OMNI SNOWDEN NEWSLETTER #1, July 9, 2013.
Compiled by Dick Bennett for a Culture of Peace and Justice.

My blog:
War Department/Peace Department
http://jamesrichardbennett.blogspot.com/

Newsletters
http://www.omnicenter.org/newsletter-archive/
See newsletters on National Security State (NSS), Pentagon, Secrecy, Surveillance, and many more.

Index:
http://www.omnicenter.org/omni-newsletter-general-index/

Contents #1 (in reverse chron. order, bold type added by Dick)

Petitions
July 13: Ellsberg, Why Snowden Had to Flee US
July 8/15: Schell, Hero Snowden vs. End of Privacy
July 5: Weisbrot, Helping Snowden
July 5: Pilger, Morales’ Plane Forced Down
June 26: Blum, Dark History of US NSS, vs. Phillip Agee
June 24: Lindorff, Hong Kong, China, Russia vs Hacker USA
June 19: Greenwald, FISA Fails Oversight
June 13: Greenwald, Snowden, Who Is He?

SIGN PETITIONS

lease sign the below petitions: Stop Watching US & call your reps. https://call.stopwatching.us/

EPIC: EPIC Joins Coalition to Demand a Congressional Investigation into NSA Surveillance

GAP Statement on Edward Snowden & NSA Domestic Surveillance
Secret FISA Court Out of Control – Makes Violently Anti-Constitutional Decision Giving up ALL Your Phone Records [Link]

EPIC Joins Coalition to Demand a Congressional Investigation into NSA Surveillance

Today, EPIC joined a coalition of over 100 civil liberties organizations and Internet companies to demand that Congress initiate a full-scale investigation into the National Security Agency's surveillance programs. In the letter sent to Congress this morning, the coalition emphasized the need for public transparency and an end to dragnet surveillance: "This type of blanket data collection by the government strikes at bedrock American values of freedom and privacy." EPIC is also leading a petition to the NSA to suspend its program of collecting information on all individuals in the United States. EPIC intends to renew its request to the Agency every week until the NSA responds. For more information see EPIC: NSA Petition.

https://call.stopwatching.us/

EPIC, Bamford, Diffie, Schneier Call for Suspension of NSA Domestic Surveillance Program Pending Public Comment

EPIC, joined by leading privacy experts including James Bamford, Whitfield Diffie, and Bruce Schneier, has petitioned the National Security Agency to suspend its domestic surveillance program pending public comment. EPIC's petition states "NSA's collection of domestic communications contravenes the First and Fourth Amendments to the United States Constitution, and violates several federal privacy laws, including the Privacy Act of 1974, and the Foreign Intelligence Surveillance Act of 1978 as amended." EPIC's petition further states that NSA's domestic surveillance "substantively affects the public to a degree sufficient to implicate the policy interests" that require public comment, and that "NSA's collection of domestic communications absent the opportunity for public comment is unlawful." EPIC intends to renew its request each week until the NSA responds. For more information and to join EPIC’s petition, see: EPIC: NSA Petition.

EPIC Calls on FCC to Investigate Unlawful Disclosure of Consumer Phone Records

In a letter to Federal Communications Commission Chairwoman Mignon Clyburn, EPIC urged the FCC to determine whether Verizon violated the Communications Act when it released consumer call detail information to the National Security Agency. In response to an unprecedented Foreign Intelligence Surveillance Court order which focused on solely domestic communications, Verizon released telephone customer information to the NSA, including telephone numbers and time and call duration. Congress explicitly charged the Commission with investigating unauthorized disclosures of consumer call detail information. EPIC’s letter stated that Verizon violated legal protections for consumer phone records when it disclosed consumer information in response to a facially invalid order. For more information, see EPIC: Foreign Intelligence Surveillance Act, EPIC: Clapper v. Amnesty Int'l, and EPIC: USA Patriot Act.
Snowden Was Correct to Flee the US

By Daniel Ellsberg, The Washington Post
08 July 13

Daniel Ellsberg is the author of “Secrets: A Memoir of Vietnam and the Pentagon Papers.” He was charged in 1971 under the Espionage Act as well as for theft and conspiracy for copying the Pentagon Papers. The trial was dismissed in 1973 after evidence of government misconduct, including illegal wiretapping, was introduced in court.

[Ellsberg, 1970s, leaking, US civil liberties, functioning Bill of Rights, and free press. –Dick]

Any people compare Edward Snowden to me unfavorably for leaving the country and seeking asylum, rather than facing trial as I did. I don't agree. The country I stayed in was a different America, a long time ago.

After the New York Times had been enjoined from publishing the Pentagon Papers - on June 15, 1971, the first prior restraint on a newspaper in U.S. history - and I had given another copy to The Post (which would also be enjoined), I went underground with my wife, Patricia, for 13 days. My purpose (quite like Snowden's in flying to Hong Kong) was to elude surveillance while I was arranging - with the crucial help of a number of others, still unknown to the FBI - to distribute the Pentagon Papers sequentially to 17 other newspapers, in the face of two more injunctions. The last three days of that period was in defiance of an arrest order: I was, like Snowden now, a "fugitive from justice."

Yet when I surrendered to arrest in Boston, having given out my last copies of the papers the night before, I was released on personal recognizance bond the same day. Later, when my charges were increased from the original three counts to 12, carrying a possible 115-year sentence, my bond was increased to $50,000. But for the whole two years I was under indictment, I was free to speak to the media and at rallies and public lectures. I was, after all, part of a movement against an ongoing war. Helping to end that war was my preeminent concern. I couldn't have done that abroad, and leaving the country never entered my mind.
[Snowden, 2013, leaking, US intensified repression, damaged Bill of Rights, secrecy, punishment, totalitarianism. –Dick]

There is no chance that experience could be reproduced today, let alone that a trial could be terminated by the revelation of White House actions against a defendant that were clearly criminal in Richard Nixon’s era - and figured in his resignation in the face of impeachment - but are today all regarded as legal (including an attempt to "incapacitate me totally").

I hope Snowden’s revelations will spark a movement to rescue our democracy, but he could not be part of that movement had he stayed here. There is zero chance that he would be allowed out on bail if he returned now and close to no chance that, had he not left the country, he would have been granted bail. Instead, he would be in a prison cell like Bradley Manning, incommunicado.

He would almost certainly be confined in total isolation, even longer than the more than eight months Manning suffered during his three years of imprisonment before his trial began recently. The United Nations Special Rapporteur for Torture described Manning's conditions as "cruel, inhuman and degrading." (That realistic prospect, by itself, is grounds for most countries granting Snowden asylum, if they could withstand bullying and bribery from the United States.)

Snowden believes that he has done nothing wrong. I agree wholeheartedly. More than 40 years after my unauthorized disclosure of the Pentagon Papers, such leaks remain the lifeblood of a free press and our republic. One lesson of the Pentagon Papers and Snowden's leaks is simple: secrecy corrupts, just as power corrupts.

In my case, my authorized access in the Pentagon and the Rand Corp. to top-secret documents - which became known as the Pentagon Papers after I disclosed them - taught me that Congress and the American people had been lied to by successive presidents and dragged into a hopelessly stalemated war that was illegitimate from the start.

Snowden's dismay came through access to even more highly classified documents - some of which he has now selected to make public - originating in the National Security Agency (NSA). He found that he was working for a surveillance organization whose all-consuming intent, he told the Guardian's Glenn Greenwald, was "on making every conversation and every form of behavior in the world known to them."

It was, in effect, a global expansion of the Stasi, the Ministry for State Security in the Stalinist "German Democratic Republic," whose goal was "to know everything." But the cellphones, fiber-optic cables, personal computers and Internet traffic the NSA accesses did not exist in the Stasi's heyday.

As Snowden told the Guardian, "This country is worth dying for." And, if necessary, going to prison for - for life.

But Snowden's contribution to the noble cause of restoring the First, Fourth and Fifth amendments to the Constitution is in his documents. It depends in no way on his reputation or estimates of his character or motives - still less, on his presence in a courtroom arguing the current charges, or his living the rest of his life in prison. Nothing worthwhile would be served, in my opinion, by Snowden voluntarily surrendering to U.S. authorities given the current state of the law.

I hope that he finds a haven, as safe as possible from kidnapping or assassination by U.S. Special Operations forces, preferably where he can speak freely.
What he has given us is our best chance - if we respond to his information and his challenge - to rescue ourselves from out-of-control surveillance that shifts all practical power to the executive branch and its intelligence agencies: a United Stasi of America.

[End Ellsberg]

America's Surveillance Net - TheNation

Jonathan Schell - TheNation

America's Surveillance Net
There is a revolution afoot—one that is being carried out by the government against the fundamental law of the land. [A brief, excellent essay tracing the rise of repression in the US and the great service to democracy by Snowden. –Dick]
http://www.thenation.com/article/174889/americas-surveillance-net#axzz2XBLcJHyq
A school of fish swims peacefully in the ocean. Out of sight, a net is spread beneath it. At the edges of the net is a circle of fishing boats. Suddenly, the fishermen yank up the edges of the net, and in an instant the calm, open ocean becomes a boiling caldron, an exitless, rapidly shrinking prison in which the fish thrash in vain for freedom and life.

Increasingly, the American people are like this school of fish in the moments before the net is pulled up. The net in question is of course the Internet and associated instruments of data collection, and the fishermen are corporations and the government. That is, to use the more common metaphor, we have come to live alongside the machinery of a turnkey tyranny. As we now know, thanks to the courageous whistleblower Edward Snowden, the National Security Agency has been secretly ordering Verizon to sweep up and hand over all the metadata from the phone calls of millions of its customers: phone numbers, duration of calls, routing information and sometimes the location of the callers. Thanks to Snowden, we also know that unknown volumes of like information are being extracted from Internet and computer companies, including Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube and Apple.

The first thing to note about these data is that a mere generation ago, they did not exist. They are a new power in our midst, flowing from new technology, waiting to be picked up; and power, as always, creates temptation, especially for the already powerful. Our cellphones track our whereabouts. Our communications pass through centralized servers and are saved and kept for a potential eternity in storage banks, from which they can be recovered and examined. Our purchases and contacts and illnesses and entertainments are tracked and agglomerated. If we are arrested, even our DNA can be taken and stored by the state. Today, alongside each one of us, there exists a second, electronic self, created in part by us, in part by others. This other self has become de facto public property, owned chiefly by immense data-crunching corporations, which use it for commercial purposes. Now government is reaching its hand into those corporations for its own purposes, creating a brand-new domain of the state-corporate complex.

Surveillance of people on this scale turns basic liberties—above all the Fourth Amendment, which protects citizens against unreasonable search and seizure—into a dead letter. Government officials, it is true, assure us that they will never pull the edges of the net tight. They tell us that although they could know everything about us, they won’t decide to. They’ll let the information sit unexamined in the electronic vaults. But history, whether of our country or others, teaches that only a fool would place faith in such assurances. What one president refrains from doing the next will do; what is left undone in peacetime is done when a crisis comes.

The executive branch offers a similar assurance about its claimed right to kill American and foreign citizens at its sole discretion. But to accept such assurances as the guarantee of basic liberties would be to throw away bedrock principles of our constitutional order. If there is any single political idea that deserves to be called quintessentially American, it is the principle that government power must be balanced and checked by other government power, which is why federal power is balanced by state power and is itself divided into three branches.

The officials—most notably President Obama—have assured us that this system is intact, that the surveillance programs are “under very strict supervision by all three branches of government,” in Obama’s words. But the briefest examination of the record rebuts the claim.
In this matter, the interactions of the three branches are a cause not for reassurance but for deeper alarm. It’s not that the legislative and judicial branches are not involved; it’s that each, in its own way, has abandoned its appointed constitutional role.

The story arguably begins with George W. Bush’s end run around the legal system after the terrorist attacks of 2001, when, in complete disregard of the law, he initiated warrantless domestic surveillance by the NSA. So clearly illegal and extreme was this program that high-ranking officials of his administration, including James Comey, deputy attorney general, and Robert Mueller, director of the FBI, threatened to resign. Bush backed off some of the measures, and the confrontation did not become known until much later.

What happened then? Did Congress check this executive usurpation? Did it castigate Bush, forbid the crimes, hold his officials accountable? It did not. It adopted the worst features of the Bush program as law, in the Protect America Act of 2007 and the Foreign Intelligence Surveillance Amendments Act of 2008; it also immunized from legal repercussions corporations that had secretly knuckled under to Bush’s wrongdoing. Far from correcting the abuses, Congress institutionalized them. At the same time, it supported the executive branch’s cloak of secrecy over those abuses and the classification of the legal opinions of the FISA court, whose rulings have given legal protection to the new surveillance programs. The Obama administration’s legal opinions on the practices are also classified.

As for the judicial branch, it happens that in 1979, the Supreme Court ruled that the sort of metadata collected from Verizon is not covered by the Fourth Amendment. (In fairness, there is no sign that the Court anticipated or meant to approve the sort of indiscriminate dragnet of metadata now under way. Thus, a lawsuit recently brought by the ACLU to stop this has a chance of succeeding.) The FISA court almost never refuses government requests. James Bamford, an expert on NSA surveillance, has characterized this institution as “a super hush-hush surveillance court that is virtually impotent.”

Our system of checks and balances has gone into reverse. The three branches, far from checking one another’s power or protecting the rights of Americans, entered one after another into collusion to violate them, even to the extent of immunizing the wrongdoers. Balanced, checked power has become fused power—exactly what the founders of this country feared above all else. The political parties have been no more useful as checks than the branches of government; their leaderships stand together protecting the abuses, though individual senators, including Jeff Merkley and Ron Wyden, have proposed sensible reforms.

Finally, even elections have proven ineffective: the voters chose a president who taught constitutional law running on a platform of stopping civil liberties abuses; but he has become the author of new abuses. Even now, his soothing demeanor and reputation for liberalism (“Change we can believe in”) confuses and thwarts those who otherwise would be reacting with anger.
What should Americans do when all official channels are unresponsive or dysfunctional? Are we, as people used to say, in a revolutionary situation? Shall we man the barricades? The situation is a little more peculiar than that. There is a revolution afoot, but it is not one in the streets; it is one that is being carried out by the government against the fundamental law of the land. That this insurrection against the constitutional order by officials sworn to uphold it includes legal opinions and legislation only makes it the more radical and dangerous. In other words, the government is in stealthy insurrection against the letter and the spirit of the law.

What’s needed is counterrevolution—an American restoration, returning to and reaffirming the principles on which the Republic was founded. Edward Snowden, for one, knew what to do. He saw that when government as a whole goes rogue, the only force with a chance of bringing it back into line is the public. He has helped make this possible by letting the public know the abuses that are being carried out in its name. Civil disobedients are of two kinds: those inspired by universal principles, and those inspired by national traditions. Each has its strengths. Julian Assange of WikiLeaks is the first kind; Snowden, the second. Asked why he had done what he did, Snowden replied, “I am neither traitor nor hero. I am an American.” He based his actions on the finest traditions of this country, which its current leaders have abandoned but which, he hopes, the current generation of Americans still share. In the weeks and months ahead, we’ll find out whether he was right. Jonathan Schell

More coverage of the NSA spying scandal from this week’s Nation can be viewed here and here.

Jonathan Schell

The "Edward Snowden Aviation Club" and Other Ways to Beat US Persecution

Friday, 05 July 2013 09:41 By Mark Weisbrot, The Guardian | Op-Ed
(From David D)

Some countries have offered asylum but the NSA whistleblower will need transport. How about concerned citizens raising money for a private plane?

[Individuals sign petitions and raise money.]

Country gives asylum and other countries support it. –Dick]

With Edward Snowden stuck in limbo in the Moscow airport transit space, many people in the United States and around the world are wondering what can be done to help him. More than 123,000 Americans have signed a petition on the White House website saying that "Edward Snowden is a national hero and should be immediately issued a full, free, and absolute pardon". Other petitions of support have gathered as many as 1.3 million signatures.

Actually there is quite a bit that can be done by various people to help Snowden reach a safe place where he can be free from persecution by the US government.

The governments of Ecuador, Russia, and Venezuela have invited Snowden to apply for asylum, and there is little doubt that it would be granted. The legal basis for political asylum is very strong, especially since the US has charged Snowden under the Espionage Act. Since it is pretty clear that there was no espionage involved here – no evidence that he collaborated or even met with any foreign governments – this is one obvious indicator that Snowden has a well-founded fear of persecution. And politically, despite efforts by much of the media to brand Snowden a criminal and a traitor, most of the world appears to sympathise with him. Any government that helps him would almost certainly have popular support at home.
The problem is that these governments are reluctant to take the necessary steps to get Snowden freedom because of possible US retaliation. Of course, retaliation is not as likely as many people think: Washington was angry with Hong Kong for about a day after it rejected a request for extradition, and then it blew over. John Kerry's warnings of "consequences" for Russia and China were reversed on Thursday by President Obama, who sought to lower the profile of the issue. Another recent example of threatened retaliation that did not materialise was the US threats to Palestinians for seeking UN recognition of their state.

And there are things that other governments could do to help this process along. First and easiest, the governments of South America – perhaps through UNASUR or another regional body – can denounce Washington's threats to cut off Ecuador's trade preferences in retaliation for offering to receive Snowden's application for political asylum. They took similar steps in response to the UK's threats to invade Ecuador's embassy in London to capture Julian Assange, and these moves were politically successful.

Second, more governments can make statements in support of what Snowden did, as politely as they prefer, and offer to receive an application for political asylum – something that they are required to do under international law in any case. The more governments that make such statements, the more difficult it is for Washington to isolate or retaliate against any one of them.

Third, although Ecuador was reluctant to offer travel documents for Snowden, other governments can. Again, the more governments that state their willingness to do so, the less likely retaliation from Washington becomes.

Then there is the question of how he gets to a safe country. Here, any friendly government could offer him a private plane – it is a minimal expense for a government. Prominent citizens from the US and other countries could offer to accompany Snowden, to reduce the chances of risky behaviour by the US military (although Obama has said that he "was not going to scramble any jets" to get Snowden). The Russian government could also make sure that the Aeroflot flight to Cuba, if it carries Snowden, is re-routed so that it does not fly too close to the US.

The Russian government, if it is unwilling to offer Snowden a visa for its own country, could provide transportation to the Ecuadorian or another government embassy in Moscow, where Snowden could apply for asylum and then resolve the travel document issue. From there, the Russians would be legally obligated to offer Snowden safe passage to the country that had offered him asylum. (The British government's confinement of Julian Assange in the Ecuadorian embassy in London for the past year, after he has received asylum from Ecuador, is illegal under international law.)

Finally, there is the "second superpower", as global civil society was named in 2003 when tens of millions of people hit the streets worldwide against the planned US-led invasion of Iraq. In addition to pressuring their governments to take one or more of the various steps outlined above, citizens can act on their own. For example, they could form a "Snowden Aviation Club", to raise money for a private plane to take him to a safe place. Or even a helicopter to transport him to the Ecuadorian embassy in Moscow. The funds for either of these options should be easy to raise, given his popular support.

Edward Snowden has performed a heroic service to the people of the US and the world, by exposing widespread government abuses that are a threat to freedom everywhere. It's up to everyone who understands this to make sure he is not persecuted for doing so.
Edward Snowden

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* (2002). 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 twelve miles away. Detailed plans of the company's invention were then passed on to Kenetech.

In 1994, Thomson SA, 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 US 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 twelve years (1957 to 1969) 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 thirty 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
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.

Any part of this report may be disseminated without permission, provided attribution to William Blum as author and a link to this website are given.

Books by William Blum

*America's Deadliest Export: Democracy: The Truth About US Foreign Policy and Everything Else*

*Killing Hope: US Military and CIA Interventions Since World War Two*

*Rogue State: A Guide to the World's Only Superpower*

*Freeing the World to Death: Essays on the American Empire*

Read more at [http://williamblum.org/about/](http://williamblum.org/about/)

To rescue an old man from the clutches of the capitalist imperialist meanies: [http://williamblum.org/about/](http://williamblum.org/about/)

Send comments, typos found, money, love notes, hate mail, death threats, letter bombs, and anthrax to [bblum6@aol.com](mailto:bblum6@aol.com)

[www.killinghope.org/bblum6/aer118.html](http://www.killinghope.org/bblum6/aer118.html)

[https://billtotten.wordpress.com/](https://billtotten.wordpress.com/)

[http://www.ashisuto.co.jp](http://www.ashisuto.co.jp)

[End Blum]

---

**China, Hong Kong and Russia Foil US Attempt to Silence NSA Whistleblower**

**Dave Lindorff, Op-Ed, NationofChange, June 24, 2013:** Edward Snowden’s revelations also exposed the U.S. as a hypocrite in accusing China of criminally hacking
into U.S. corporate and government computers. It turns out that the **U.S. itself is the biggest official hacker**, with a massive campaign run out of the NSA, of hacking into Chinese, Hong Kong, Iranian and other countries' computer systems and of actually engaging in a kind of undeclared computer warfare against rival states by which this country is not, officially, at war.

---

**Public Split on NSA Leak Impact, Most Say Prosecute Snowden**, Pew Research Center

The public is divided over whether the leak of classified information about NSA phone and internet surveillance serves the public interest. But a majority says that former government contractor Edward Snowden should be criminally prosecuted. Young people are more likely than other age groups to think that the NSA leak serves the public interest.

**READ THE REPORT**

---

**Glenn Greenwald | Documents Reveal Lack of FISA Court Oversight**

Glenn Greenwald, Guardian UK

Greenwald writes: "Top secret documents obtained by the Guardian illustrate what the Fisa
court actually does - and does not do - when purporting to engage in 'oversight' over the
NSA's domestic spying."

Reader Supported News | 09 June 13

BREAKER | Edward Snowden: The Whistleblower Behind Revelations of NSA Surveillance

Glenn Greenwald, Ewen MacAskill, Laura Poitras, Guardian UK
Excerpt: "The individual responsible for one of the most significant leaks in US political history is Edward Snowden, a 29-year-old former technical assistant for the CIA."

John Pilger writes here: Germany's Der Spiegel has described the Obama administration as "soft totalitarianism".

President Morales arrives back in La Paz, Bolivia. (photo: Zuma/Rex Features)
Forcing Down Evo Morales's Plane Was an Act of Air Piracy  By John Pilger, Guardian UK  05 July 2013  (from David D)

Imagine the aircraft of the president of France being forced down in Latin America on "suspicion" that it was carrying a political refugee to safety - and not just any refugee but someone who has provided the people of the world with proof of criminal activity on an epic scale.

Imagine the response from Paris, let alone the "international community", as the governments of the west call themselves. To a chorus of baying indignation from Whitehall to Washington, Brussels to Madrid, heroic special forces would be dispatched to rescue their leader and, as sport, smash up the source of such flagrant international gangsterism. Editorials would cheer them on, perhaps reminding readers that this kind of piracy was exhibited by the German Reich in the 1930s.

The forcing down of Bolivian President Evo Morales's plane - denied airspace by France, Spain and Portugal, followed by his 14-hour confinement while Austrian officials demanded to "inspect" his aircraft for the "fugitive" Edward Snowden - was an act of air piracy and state terrorism. It was a metaphor for the gangsterism that now rules the world and the cowardice and hypocrisy of bystanders who dare not speak its name.

In Moscow, Morales had been asked about Snowden - who remains trapped in the city's airport. "If there were a request [for political asylum]," he said, "of course, we would be willing to debate and consider the idea." That was clearly enough provocation for the Godfather. "We have been in touch with a range of countries that had a chance of having Snowden land or travel through their country," said a US state department official.

The French - having squealed about Washington spying on their every move, as revealed by Snowden - were first off the mark, followed by the Portuguese. The Spanish then did their bit by enforcing a flight ban of their airspace, giving the Godfather's Viennese hirelings enough time to find out if Snowden was indeed invoking article 14 of the Universal Declaration of Human Rights, which states: "Everyone has the right to seek and to enjoy in other countries asylum from persecution."

Those paid to keep the record straight have played their part with a cat-and-mouse media game that reinforces the Godfather's lie that this heroic young man is running from a system of justice, rather than preordained, vindictive incarceration that amounts to torture - ask Bradley Manning and the living ghosts in Guantánamo.

Historians seem to agree that the rise of fascism in Europe might have been averted had the liberal or left political class understood the true nature of its enemy. The parallels today are very different, but the Damocles sword over Snowden, like the casual abduction of Bolivia's president, ought to stir us into recognising the true nature of the enemy.

Snowden's revelations are not merely about privacy, or civil liberty, or even mass spying. They are about the unmentionable: that the democratic facades of the US now barely conceal a systematic gangsterism historically identified with, if not necessarily the same as, fascism. On Tuesday, a US drone killed 16 people in North Waziristan, "where many of the world's most dangerous militants live", said the few paragraphs I read. That by far the world's most
dangerous militants had hurled the drones was not a consideration. President Obama personally sends them every Tuesday.

**In his acceptance of the 2005 Nobel prize in literature, Harold Pinter referred to "a vast tapestry of lies, upon which we feed". He asked why "the systematic brutality, the widespread atrocities" of the Soviet Union were well known in the west while America's crimes were "superficially recorded, let alone documented, let alone acknowledged". The most enduring silence of the modern era covered the extinction and dispossession of countless human beings by a rampant US and its agents. "But you wouldn't know it," said Pinter. "It never happened. Even while it was happening it never happened."

This hidden history - not really hidden, of course, but excluded from the consciousness of societies drilled in American myths and priorities - has never been more vulnerable to exposure. **Snowden’s whistleblowing, like that of Manning and Julian Assange and WikiLeaks, threatens to break the silence Pinter described. In revealing a vast Orwellian police state apparatus servicing history's greatest war-making machine, they illuminate the true extremism of the 21st century.** Unprecedented, Germany's Der Spiegel has described the Obama administration as "soft totalitarianism". If the penny is falling, we might all look closer to home.

END SNOWDEN NEWSLETTER #1 JULY 9, 2013

--
Dick Bennett
My blog:
War Department/Peace Department
[http://jamesrichardbennett.blogspot.com/](http://jamesrichardbennett.blogspot.com/)
Newsletters

Index:
[http://www.omnicenter.org/omni-newsletter-general-index/](http://www.omnicenter.org/omni-newsletter-general-index/)
National/International Days
See Newsletters
Peace, Justice, Ecology Birthdays
See INMOtion
[jbennet@uark.edu](mailto:jbennet@uark.edu)
(479) 442-4600
2582 Jimmie Ave.
Fayetteville, AR 72703