GlobalResearch
Center for Research on Globalization

Eavesdropping on the Planet, Whistleblowers and Edward Snowden

By William Blum
Global Research, June 26, 2013
The Anti-Empire Report

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

In the course of his professional life in the world of national security Edward Snowden must have gone through numerous probing interviews, lie detector examinations, and exceedingly detailed background checks, as well as filling out endless forms carefully designed to catch any kind of falsehood or inconsistency. The *Washington Post* (June 10) reported that "several officials said the CIA will now undoubtedly begin reviewing the process by which Snowden may have been hired, seeking to determine whether there were any missed signs that he might one day betray national secrets."

Yes, there was a sign they missed – Edward Snowden had something inside him shaped like a conscience, just waiting for a cause.

It was the same with me. I went to work at the State Department, planning to become a Foreign Service Officer, with the best – the most patriotic – of intentions, going to do my best to slay the beast of the International Communist Conspiracy. But then the horror, on a daily basis, of what the United States was doing to the people of Vietnam was brought home to me in every form of media; it was making me sick at heart. My conscience had found its cause, and nothing that I could have been asked in a pre-employment interview would have alerted my interrogators of the possible danger I posed because I didn't know of the danger myself. No questioning of my friends and relatives could have turned up the slightest hint of the radical anti-war activist I was to become. My friends and relatives were to be as surprised as I was to be. There was simply no way for the State Department security office to know that I should not be hired and given a Secret Clearance. 1

So what is a poor National Security State to do? Well, they might consider behaving themselves. Stop doing all the terrible things that grieve people like me and Edward Snowden and Bradley Manning and so many others. Stop the bombings, the invasions, the endless wars, the torture, the sanctions, the overthrows, the support of dictatorships, the unmitigated support of Israel; stop all the things that make the United States so hated, that create all the anti-American terrorists, that compel the National Security State – in pure self defense – to spy on the entire world.

Eavesdropping on the planet

The above is the title of an essay that I wrote in 2000 that appeared as a chapter in my book *Rogue State: A Guide to the World's Only Superpower*. Here are some excerpts that may help to put the current revelations surrounding Edward Snowden into perspective …

Can people in the 21st century imagine a greater invasion of privacy on all of earth, in all of

history? If so, they merely have to wait for technology to catch up with their imagination.

Like a mammoth vacuum cleaner in the sky, the National Security Agency (NSA) sucks it all up: home phone, office phone, cellular phone, email, fax, telex … satellite transmissions, fiber-optic communications traffic, microwave links … voice, text, images … captured by satellites continuously orbiting the earth, then processed by high-powered computers … if it runs on electromagnetic energy, NSA is there, with high high tech. Twenty-four hours a day. Perhaps billions of messages sucked up each day. No one escapes. Not presidents, prime ministers, the UN Secretary-General, the pope, the Queen of England, embassies, transnational corporation CEOs, friend, foe, your Aunt Lena … if God has a phone, it's being monitored … maybe your dog isn't being tapped. The oceans will not protect you. American submarines have been attaching tapping pods to deep underwater cables for decades.

Under a system codenamed ECHELON, launched in the 1970s, the NSA and its junior partners in Britain, Australia, New Zealand, and Canada operate a network of massive, highly automated interception stations, covering the globe amongst them. Any of the partners can ask any of the others to intercept its own domestic communications. It can then truthfully say it does not spy on its own citizens.

Apart from specifically-targeted individuals and institutions, the ECHELON system works by indiscriminately intercepting huge quantities of communications and using computers to identify and extract messages of interest from the mass of unwanted ones. Every intercepted message – all the embassy cables, the business deals, the sex talk, the birthday greetings – is searched for keywords, which could be anything the searchers think might be of interest. All it takes to flag a communication is for one of the parties to use a couple or so of the key words in the ECHELON "dictionary" – "He lives in a lovely old white house on Bush Street, right near me. I can shoot over there in two minutes." Within limitations, computers can "listen" to telephone calls and recognize when keywords are spoken. Those calls are extracted and recorded separately, to be listened to in full by humans. The list of specific targets at any given time is undoubtedly wide ranging, at one point including the likes of Amnesty International and Christian Aid.

ECHELON is carried out without official acknowledgment of its existence, let alone any democratic oversight or public or legislative debate as to whether it serves a decent purpose. The extensiveness of the ECHELON global network is a product of decades of intense Cold War activity. Yet with the end of the Cold War, its budget – far from being greatly reduced – was increased, and the network has grown in both power and reach; yet another piece of evidence that the Cold War was not a battle against something called "the international communist conspiracy".

The European Parliament in the late 1990s began to wake up to this intrusion into the continent's affairs. The parliament's Civil Liberties Committee commissioned a report, which appeared in 1998 and recommended a variety of measures for dealing with the increasing power of the technologies of surveillance. It bluntly advised: "The European Parliament should reject proposals from the United States for making private messages via the global communications network [Internet] accessible to US intelligence agencies." The report denounced Britain's role as a double-agent, spying on its own European partners.

Despite these concerns the US has continued to expand ECHELON surveillance in Europe, partly because of heightened interest in commercial espionage – to uncover industrial information that would provide American corporations with an advantage over foreign rivals.

German security experts discovered several years ago that ECHELON was engaged in heavy commercial spying in Europe. Victims included such German firms as the wind generator manufacturer Enercon. In 1998, Enercon developed what it thought was a secret invention, enabling it to generate electricity from wind power at a far cheaper rate than before. However, when the company tried to market its invention in the United States, it was confronted by its American rival, Kenetech, which announced that it had already patented a near-identical development. Kenetech then brought a court order against Enercon to ban the sale of its equipment in the US. In a rare public disclosure, an NSA employee, who refused to be named, agreed to appear in silhouette on German television to reveal how he had stolen Enercon's secrets by tapping the telephone and computer link lines that ran between Enercon's research laboratory and its production unit some 12 miles away. Detailed plans of the company's invention were then passed on to Kenetech.

In 1994, Thomson S.A., located in Paris, and Airbus Industrie, based in Blagnac Cedex, France, also lost lucrative contracts, snatched away by American rivals aided by information covertly collected by NSA and CIA. The same agencies also eavesdropped on Japanese representatives during negotiations with the United States in 1995 over auto parts trade.

German industry has complained that it is in a particularly vulnerable position because the government forbids its security services from conducting similar industrial espionage. "German politicians still support the rather naive idea that political allies should not spy on each other's businesses. The Americans and the British do not have such illusions," said journalist Udo Ulfkotte, a specialist in European industrial espionage, in 1999.

That same year, Germany demanded that the United States recall three CIA operatives for their activities in Germany involving economic espionage. The news report stated that the Germans "have long been suspicious of the eavesdropping capabilities of the enormous U.S. radar and communications complex at Bad Aibling, near Munich", which is in fact an NSA intercept station. "The Americans tell us it is used solely to monitor communications by potential enemies, but how can we be entirely sure that they are not picking up pieces of information that we think should remain completely secret?" asked a senior German official. Japanese officials most likely have been told a similar story by Washington about the more than a dozen signals intelligence bases which Japan has allowed to be located on its territory.

In their quest to gain access to more and more private information, the NSA, the FBI, and other components of the US national security establishment have been engaged for years in a campaign to require American telecommunications manufacturers and carriers to design their equipment and networks to optimize the authorities' wiretapping ability. Some industry insiders say they believe that some US machines approved for export contain NSA "back doors" (also called "trap doors").

The United States has been trying to persuade European Union countries as well to allow it "back-door" access to encryption programs, claiming that this was to serve the needs of law-enforcement agencies. However, a report released by the European Parliament in May 1999 asserted that Washington's plans for controlling encryption software in Europe had nothing to do with law enforcement and everything to do with US industrial espionage. The NSA has also dispatched FBI agents on break-in missions to snatch code books from foreign facilities in the United States, and CIA officers to recruit foreign communications clerks abroad and buy their code secrets, according to veteran intelligence officials.

For decades, beginning in the 1950s, the Swiss company Crypto AG sold the world's most sophisticated and secure encryption technology. The firm staked its reputation and the security concerns of its clients on its neutrality in the Cold War or any other war. The purchasing nations, some 120 of them – including prime US intelligence targets such as Iran, Iraq, Libya and Yugoslavia – confident that their communications were protected, sent messages from their capitals to their embassies, military missions, trade offices, and espionage dens around the world, via telex, radio, and fax. And all the while, because of a secret agreement between the company and NSA, these governments might as well have been hand delivering the messages to Washington, uncoded. For their Crypto AG machines had been rigged before being sold to them, so that when they used them the random encryption key could be automatically and clandestinely transmitted along with the enciphered message. NSA analysts could read the messages as easily as they could the morning newspaper.

In 1986, because of US public statements concerning the La Belle disco bombing in West Berlin, the Libyans began to suspect that something was rotten with Crypto AG's machines and switched to another Swiss firm, Gretag Data Systems AG. But it appears that NSA had that base covered as well. In 1992, after a series of suspicious circumstances over the previous few years, Iran came to a conclusion similar to Libya's, and arrested a Crypto AG employee who was in Iran on a business trip. He was eventually ransomed, but the incident became well known and the scam began to unravel in earnest.

In September 1999 it was revealed that NSA had arranged with Microsoft to insert special "keys" into Windows software, in all versions from 95-OSR2 onwards. An American computer scientist, Andrew Fernandez of Cryptonym in North Carolina, had disassembled parts of the Windows instruction code and found the smoking gun – Microsoft's developers had failed to remove the debugging symbols used to test this software before they released it. Inside the code were the labels for two keys. One was called "KEY". The other was called "NSAKEY". Fernandez presented his finding at a conference at which some Windows developers were also in attendance. The developers did not deny that the NSA key was built into their software, but they refused to talk about what the key did, or why it had been put there without users' knowledge. Fernandez says that NSA's "back door" in the world's most commonly used operating system makes it "orders of magnitude easier for the US government to access your computer."

In February 2000, it was disclosed that the Strategic Affairs Delegation (DAS), the intelligence arm of the French Defense Ministry, had prepared a report in 1999 which also asserted that NSA had helped to install secret programs in Microsoft software. According to the DAS report, "it would seem that the creation of Microsoft was largely supported, not least financially, by the NSA, and that IBM was made to accept the [Microsoft] MS-DOS operating system by the same administration." The report stated that there had been a "strong suspicion of a lack of security fed by insistent rumors about the existence of spy programs on Microsoft, and by the presence of NSA personnel in Bill Gates' development teams." The Pentagon, said the report, was Microsoft's biggest client in the world.

Recent years have seen disclosures that in the countdown to their invasion of Iraq in 2003, the United States had listened in on UN Secretary-General Kofi Annan, UN weapons inspectors in Iraq, and all the members of the UN Security Council during a period when they were deliberating about what action to take in Iraq.

It's as if the American national security establishment feels that it has an *inalienable right* to

listen in; as if there had been a constitutional amendment, applicable to the entire world, stating that "Congress shall make no law abridging the freedom of the government to intercept the personal communications of anyone." And the Fourth Amendment had been changed to read: "Persons shall be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, except in cases of national security, real or alleged." 2

The leading whistleblower of all time: Philip Agee

Before there was Edward Snowden, William Binney and Thomas Drake … before there was Bradley Manning, Sibel Edmonds and Jesselyn Radack … there was Philip Agee. What Agee revealed is still the most startling and important information about US foreign policy that any American government whistleblower has ever revealed.

Philip Agee spent 12 years (1957-69) as a CIA case officer, most of it in Latin America. His first book, *Inside the Company: CIA Diary*, published in 1974 – a pioneering work on the Agency's methods and their devastating consequences – appeared in about 30 languages around the world and was a best seller in many countries; it included a 23-page appendix with the names of hundreds of undercover Agency operatives and organizations.

Under CIA manipulation, direction and, usually, their payroll, were past and present presidents of Mexico, Colombia, Uruguay, and Costa Rica, "our minister of labor", "our vice-president", "my police", journalists, labor leaders, student leaders, diplomats, and many others. If the Agency wished to disseminate anti-communist propaganda, cause dissension in leftist ranks, or have Communist embassy personnel expelled, it need only prepare some phoney documents, present them to the appropriate government ministers and journalists, and – presto! – instant scandal.

Agee's goal in naming all these individuals, quite simply, was to make it as difficult as he could for the CIA to continue doing its dirty work.

A common Agency tactic was writing editorials and phoney news stories to be knowingly published by Latin American media with no indication of the CIA authorship or CIA payment to the media. The propaganda value of such a "news" item might be multiplied by being picked up by other CIA stations in Latin America who would disseminate it through a CIA-owned news agency or a CIA-owned radio station. Some of these stories made their way back to the United States to be read or heard by unknowing North Americans.

Wooing the working class came in for special treatment. Labor organizations by the dozen, sometimes hardly more than names on stationery, were created, altered, combined, liquidated, and new ones created again, in an almost frenzied attempt to find the right combination to compete with existing left-oriented unions and take national leadership away from them.

In 1975 these revelations were new and shocking; for many readers it was the first hint that American foreign policy was not quite what their high-school textbooks had told them nor what the *New York Times* had reported.

"As complete an account of spy work as is likely to be published anywhere, an authentic account of how an ordinary American or British 'case officer' operates … All of it … presented with deadly accuracy," wrote Miles Copeland, a former CIA station chief, and

ardent foe of Agee. (There's no former CIA officer more hated by members of the intelligence establishment than Agee; no one's even close; due in part to his traveling to Cuba and having long-term contact with Cuban intelligence.)

In contrast to Agee, WikiLeaks withheld the names of hundreds of informants from the nearly 400,000 Iraq war documents it released.

In 1969, Agee resigned from the CIA (and colleagues who "long ago ceased to believe in what they are doing").

While on the run from the CIA as he was writing *Inside the Company* – at times literally running for his life – Agee was expelled from, or refused admittance to, Italy, Britain, France, West Germany, the Netherlands, and Norway. (West Germany eventually gave him asylum because his wife was a leading ballerina in the country.) Agee's account of his period on the run can be found detailed in his book *On the Run* (1987). It's an exciting read.

Notes

1. To read about my State Department and other adventures, see my book *West-Bloc Dissident: A Cold war Memoir (2002)* ↩
2. See *Rogue State: A Guide to the World's Only Superpower*, chapter 21, for the notes for the above. ↩
