S. Eugene Poteat
President

Too Big To Keep Secrets?

Not Too Big to Fail If We Don't!

This issue covers leakers of all stripes, not just youngsters like Pvt. Bradley Manning, and that runaway, conniving contractor, Edward Snowden, who just revealed he was already stealing secrets in 2009 with his first cleared job at Dell. But also those mature, seasoned intelligence officers who, mid-or-late career, bypassed all channels for airing grievances and cozied up, instead, with newspaper reporters, or hid leaks with co-authors to increase the value of a forthcoming book, or leaked to friends in Congress to halt programs they found unappealing, or spilled reams of data on various anti-American websites just because they could. Some of these include Thomas Drake of NSA, Stephen Jin-Woo Kim of the State Department, and Mary McCarthy, John Kiriakou, Jeffrey Sterling, all of CIA. And, sadly, most of these – until the conviction of Kiriakou – did so with impunity, even after being caught. Too often the policy was one of "hands-off" when it was realized the leaker was the friendly officer in the next office or down the hall.

With thieving intelligence neophytes like Manning and Snowden, the spillage of secrets underscores the risks of handing too much access, too quickly, to those who have high tech skills but no understanding of the world in which they live: its history, heritage, dangers, threats and the positive – and negative – role computers can play in our national security and safety. They were devoid of social competence, maturity, wisdom, and any study of history. Too often these young military officers or computer geeks are encouraged by the media to see themselves as heroes, and they lap up the attention, even if it includes stealing classified secrets to keep the praise coming. Journalists and WikiLeaks recruiters – like foreign intelligence spotters – know how to work those ego levers to keep the secrets flowing.

Manning and Snowden are not dissimilar from that list of older IC leakers and malcontents: arrogant and unstable, simmering with grudges and grievances, exactly the sort with security clearances foreign intelligence agencies hunger to recruit. For that reason, these folks should never have been given clearances if our personality assessment tests were accurate. These incidents strongly call into question the IC vetting process.

Unfortunately, those Government elders charged with managing the high tech side of the IC, have the requisite maturity, education, and real world experience, but limited computer knowledge, and end up hiring the Snowdens without realizing that smug, cocksure hires like this can compromise – in seconds – sophisticated billion-dollar classified programs; programs that took decades of planning, review, approvals, and cautious implementation. Billions of dollars wiped out when an ignorant rube with a $5 USB thumb-drive hands it to reporters, WikiLeaks, or other spies. For this alone, those bosses and recruiters share the blame for Snowden's traitorous activity and quick defection to China, then Russia, where fleeing traitors usually turn up.

What is it that NSA does that has people, including some in Congress, riled-up, clamoring to rein in PRISM? Of course we first see the obligatory public show of alarm by those who knew of the program for years. But what NSA does not do is listen to our phone conversations—nor examine all that mindless Internet chatter on emails, Skype, Facebook, LinkedIn, Twitter, blogs, and webpages. Nothing more useless. But NSA does search for terrorists by collecting telephone dialing information; numbers, dates, time, and duration of calls, between people in the US. and people already under investigation or suspicion as possible terrorists, here and abroad. For our safety. And does similar collation with emails, voice, data, and website visits. This monitoring helps determine where the plotters and adversaries might be located, what they are planning, when they might seek to advance from internet boasts and posturing and move towards action: with whom, where, and with what kinds of weapons. Far beyond human capability, NSA sorts through "Big Data" – yottabytes of metadata. If the computers find a pattern indicative of terrorist chatter, or a call between someone in Pakistan planning an attack on the US or an ally, the NSA and FBI zero-in to further assess the conversation—all legal and warranted by the Foreign Intelligence Surveillance Court (FISA). At least 14 federal judges have approved NSA's acquisition of metadata every 90 days since 2006 under the provision of FISA. The court's order imposes strict limitations to insure the data are used only for counterterrorism analysis and not for political opposition research, or idyll snooping on entertainment figures, spouses, sports figures, et al. And for good reason.

Everyone has something to hide. Perhaps it is a child struggling with drugs, a predilection for online pornography, adulterous affairs, financial shenanigans, payoffs, gambling, pedophilia, undisclosed medical conditions, bankruptcies, personal or financial misrepresentations, acts of revenge, fraud, secrets being sent to journalist chums, insider trading...the list goes on. But should we sacrifice the safety of a nation to protect these aspects of being human? Certainly not. The outcry of fear at the revelation of NSA's PRISM program, claiming it's a violation of personal freedom, makes me suspect these concerns have little to do with Fourth Amendment rights and all to do with fear of exposure of one or more of the items listed above.

Our Congress has oversight of the intelligence community and its activities, and despite their *own* fears and foibles and exposed secrets of corruption, hidden campaign donors, sexting and other peccadilloes, it has continued to approve the NSA program. Why? Because it recognizes—as should we all—the national security implications of not doing so—of facing terrorists blindfolded; hence, a meta-

data analysis program in an age of WMD terrorism trumps all of our personal embarrassments and concerns.

The Historical Underpinnings of National Surveillance

Monitoring communications is as old as communications itself and has always brought out libertarians who believe their privacy is more important than our nation's security. We all are routinely monitored; not by the Government, but by our credit card companies, banks, retail stores, search engines, and our Internet providers. What they learn about us is sold and traded to others every second we're online, to target us with ads, promotions, or even to limit our insurance policies, friends, or job prospects. Conduct a Google search and up pops advertisements suggesting products based on prior searches. And it is built on data far more intrusive and permanent than that collected by NSA to counter terrorists.

Those tracking cookies, in the thousands, secretly installed on your computer by browsers, are paid for because they underwrite all those free search engines and websites most of us frequent. And all swear they will keep our personal information secure.

Surveillance by the US government, in far less detail, is more important and is done because such data means life-or-death in war, getting it to those needing it in a timely manner. Samuel Morse's electric telegraph, and later Marconi's wireless, solved the problem by giving birth not only to rapid, long-distance communications, but also spawned intercept techniques, coding and codebreaking, crucial in war. And just as quickly, the telegraph was targeted by adversaries who tapped into the lines, injecting false messages. One soldier even discovered that by placing his tongue on a telegraph line he could read the Morse code transmissions. President Lincoln, with his keen interest in new technologies, used the telegraph extensively to communicate with his generals. Lincoln gave his Secretary of War, Edwin Stanton, sweeping powers, including control and monitoring of all telegraph lines, control of the press through censorship, establishment of a secret police, and extrajudicial arrests of reporters [having early on recognized them as equivalent to spies].

Lincoln's sweeping wartime powers over telegraph communications went unquestioned. There were no outcries, no one complained, for the nation was at war, and everyone understood surveillance was crucial and that these emergency wartime measures were not permanent. As the war ended, so did the surveillance and monitoring. And so will it end when our war against terrorism comes to its close.

After the Great War – "the war to end all wars" – America's mood was peace and disarmament, and our politicians were convinced future wars could be avoided by good faith arms limitations negotiations. When it was discovered that the US State Department, with the British, had intercepted and decoded the Japanese communications to determine their negotiating position, Secretary of State Henry L. Stimson made his now infamous statement, "Gentlemen don't read each other's mail," and closed down the State Department's intercept and codebreaking operation. Congress went further, passing the Communications Act of 1934, making it illegal to intercept and decode communications of anyone, including an enemy, placing our nation's future security in jeopardy.

Fortunately, our Army and Navy codebreakers were realists. They continued to master the art of intercepts and codebreaking—in time to save our nation in WWII by breaking the Japanese codes that led to victory over a superior Japanese fleet in the Battle of Midway, turning the tide of war against the enemy. Because of this surveillance – of a cryptologic nature – a handful of American ships devastated the Japanese fleet and changed the balance of power in the Pacific, permanently. WWII easily could have been lost had we not intercepted and broken German and Japanese codes. The Cold War never became hot because intelligence collecting by *both* sides led to Mutual Assured Destruction (MAD), keeping the lid on a simmering nuclear cauldron.

Monitoring of Enemy Communications is a Necessity

9/11 may have seemed a mere TV special, forgotten by some; and other than a few pressure-cooker bombings, many Americans think the war on terror was a blip, is now over, or was never a real war. Worse, 70% of Americans have been deliberately misinformed by the press into believing the Government is using its surveillance operations for purposes other than fighting terrorism. The world is awash with telecommunications: everyone is online, including those planning wars and terrorist attacks. While Congress recently dodged losing a vote to defund NSA's collection of phone records by a margin of 205 to 217, it was the closest since 9/11. Nothing would make terrorists and secret leakers happier than seeing such a program defunded. Fortunately, in his recent press conference, the President made it emphatically clear that NSA would continue its surveillance, and added that he would look into what could be done to keep the public better informed.

Snowden stole information not to expose PRISM to American voters [why then flee to China and Russia?] to strengthen our democracy or to right a wrong, but with the aim of grandstanding, attention-seeking, and to weaken critical intelligence capabilities. All he did is expose a crucial program also used in the UK, France, Germany, Russia, China, and much of the rest of the world; albeit denied by all, as they should, for it is a valuable, *covert* tool essential for protection of these countries and their allies. Snowden's stolen files have now made it easier for China and Russia to protect their communications from Western surveillance, and, far worse, has instructed terrorists how to cloak their communications as they plot future attacks against the US and our allies. Is that an achievement to be proud of?

When the next attack occurs, let's see if the press properly credits Snowden, Manning, and those other exalted leakers, for all those stolen secrets they then broadcast that seriously hobbled US national security defenses.