process vast quantities of communication between entirely innocent people," concludes the *Guardian*.

In disclosing the NSA documents pertaining to the GCHQ, Snowden told the *Guardian* that he wanted to show that, "It's not just a US problem. The UK has a huge dog in this fight. They are worse than the US."

edspannaus@verizon.net

EIR Special Report

Obama's War on America: 9/11 Two

NEW, UPDATED EDITION

A new, updated edition of the EIR Special Report, "Obama's War on America: 9/11 Two" is now available from larouchepub.com. The expanded report is an urgent intervention into the ongoing strategic crisis brought on by the British/Saudi/Obama alliance behind the overthrow of Qaddafi, and the subsequent explosion of jihadist uprisings throughout Africa and the Arab world.

THE ORIGINAL MATERIAL:

- Obama's 9/11
- The London-Saudi Role in International Terrorism
- 9/11 Take One

THE UPDATES:

- LaRouchePAC's Fact Sheet on Obama's alliance with al-Qaeda
- LaRouchePAC's draft questions for Congress
- A transcript of the pre-election press conference held by Lyndon LaRouche and Jeffrey Steinberg on the impeachable crimes of Barack Obama.

Price **\$100** (Paperback or PDF. For paper, add shipping and handling; Va. residents add 5% sales tax)

Order from **EIR News Service** 1-800-278-3135

Or online: www.larouchepub.com

