TITLE: Tapping President Trumps Wires – A Spy Hunters Perspective

Authors: James M. Atkinson; Stan Spring

Publication Date: March 17, 2017

SYNOPSIS: Our modern day lives are brief, very intense flashes of light, circling The World on ultra-pure puffs of smoke, and our government craves to capture all those flashes of lights.

Introduction

On March 4, 2017, President Donald Trump, the 45th President of the United States, penned the following Tweet: "March 4 Early Saturday morning, while away at his Mar-a-Lago estate in Florida, Trump fired off his first tweet accusing Obama of wiretapping his phones at Trump Tower in New York during the election."

That twitter message has spawned a daily furor of sound bites in the news media describing in great detail the denials, spins, double talk, within the ambit of congressional "concern". Although when John LeCarre chose to use the word "circus" to describe the highest echelon of Britain's MI6, it's secret intelligence service, it is doubtful that he envisioned the acute relevance "circus" has today to describe the Alice in Wonderland drama being presented in the media regarding President Trump's tweet.

The far more cogent, sinister and impacting story is not the circus drama between President Trump and his detractors: it is the fact that there is no doubt that routine clear intercepts and eavesdropping has and is continuing without a peep from any of the nationally recognized news agencies reminiscent of Rome's bread and circus days.

Detailed below is a detailed account of routine spy intercept programs which are designated as "legal" in which Trump Tower, like millions of others, were indeed intercepted. In the spirit of this looking glass wonderland, ongoing saga; let one say that "wiretapping" conveys the general idea of what has and is happening; however, as the sophists hone their skills in denials and articulations of denial, it should be said communications these days are not carried over "wires" but fiber optic cables. No doubt there will be a panoply of intelligence and congressional pundits pouncing on the distinction to prove that Trump is wrong. In fact, Trump is right. Here's why.

Modern Technological Marvels

Modern communications systems consist of three elements or functional sub-systems. The first is the called a *subscriber device* which converts speech or audio signals and video images (analog data) into a carefully standardized stream of data, whereby things like sound, photographs, and moving images are converted into their digital equivalents. An example is a traditional residential telephone or cable television box.

The second sub-system is called a *transmission system*, which includes a method to take the "carefully standardized stream of data that represents analog things" and send it to a shared interconnection point. This interconnection point is called a *switching system*. For each quantity of transmission systems, a different switching system is required. These switching systems are interconnected to other switching systems by means of interconnected transmission systems to form a global switching system.

Digital devices, like modern computers, video cameras, 4K televisions, cellular telephone, tablets and other technological marvels, connect to the Internet. Typically, these devices' signals originate digitally. The originating device is known as the *subscriber's device.*

Because modern communications systems, such as cable TV systems, cellular systems, and the Internet requires very rigid protocols or *technical etiquette*. These protocols allow manipulation of the systems so that they perform as intended and without interruption. Customers or *end users* are generally unaware that the protocols insuring quality digital quality reception are equally capable of spying on them.

In bygone years, Ma Bell installed two copper wires into a family's home for the telephone. These two copper, phone wires traveled from the home into a shared cable outside on the telephone pole. As these outside cables got closer to the switching center, the cables got thicker and bigger, incorporating huge numbers of other telephone wires. By the time these final cables reached Ma Bell's switching center, they were as thick as a person's wrist and often included over 600 telephone lines.

This method of phone service cabling had some serious setbacks. When the cables were more than a few miles away from the switching center, phone company engineers encountered problems with reliability and consistent service quality. These massive cables became highly vulnerable to wiretapping. Often, the switching station servicing these cables required several acres of equipment.

Massive Concentrated Access

With the advent of modern communications, the phone company began a new process called *multiplexing*. Multiplexing blended customers' phone signals together

with other customers' signals; thereby providing much greater number of phone numbers on existing cables. Rather than continue costly, massive cables, Ma Bell opted to install these multiplexers on the already existing phone architecture. The use of multiplexing was virtually invisible to the customer both when they were first used, and still to the modern day.

The next advance came with fiber optic cables. Initially, fiber optics were used by Ma Bell to interconnect their switching facilities in the U.S. as well as foreign switching stations connected by undersea cables across the oceans.

With the explosive consumer growth of the Internet and cell phones, fiber optic transmission systems are the preferred connection. Presently, the U.S. is interlaced with millions of miles of fiber optic cabling.

Today's fiber optic systems use multiplexers; just like the old, copper cable systems did before the rise of fiber. Modern fiber optic multiplexers reach thousands of miles, rather than copper system multiplexers that reached only a few miles.

Modern fiber enables the multiplexing of millions of customers on a single fiber the size of a human hair. Despite the small size, fiber renders astounding reliability and accuracy. Initially, fiber optic multiplexers required considerable human intervention to maintain the system. With technical advances, these fiber systems were programmed to maintain themselves with super quality and efficiency.

While fiber optic multiplexing systems deliver high quality, efficient communications; they contain inherent vulnerabilities and serious weaknesses that can be equally exploited as a superb, massive scale surveillance system.

The Fly in the Ointment

The most glaring vulnerability can be exploited with physical access to the multiplexer. With physical access to the multiplexer, tens of thousands of phones and computers can be invaded. By gaining physical access to the multiplexer, the software that runs the multiplexers can be hacked so all communications can be received at listening posts in Kunia, Hawaii or Lackland, Texas, for example.

So where are these multiplexers? Multiplexers are everywhere. It's no secret that the occupants of Trump Tower, like many luxury high-rise buildings in New York City, have multiplexers to operate their fiber optic systems.

The daily news is rife with allegations and denials of the eavesdropping of Trump Tower and President Trump during the 2016 campaign. Because Trump Towers is no different than other high rise buildings in New York City when it comes to communications (i.e. there are multiplexers), all of the computers and phone lines in

Trump Tower could have been compromised and tapped: compromised without zero oversight.

The invasion of these multiplexers is far more insidious than any eavesdropping performed during the days of copper wiring. Not only can all communications be intercepted, harmless desktop phones, computer cameras, cell phones, tablets and televisions can be remotely activated for full audio and video surveillance of a person's every moment. The microphones in the desktop phones, cell phones, computers, laptops, tablets and televisions can be activated even when these devices are "off".

Adding another twist to this murder mystery about who killed the victim, "privacy"; a modern eavesdropper with access to the multiplexer and its software, can direct the multiplexer to direct all data (including the remotely retrieved video and audio from a person's computers, phones, tablets, etc.) to dozens or hundreds of artificially created pathways leading to listening posts anywhere in the world

Freedom From Detection (Usually)

No eavesdropper likes to get caught. One problem with penetrating multiplexers and their software is that it is not complexly difficult to track additional fiber optic cables attached to a target system. By merely manipulating the multiplexer and its software, a skilled eavesdropper can insure his or her freedom from capture. This does not mean the eavesdropper is bullet proof. It does mean that it takes a highly skilled, well-equipped spy hunter to catch the eavesdropper.

Access By Default – A Key to Help the Eavesdroppers

There are millions of AT&T/Lucent, Conexant, Optisphere, Fujitsu and other fiber products in use throughout the United States. Believe it or not, factory default accounts and the default passwords are present in many systems even decades after their initial installation. In less than a minute of physical access to these multiplexers, multiple backdoors can be injected into the system for further, future use. Most remarkably, most multiplexers are installed in a locked, steel cabinet. Typically, these cabinets; however, literally have no back whatsoever. Others, while locked, often have the key hanging next to the "secure" multiplexer, or the key is actually in the lock.

Ironically, it is the exception, and not the norm, to find that the keys and passwords to multiplexers are not written on the lock box with keys hanging next to the box. Buildings in New York City, Boston, Chicago, Atlanta and other major cities across the U.S. are no exception to the norm.

Flexible Restrictions on the Government

The Constitution of the United States provides that no government entity or government employee, including law enforcement, is allowed to eavesdrop on any U.S. Citizen without a court order. Despite this guarantee, court orders are routinely obtained with hyperbolized, sworn "true facts" in which police either lie or distort the truth in order to fraudulently obtain the warrant.

Extremely careful examination of warrants, and the affidavits used by government officials to obtain them often reveals organized deceptions that are routinely used, and which gravely offend the Constitution of the United States.

Political eavesdropping has been around since the invention of the telephone and telegraph, and little has changed, but the technology. In politics, it is normal, and even common for a Watergate style of situation to take place, where one political party bugs the other political party, or the support team for one candidate bugs the candidate of the other party. It is a dirty business, but very commonplace, and very old tradition.

Reigning in the Government and Breaches of Constitutional Law

On March 4, 1789, the Bill of Rights consisting of the first ten amendments to the United States Constitution became the rule of law for these United States. Of particular import is the Fourth Amendment, which read:

> "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

On June 19, 1968, under the presidency of Lyndon B. Johnson, Congress enacted the Omnibus Crime Control and Safe Streets Act of 1968. Although the act is, more often than not, remembered for establishing the Law Enforcement Assistance Administration (LEAA); it also enacted sweeping restrictions and criminal penalties for the possession and use of "devices designed primarily for the surreptitious interception of wire and/or wire" communications. Title III also criminalized mere possession of bugging devices and associated wiretapping and eavesdropping.

Ironically, Title III, as it is generally referred to in law enforcement circles, was enacted because of Congressional concerns about abuses by law enforcement in electronic surveillance. This legislative concern is expressed in the Congressional record of same.

In 1974, Congress conducted an overview by establishing the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance. A 22 volume bound record of these proceedings was confected with a single volume report issued in 1976.

Despite the 4th Amendment and Title III restrictions, later issuance of Presidential Executive Orders, many cloaked under national security, coupled with a series of clever manipulations by intelligence agencies has resulted in wholesale eavesdropping for decades.

Of course, a whole new dicta has arisen to thwart these "guaranteed" rights of Americans. For example, NSA maintains that its' wholesale storage of every email, text message, phone call, fax, and other communications is not an "intercept". Only when data is retrieved and viewed does an "intercept" occur. As one will see, this news topic is nothing more than bread and circus drama for the masses.

The term "special relationship" often associated with the relationship between the United States and Great Britain will take on a much, much deeper meaning within the daily operations of the United States, United Kingdom (British), Canadian, Australia, and New Zealand intelligence agencies. This special relationship runs much deeper within the intelligence cabal of LeCarre's circus in Cambridge. With the use of this special relationship, the Canadian, United Kingdom, and United States countries with the rule of law, routinely side step Constitutional protections daily for a multitude of reasons, which include political spying and political repression.

Special Top Secret ECI Wiretapping

The United States government has a special relationship and written contract with every single company that provides undersea, fiber optic communications entering or exiting the United States. Under these contracts, the U.S. Government is provided with unrestricted back doors to every single fiber optic cable entering or leaving the US. There is even a special classification for any connection between the U.S. Government and specifically named companies who provide access to the their fiber cables inside these companies' transmission and/or switching systems. These access points are usually right at the multiplexers inside the communication company buildings.

The special relationship bears the classification "ECI" which stands for *Exceptionally Controlled Information*. This ECI designation means that the specific phone company or fiber optic operator has actually and formally granted the U.S. Government access to the most vulnerable portion(s) of its communications system. This access occurs with virtually no oversight or supervision. Through ECI, the U.S. government collects everything, missing nothing. These *collected* communications can be exploited months or years later. Without any supervision or oversight, one wonders who regulates the regulators? To avoid any accusations of abuse these government

entities exploit their special relationships by using what is called the *New York Reach Around*.

To achieve complete access and exploit the New York Reach Around, an interesting relationship has evolved between the government and fiber optic operators. In order for any fiber optic cable to enter or leave the United States, the operator is required to obtain a special license from the Federal Communications Commission (FCC).

This is procedure is maintained through a special national security department of the FCC called the *International Bureau.* The International Bureau, as a condition precedent to licensing, requires the cable operators to contract with the U.S. Government allowing full and complete access to the contents of each and every cable. By virtue of this agreement, any requirements for warrants or court orders are eviscerated. By virtue of these agreements, no oversight or supervision is required. These undersea cable operators and the U.S. Government of course do not advertise any of this.

FAIRVIEW LONG LINES TITANPOINTE SKYSCRAPER

For example, the U.S. Government has a series of contracts with AT&T in which AT&T agrees to permit the federal government unsupervised access to all customer communications that passed over its undersea cables, domestic transmission facilities, and domestic switching systems. In these documents,[1] AT&T is given a special code name. Each of its facilities where this sort of eavesdropping takes place is given different code names. For example, there are several major access points that are on domestic soil which AT&T (FAIRVIEW) has given the NSA access to, which use location codenames such as KILLINGTON, COPPERMOUNTAIN MAVERICK, WHISTLER, SUNVALLEY, CLIFFSIDE, TAHOE, BRECKENRIDGE, EAGLE, EDEN, TITANPOINTE (33 Thomas Street), PINECONE, SILVER COLLAM and others.

It does bear mentioning that when an ECI relationship is established that in various documents the company itself will be given one codename, then the overall project an umbrella name, then under the umbrella each portion will be give a code name, and then each location or sub-location, yet a different name, and tremendous care is take to isolate the name so there is little reference to one another.

To take this one more step, the AT&T Long Lines Building at 33 Thomas Street (code named TITANPOINTE) is operated by AT&T under a code name of LITHIUM, with RIMROCK access (a code name of for a hack into the 4ESS switching system), and also to the code name RIMROCK program by way of the satellite dishes on the roof. Thus, by way of the cable vault in the 3rd basement virtually anything in New York

[1] "Edward Snowden: the whistleblower behind the NSA surveillance revelations | US news". The

City can be tapped or tracked, and vast swathes of the inside of this building, as well as access to fiber optic systems are rented to the NSA, and even to the FBI. The TITANPOINTE is fed data from the PINECONE facility, which provides control and access to the shared fiber optic backboard, and the proprietary cables. This collected data is then funnel into the corporate networks of AT&T BLARNEY local area network (HIGHDECIBEL) and then into the corporate AT&T network to the codename PINWALE (RAGTIME) servers which harvest based on dictionary tasked terms. But, all of the aforementioned networks, access points, and hard drives all fall under the umbrella of codename FAIRVIEW. AT&T or Verizon controls the fiber optic or copper cables when they enter the cable subterranean vault, and AT&T operated the initial router or multiplexer that handled the cable/fiber that enters the building. Then AT&T runs the PINECONE SCIF inside TITANPOINTE which they hand off to another router/multiplexer in a "colocation" interconnection point and hand off the data from AT&T at that point over to the NSA under a interface called WEALTHYCUSTER (and NSA machine – the first NSA machine in the stream) which stiches together bits and bytes to reconstruct the intercepted data, which is then forwarded to another NSA owned and operated system called MAILORDER, which then sends the data to an AT&T gateway between MAILORDER and BLARNEY, and then to NSA leased lines to the NSA server called PINWALE (RAGTIME).

The aforementioned method is used to collect general Internet activities such as E-Mail, and web browsing. In order to capture voice, fax, or modem traffic via TITANPOINT thing are a bit more complicated, so they will be explained at this point. The routers inside the PINECONE facility at TITANPOINT need to process VOIP (voice over Internet protocol) in a different manner, so the AT&T MAILORDER router connects to VOIP traffic though code named SAGUARD by way of the TURNSTILE gateway. VOIP collection is fairly simple to harvest and then channelled to the NSA, but fax and modem calls are a little more complicated. AT&T RIMROCK Access (at TITANPOINTE) provides access to the fax and modem traffic, though codename NSA LOPERS which feeds voice signals directly to the NSA MAILORDER router (as above), but data and fax is processed through codenamed TINSEL/STONEGATE before it goes to the NSA MAILORDER server for the BLARNEY program at AT&T at the TITANPOINTE skyscraper. Then AT&T router splits off the metadata to a separate long term storage mechanism for use outside the NSA, but both the metadata and the actual call itself is copied to the NSA FAIRVIEW MAILORDER gateway to the NSA BLARNEY MAILORDER router and then the corporate MAILORDER and then split into one of two paths either through CONVEYANCE or FISHWAY to be stored in the NSA controlled NUCLEON or PINWALE servers. These functions then pass to Cisco Routers/multiplexer and then to a fiber optic SONET network to interconnect 15+ related eavesdropping nodes (BIRCHWOOD, MAYTAG, EAGLE, EDEN, TITANPOINTE, SUBSTRATUM, SPORTCOAT, QUEENSLAND, SCALLION, QUARTERPOUNDER, DOGHUT, HOMEMAKER, APPLE1, CLEVER DEVICE, *et. al).*

TITANPOINTE is also the primary hub for eavesdropping on the United Nations Headquarters, every foreign embassy in New York or surrounding area, the homes

of every foreign diplomat, and even the homes and offices of every lowly employee of every single embassy or diplomatic mission in the area. The is even two other backup sites in New York City which will take over eavesdropping on these targets should TITANPOINTE go off-line, plus a half dozen tertiary locations outside of the NYC area. The FBI and NSA actually lease four floors of this building (TITANPOINTE) as part of the BLARNEY program, and to get into one of these four floor a visitor must possess a Top Secret clearance and having been read into the ECI program for AT&T, Sprint, SCI, and other companies who are eavesdropped upon via this facility.

This is not even close to the full extend of the eavesdropping as AT&T, Verizon, Sprint, *et al.* also operates over 50 similar intercept location around the country, so that nothing escapes the eavesdropping machine run by the NSA.

COOL SPY HUNTING METHOD

Amusingly, the NSA even has reserved parking at TITANPOINTE, so that the undercover FBI vehicles driven from Maryland can park right in front of the building, along with their windshield mounted FBI issued SpeedPass that can be used to track their every movement. It is always wise to understand that there are spy hunters, who track the spies, no matter whom the spy is or whom they work for, and it is very easy to interrogate a SpeedPass/EZ-Pass module and then tack all those vehicle movements, and then in turn the movements of any cell phone in the vehicles, and then to track those same phones to NSA employees offices, homes, and so on. This of course can lead to the leasing company used for the cover vehicles, and then in turn to every undercover vehicles, and so on as the leasing company has installed tracking devices into all of their vehicles, so that the spy hunter can merely acquire the GPS logs of these vehicles, and geo-fence the TITANPOINT and related locations, and watch-the-watchers, even when they visit Guam.

Thereafter, AT&T will only be referred to directly in the initial contracts and papers used to setup the codenames. The assigned, new codenames are then used outside the initial set-up contract. Despite these maneuvers, highly skilled, trained and creative intelligence analysis can, through open source research, locate each and every one of these undersea cables, their locations, and incoming/outgoing points where the cables contact the company's multiplexers exploited by the U.S. Government. Because the Canadian and British governments have similar arrangements with cable operators in their countries, they mirror all the data the NSA collects, while NSA mirrors the same data the U.K.'s GCHQ a/k/a *Government Communications Headquarters* collects. This mirroring effect has evolved into a convenient, cozy special relationship bearing its progeny known as a *New York Reach Around*. Of course the United States also has a cozy, and very special relationship with the Canadian government agency responsible for handling wide scale eavesdropping thought the Communications Security Establishment (CSE), and all three agencies shared responsibilities and resources between each other.

When the President needs illegal eavesdropping to be performed that would clearly violate the Constitution of the United States, a requires will be made to the British or Canadian government under the guise of a terrorism case, and one or both of those governments will target the wires in the United States. Of course Australia (Australian Defence Signals Directorate – DSD) and New Zealand (Government Communications Security Bureau – GCSB) also have an equally special relationship so there ends up being five different countries, that have access into the fiber optic systems of the other countries, and who can and will have access things that were off limits to the primary company, and which will be unlawfully collected, and shared for political gain, and there is a special name called "Five Eyes" or "SPOKE" where all five of these nations spy on not merely the rest of the world, but also on each other of internal political controls.

The New York Reach Around

When a spy hunter is deploying his/her special skills and equipment, it is not uncommon to find a skyscraper on Park Avenue in New York City with a comprehensive, state of the art, and fiber optic communication system. This system's optical fibers initially pass to Pearl Street, Hudson, Eighth Avenue or Broad Street or any of a dozen other similar, interconnected communications facilities in New York City. From one of those locations, the skyscraper's communications bounce over to one of the numerous undersea cable stations located on Long Island or in New Jersey. From one of these points, the communications are delivered by undersea cable to England or Canada. When the communications are received in England, they then return to the United States to the phone company on Broad Street or Pearl Street after passing through a GCHQ beam splitter, and then an NSA controlled beam splitter.

This communications' delivery is, in spy hunting jargon, called the *New York Reach Around*. The signals from the Skyscraper on Parke Avenue, may actually not merely routed to Canadian, England, via East Coast fibers, but it may also end up getting routed through Australia and New Zealand systems, and re-enter the United States on the West coast, and pass across the country to return to New York City, just so all five nations get access to some business executive calling in a pizza order to the restaurant down the street from his office… during his presidential campaign.

There is an overriding reason the U.S. government pays a premium for this delivery system and uses it as much as it can. First, the various Congressional Committees that is supposed to supervise, do not. Second, communications desired to be intercepted against U.S. citizens physically inside the United States can legitimately be received by the NSA or other intelligence agencies from their counterparts in the UK, Canada and elsewhere.

It is a noteworthy, albeit troubling aspect of the international fiber optic landing stations in the United States, that every bit of data, every second of every phone call

and every frame of every video conference in Manhattan can be funneled out of the United States through the undersea cables in Mastic Beach, Far Rockaway, Crab Meadow, Manhattan Beach, or Long Beach, NY and sent to England. Once received legitimately in England by its GCHQ, the same data, phone call, videoconference can then be relayed back to the United States to be intercepted by the NSA.

To add icing on the cake, GCHQ and MI-5/MI-6 then prepare an analysis of what they saw on their side of the fiber for the NSA, while the NSA and CIA prepare an analysis for GCHQ of what was seen on this end. These special relationship partners exchange reports, and crisscross each other's reports for whatever purpose they desire, including political gain on both sides of the Atlantic. Similar arrangements exist with Canada, Australia, New Zealand and other countries.

It does bear mentioning that a skilled Technical Surveillance Counter Measures (TSCM) specialist can detect this sort of manipulation and can do so covertly.

The Five Eyes Reach Around in Action

To compound these special relationships, even private, leased fiber optic lines, which are only supposed to travel a few miles to the multiplexers they use, can be exploited using the New York Reach Around. These same, short run signals can be sent around the world, allowing each, receiving nation to obtain private information and communications of U.S. citizens. Of course, the US has no mechanism to prevent abuses by those foreign nations. Cynics might suggest such abuses by these foreign governments inures to the benefit of the U.S. government – all without any oversight.

Let one suppose, for example, there is an electronics engineer by the name of Mr. Atkinson (a U.S. Citizen) lives in the Boston area. He wishes to call a business customer in Manhattan (who is also a U.S. Citizen). The conversation involves the design of a telemetry encryption module for use in military drone aircraft operated by the United States and used for military strikes in foreign lands. Both Atkinson in Boston and the Manhattan business customer are electronics engineers for equipment of this type. Both have done these sorts of design projects together in the past. Presently, the U.S. Government uses modules on the Predator and Global Hawk drone aircraft engineered by these conversants. The designs are not classified or restricted, although the designs have tremendous competitive and strategic value. To insure their own security and privacy, both parties use a high performance encryption system that exceeds all, current military specifications.
As a result of the professions, work history and the fact they design military weapons systems; these conversants are of interest to intelligence agencies across the globe.

In the normal course of call routing, the communications between the two have to get routed from Boston to Canada, then to England. From England the conversations

are sent to Mastic Beach undersea landing station, then to Broad Street in NYC, and then to the Park Avenue skyscraper, and back again.

By this means, the governments of Canada and England have full access to these private, U.S. citizen communications. Simultaneously, the U.S. government gains mirror access since the communications crossed international borders.

The various intelligence agencies of all these three nations now are aware (if previously unknown) of these U.S. citizen parties. The result is that their further, future communications to or from anybody are given *extra special attention*. Interestingly, once any encryption is detected on communications (voice or data) the priority value for intercept increases and the targeting of past and future conversations goes up. These parties' future communications become targeted as intercepts of high value.

When intelligence services realize the existence of non-standardized encryption is being used, these services go into a frenzied mode to quickly try to adjust their analysis computers to accommodate the new encryption protocol. The end result of a U.S. citizen's attempt to secure privacy through encryption on phone calls can have the opposite effect. A U.S. Citizen can be targeted for no other reason than the use of strong encryption systems.

Shutting Down The NSA Interceptions, Legally

But, there is also a method by which U.S. Citizens can frustrate this, which the various spy agencies get highly upset when utilized. First, the U.S. citizen needs to have an unexpired U.S. Passport (this is vital). Second, they need to have a traditional telephone line installed into their homes, even if they do not use it. The phone line needs to be installed at the address they use on their U.S. Passport. They need to receive mail at this address, to include several magazine and newspaper subscriptions. They need to have all of their utility bills delivered to this address. Third, they need to register to vote, using this same address, and ensure that they are maintained on the local voting rolls or citizen census. Fourth, they need to ensure they register with the selective service through this address, use this address for their driver's license and any other sort of government license, and get politically oriented junk mail at this address. It is also important to gain cable TV service to this address, under the name of the U.S. citizen, and of course to do the same with any sort of cell phone service, so that there is a huge number of what are called Constitutional Anchors whereby the U.S. citizen creates a multilayered series of proofs that the location is in fact that of a U.S. citizen. To further strengthen these Constitutional Anchors the phone at the location needs to be answered rather formally by politely announcing the location the caller has reached, and then announcing the name of the person who is answering the call. The caller on the other end, then needs to state who they are, and where they are calling form so that to an eavesdropped there will be no question that both sides of the call are on U.S.

soil as this legally sabotages the various forms of the reach around in terms of forcing a sort of block where the intercept (tapping) may still take place, but the actual audio of the call is not supposed to be permitted into NSA records. It does not actually stop eavesdropping, but rather complicates matters for the government if or when they do eavesdrop. In addition, ensure that your cell phone or data plans have your home address lists as the billing address, and ensure that your cell phone number is on one of the exchanges listed within 15-20 miles of your home, is a direction opposite that of your nearest larger city. Of course, you do not want the phone number to be any prefix or exchange within 30 miles of Washington, DC nor within a 50 mile radius of New York City, NY, or 30 mile radius of White Plains, NY.

Decades of Unlawful Eavesdropping Results in "More Careful" Wiretapping

After many decades of severe abuse by U.S. Intelligence Agencies unlawfully spying on U.S. Citizens, President Reagan, in 1981, issued Executive Order 12333. This Executive Order also had a classified addendum to it. While in the public document the President ordered U.S. Government agencies to knock it off; the private, non-public classified addendum[2] allowed them to continue providing they were merely *more careful*. The *more careful* part still permitted wholesale eavesdropping. It authorized the storage of intercepted data until the end of time. It further required that when government agencies went sifting through the intercepted materials, they were supposed to ignore anything involving U.S. Citizens. This was widely ignored.[3]

A Long History of Presidents Bugging Their Political Opponents

The National Security Agency (NSA) was formed in 1952 during the Truman Administration as a covert agency within the Department of Defense. Initially its personnel were largely Army personnel intermixed with CIA personnel. The NSA (members jokingly called it *No Such Agency*) was hidden from Congress. It was adroitly designed as an extension of the Armed Forces Security Agency formed in 1945 (also under Truman).

Even prior to 1945, going back to July 1917 (during the Wilson administration), when Herbert O. Yardley became the head of the Cipher Bureau of Military Intelligence (MI-8), he immediately targeted U.S. citizens and New York based businesses initiating eavesdropping against them through the *Black Chamber*.[4] The abundance of positive history of these agencies must be objectively combined with

[2] https://www.dni.gov/files/documents/0909/DoD%20Procedures%20Classified%20Annex.pdf
[3] https://www.dni.gov/files/documents/0909/DoD%20Procedures%20Classified%20Annex.pdf
[4] "Factbox: History of mass surveillance in the United States". Reuters.

the abundance of illegal eavesdropping against U.S. citizens for political purposes in which they also engaged. [5]

During the Eisenhower administration, Eisenhower ordered the to initiate a massive eavesdropping campaign on civil rights activists and leaders such as the Reverend Martin Luther King. The Southern Christian Leadership Conference was viewed as a tool of racial and religious oppression also subject to government eavesdropping. [6]

Under both the Johnson and Nixon administrations, the NSA was ordered to spy on the poor and poverty stricken (mostly Black) citizens of the United States to provide the President with leverage from which he could marginalize the poor blacks in terms of voting. This NSA program was not subtle. It was used to manipulate the respective Presidential campaigns. [7]

At the beginning of the Nixon Administration, Nixon repurposed part of the NSA to spy on his political enemies and anyone else he felt might provide future "political difficulties". Nixon went so far as eavesdropping on Congressional members and Justices of the Supreme Court using the NSA. Nixon, during his era, felt justified in having Black, Jewish, and poor U.S. Citizens bugged or wiretapped.[8]

Let Us Not Forget "Tricky Dickey"

The very grave constitutional violations by President Nixon were merely a side effect of identical abuses that went unchecked by Presidents Johnson, Eisenhower, Truman, and others. President Nixon pushed the envelope to an all time pinnacle of misconduct. Nixon's conduct regarding electronic surveillance was so egregious that Congress stepped in during the Ford Administration. As a response to the Nixon era abuses, Congress formed the Church Commission to investigate serious misconduct by not only the FBI, but also the CIA and the NSA. All three had been used for eavesdropping and intelligence activities against Blacks, Jews, Communists, Socialists, and Nixon's political enemies = real or simply perceived. The final report of the Church Committee dealt harshly with these agencies and their Presidentially ordered (mostly through Nixon) criminal conduct:

> "The Committee finds that the domestic activities of the intelligence community at times violated specific statutory prohibitions and infringed the constitutional rights of American citizens. The legal questions involved in intelligence programs were often not considered. On other occasions, they

[5] Herbert Yardley, *The American Black Chamber* (Bobbs-Merrill, 1931)
[6] http://www.cnn.com/2008/US/03/31/mlk.fbi.conspiracy/
[7] http://www.heritage.org/commentary/lyndon-johnsons-watergate
[8] http://www.nytimes.com/1999/02/26/us/in-tapes-nixon-muses-about-break-ins-at-foreign-embassies.html?pagewanted=2

> were intentionally disregarded in the belief that because the programs served the "national security" the law did not apply. While intelligence officers on occasion failed to disclose to their superiors programs which were illegal or of questionable legality, the Committee finds that the most serious breaches of duty were those of senior officials, who were responsible for controlling intelligence activities and generally failed to assure compliance with the law. Many of the techniques used would be intolerable in a democratic society even if all of the targets had been involved in violent activity, but COINTELPRO went far beyond that ... the Bureau conducted a sophisticated vigilante operation aimed squarely at preventing the exercise of First Amendment rights of speech and association, on the theory that preventing the growth of dangerous groups and the propagation of dangerous ideas would protect the national security and deter violence." - *Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans . United States Senate.*

The Church Committee was initially formed to investigate the wrongdoing of the FBI during the Civil Rights era. Quickly, however, it found that the NSA and CIA were also working hand in glove with the FBI to target Blacks, Jews, and the poverty stricken. The only criteria required were being deemed by the President to be a political enemy.

The Church Committee also found that President Kennedy had ordered wiretaps of congressional staff members, various members of the executive branch, Congressmen, lobbyists, law firms, attorneys, and others strictly for political gain.

The Church Committee found President Eisenhower ordered Justices of the Supreme Court be wiretapped for Eisenhower's political gain. President Johnson ordered extensive espionage, which included wiretapping during the 1964 Democratic Convention in an active effort to manipulate the Presidential campaign. The Committee also found that Johnson illegally wiretapped the Republican Party and the Senate to insure his presidential election in 1964.

The Church Committee identified major Constitutional breaches and unlawful wiretapping, burglaries, warrantless searches, and related prohibited actions by Presidents Roosevelt (1933 – 1945); President Truman (1945 – 1953); President Eisenhower (1953 – 1091); President Kennedy (1961 – 1963); President Johnson (1963 – 1969); and of course President Nixon (1969 – 1974).

The Church Committee also stated:

> "Too many people have been spied upon by too many Government agencies and too much information has been illegally collected. The Government has often undertaken the secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts on behalf of a hostile foreign power. The Government, operating

> primarily through secret and biased informants, but also using other intrusive techniques such as wiretaps, microphone "bugs", surreptitious mail opening, and break-ins, has swept in vast amounts of information about the personal lives, views, and associations of American citizens. Investigations of groups deemed potentially dangerous—and even of groups suspected of associating with potentially dangerous organizations—have continued for decades, despite the fact that those groups did not engage in unlawful activity.
>
> Groups and individuals have been assaulted, repressed, harassed and disrupted because of their political views, social beliefs and their lifestyles. Investigations have been based upon vague standards whose breadth made excessive collection inevitable. Unsavory, harmful and vicious tactics have been employed—including anonymous attempts to break up marriages, disrupt meetings, ostracize persons from their professions, and provoke target groups into rivalries that might result in deaths. Intelligence agencies have served the political and personal objectives of presidents and other high officials. While the agencies often committed excesses in response to pressure from high officials in the Executive branch and Congress, they also occasionally initiated improper activities and then concealed them from officials whom they had a duty to inform.
>
> Governmental officials—including those whose principal duty is to enforce the law—have violated or ignored the law over long periods of time and have advocated and defended their right to break the law.
>
> The Constitutional system of checks and balances has not adequately controlled intelligence activities. Until recently the Executive branch has neither delineated the scope of permissible activities nor established procedures for supervising intelligence agencies. Congress has failed to exercise sufficient oversight, seldom questioning the use to which its appropriations were being put. Most domestic intelligence issues have not reached the courts, and in those cases when they have reached the courts, the judiciary has been reluctant to grapple with them." - *Intelligence Activities and the Rights of Americans Book II, Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities United States Senate (Church Committee)". United States Senate.*

During the Ford and Carter administrations, there was illegal eavesdropping on U.S. Citizens. The Church Committee's carnage is attributed for the much-reduced scale of illegal eavesdropping by Ford and Carter. The eavesdropping, which did occur, became more sophisticated in that it was undertaken with much greater care with

an eye toward deniability. The NSA and CIA also set about to redefine themselves in order to avoid prior misconduct over the prior decades. [9]

President Reagan essentially issued a *body slam* to all U.S. intelligence agencies by publicly forcing them to back off illegal surveillance of U.S. Citizens. This public slam was tempered with his classified order addendum, which gave the intelligence agencies several loopholes from which to operate unencumbered. This was the landmark Executive Order 12333 and entitled *United States Intelligence Activities*.

Unlawful Wiretapping Under FISA

In the world of espionage against U.S. Citizens, tension exists between Regan's Executive Order 12333 and a law called the *Foreign Intelligence Surveillance Act* or FISA. When a federal agency wishes to avoid any inconvenience of obtaining a court order to eavesdrop, claims that the target is a foreign national, foreign agent of influence, or simply not a U.S. Citizen facilitates a secret and unbridled FISA warrant. Interestingly the secret FISC/FISA court is located in the E. Barrett Prettyman United States Courthouse in Washington, D.C., but the actual judges are drawn from the Federal District Court Judges across the country, and who essentially (and secretly) telecommute to the secret FISA court for a period of service. In this manner of rotating the judges, the FISC/FISA court keeps secret the names of the judges involved, so they can effect operate what is called a *Star Chamber* and evade oversight of their actions.

Another current day ploy by intelligence agencies to eavesdrop without obtaining any warrant is to perform their warrantless eavesdropping under the guise or the label of a training exercise in which they "inadvertently" stumbled upon the information intercepted.

During the Bush (Sr.) Presidency from 1989-1993 a great deal of illicit eavesdropping against U.S. citizens existed.[10] It was restrained by comparison to present day due to a technical obstacle. Bush's obstacle was that online communications were growing faster than the government's ability to collect and store what it wanted. The prior focus on U.S. citizens decreased. This decrease; however, was due to the surge in foreign communications clogging up U.S. telecommunications. The Reach Around time for valuable, intercepted information was painfully long. A solution; however, was about to take hold.

The Clinton Administration (1993-2001), enacted a series of laws which required every company who made telecommunications equipment or provided

[9] https://www.rt.com/usa/nsa-spies-jimmy-carter-457/
[10] http://www.usatoday.com/story/news/2015/04/07/dea-bulk-telephone-surveillance-operation/70808616/

communications services to build special back doors that enabled the United States, State, and Local government unsupervised access to communications systems and equipment. This legislation was called the *Communications Assistance for Law Enforcement Act* or CALEA.

Under CALEA, every company who provided any sort of service (lets say AT&T, Sprint or T-Mobile), built backdoors into every element of their system enabling law enforcement warrantless, to at will log on to a special network. The only requirement was for law enforcement to plug in the phone number or address they wanted bugged. Once entered, Voila! the target was bugged; bugged with no warrant, no oversight and no accountability. Sprint denied the existence of the special network. Sprint's denial was exposed as a lie when one of their Law Enforcement liaisons got caught on video giving lessons on how to wiretap via Sprint (via SINS) at an FBI sponsored NATIA trade show and how to do it "off-the-record." [11]

With CALEA, everyday police were now on a par with intelligence agencies: instant eavesdrop without any warrant, supervision, or accountability. Between 1968 (Title III) and CALEA, Congressional concern for law enforcement eavesdropping abuses which predicated the enactment of Title III obviously waned,

Apparently not satisfied with CALEA'S special network, during the Clinton Administration, the *New York Reach Around* became a finely honed art form. It is estimated that half of the GOP had their calls passed to foreign fiber optic cables using the *New York Reach Around* insuring their phone calls were captured for later analysis. It was stunningly expensive to perform this type of loop. It was so much so that AT&T established special facilities just to handle all the extra data flowing on their undersea international cables.[12]

And Then There was 9/11

President Bush (Jr.) was barely in office when 9/11 happened. Bush's immediate response was to instantly wiretap everything nationally, internationally, globally-anything and everything based merely on his authority as President without reservation or understanding of what exactly was going on. A close examination of the historical documents called the *President's Surveillance Program* or PSP reveals Bush had little understanding of exactly what he was signing or authorizing at the time. Curiously the Democratic leaders of the Senate Oversight Committee, pushed quite hard for Bush to sign it. A veteran of the Watergate debacle (Mr. Cheney) is seen in these historical documents dragging the top five communications companies to the White House to "get them to volunteer." After they volunteered, a new law

[11] PowerPoint Slide and video recording of Sprint SINS presentation at NATIA conference, 2004
[12] The Electronic Police State: 2008 National Rankings, by Jonathan Logan, Cryptohippie USA

was confected to insulate them from suit by citizens if it was ever revealed that this massive PSP program was in place. [13]

The PSP required reauthorization every 45 days; the last presidential semi-public reauthorization was in February 2007. In the same year, the PSP was renamed and passed into law as the *FISA Amendment Act* of July 2008.

During the Presidential Campaign of 2005, President Bush ordered the bugging, eavesdropping, and wiretapping of Democratic candidates, their support staff, political protesters, journalists, and thousands of other citizens under the justification that they might have terrorist connections.[14] Bush even went so far as having intelligence agencies sprinkle in enough probable cause to obtain secret arrest warrants issued on U.S. citizens authorizing pulling these US citizens off the street, hold them without due process and hide them from the courts in violation of U.S. Law. [15] At the time, the kidnapping and detention of politically active citizens was called the *Bush-Cheney Program* or at other times called the *Nixon-Cheney Detention Program.* [16] It was Cheney who orchestrated the initial variations of the illegal detention of U.S. Citizens during the Nixon Presidency. [17]

The Grand American Tradition Continues

As President Obama rose to become the national leader, a grand repurposing of the Bush-era PSP took place. A new hybrid arrangement came to be in which every U.S. Citizen's phone calls and data were captured, recorded, indexed and sifted with the tools which under the Bush (Jr.) administration were primarily for the frenzied detection of terrorism. These tools under the hybrid arrangement were used towards political ends and internal social control. [18] This laissez faire attitude engendered during the administration of a former "senior lecturer" Constitutional law professor at the University of Chicago eventually was publicly exposed. [19]

The National Security Agency (NSA) is the primary entity responsible for eavesdropping in and on the United States. Prior to 1981 the NSA was out of control.

---

[13] Inspectors General of the DoD, DOJ, CIA, NSA, and ODNI (2009-07-10). Unclassified Report on the President's Surveillance Program

[14] Johnson, Carrie; Nakashima, Ellen (2009-07-11). "Inspectors General Report Faults Secrecy of Surveillance Program". The Washington Post.

[15] https://www.nyclu.org/en/press-releases/victory-unlawful-mass-arrest-during-2004-rnc-largest-protest-settlement-history

[16] https://harpers.org/archive/2016/04/legalize-it-all/

[17] https://www.forbes.com/sites/eriksherman/2016/03/23/nixons-drug-war-an-excuse-to-lock-up-blacks-and-protesters-continues/#29e3524a42c8

[18] http://www.saturdayeveningpost.com/2014/04/17/culture/politics/a-brief-history-of-the-nsa.html

[19] https://www.theguardian.com/us-news/the-nsa-files

[20] After 9/11/2001 until 2005, when thousands of pages of classified documents were leaked about the quite illegal NSA surveillance program followed by leaks in 2008, 2009 and 2013, the full extent of NSA's spying on US citizens was revealed. By the time the 2013 debacle occurred, officials of the NSA were already lying to Congressional oversight committees about what they were doing (illegally).[21] The NSA got kicked into overdrive, on U.S. soil, against U.S. Citizens (illegally).[22]

Chain of Fools

In the intelligence community, there is a method called *Call Chaining*, which has existed since the days of the introduction of telegraph communications. Call Chaining is used to analyze calling patterns or E-mail patterns to sniff out the far ends of a communications network. For example, lets say that A calls B. B then sends and E-Mail to C. C forwards the E-mail from B with comments to D. D then faxes it to E. E then posts it on Facebook.

Usually a chain is kept confined because large amounts of irrelevant data are collected – so much so that it turns the charts to mush. Bush (Jr.) understood this. During Bush's administration the levels of chaining were against people with known terrorist ties in the United States, more than a few thousand.[23] Under the Obama interpretation of call-chaining not only did A through E get brought into the system becoming an eavesdropping target - so did every single user of Facebook, YouTube, or Google, or whatever other service was involved. [24] Obama's interpretation maximized data collection to new heights thereby allowing his government to illegally, but defensively eavesdrop on pretty much anybody in the U.S. they wished, for whatever reason.[25]

One of the tremendous problems with the current Internet is government agencies use this chaining method to remotely connect an innocent person to someone involved in drug trafficking, terrorism, arms smuggling. These extremely remote links will then be used as a basis of probable cause, even when there is no probable cause, and by the mere recitation of unrelated facts there will be an administrative finding sufficient to trigger wholesale eavesdropping.

---

[20] Inspectors General of the DoD, DOJ, CIA, NSA, and ODNI (2009-07-10). Unclassified Report on the President's Surveillance Program

[21]https://www.usnews.com/news/articles/2016-11-17/lawmakers-resume-calls-for-james-clapper-perjury-charges

[22] https://www.dni.gov/files/documents/2013-06 21%20DNI%20Ltr%20to%20Sen.%20Feinstein.pdf

[23] https://www.techdirt.com/articles/20140629/16130227727/nsa-appears-to-be-chaining-calls-using-phone-numbers-one-hop-out-as-new-originating-selectors.shtml

[24] http://electrospaces.blogspot.com/2016/02/how-nsa-contact-chaining-combines.html

[25] NSA collected US email records in bulk for more than two years under Obama, guardian.co.uk and Memorandum for the Attorney General "Metadata Associated with Person in the United States", November 20, 2007

I'm a US Citizen – I'm Not a Terrorist I Just Wanted to See Paris

A U.S. Citizen wants to vacation in France. This U.S. tourist wants to visit the Eiffel Tower. As any experienced, international traveler would do, the tourist performs a series of Google searches for hotels, restaurants, parks, currency exchange rates and transit means in Paris.

While the US tourist is preparing for the ultimate Paris vacation, a terrorist in Iran will travel to Paris. The terrorist is obviously not a simple tourist, but rather someone more sinister. The terrorist; however, performs similar Google searches as the U.S. tourist. The U.S. government has been tracking the Iranian terrorist for the past 15 years, and the U.S. since the date of their birth.

Although the U.S. citizen is nothing more than an innocent tourist, because both Google searches are similar, a link will be forged for each intersection of these searches in time, and place of either. Thus the innocent U.S. Citizen becomes interlaced into the whirlpool of a terrorism case. Every piece of electronics in the U.S., innocent tourist's life can now be used against him to attempt to prove or disprove the tourist is involved with the Iranian terrorist. The *probable cause* will be that the terrorist and tourist are going to be in Paris around the same time suggesting that tourist and terrorist are somehow linked. Using *call chaining,* as interpreted under the Obama Administration, every other person with whom the tourist has dealings during the duration of their life has now fallen within the ambit of the whirlpool terrorist case. In short, they are all fair game…

In Hatred We Trust

President Johnson expressed prejudice against Blacks,[26] while President Nixon expressed prejudice against Jews and Blacks.[27] Both Johnson and Nixon were quite vocal expressing prejudice supported by the audio recordings of their mutual anti-sematic and racist rants which are quite epic.[28]

[26] Theodore White. Breach of Faith: The Fall of Richard Nixon. Readers Digest Press, Athineum Publishers
[27] Theodore White. Breach of Faith: The Fall of Richard Nixon. Readers Digest Press, Athineum Publishers
[28] White, Theodore Harold (1975). Breach of faith: the fall of Richard Nixon. New York: Atheneum Publishers. ISBN 0-689-10658-0

The man, who would someday become Vice President Cheney, expressed similar prejudices heard on audio recordings that are of significant historical record.[29]

President Obama, on the other hand, has espoused prejudice against Jews, [30]Christians,[31] the nation of Israel, [32]white people,[33] rich people[34] save a small group of Democratic political leaders his party was grooming for the Presidency and long term positions in Congress.

There was widespread politically based eavesdropping against Mitt Romney and his campaign ahead of the 2012 election to insure President Obama's re-election. [35] There was even more intense eavesdropping ahead of the 2016 elections. [36]

The intelligence community even referenced to the anti-Romney surveillance program as a *Lynn Reach Around* as vast swaths of Romney communications were routed off shore through an undersea cable in Lynn, MA to Canada and England and then returned to the United States through the NSA listening posts on those cables. The information was harvested to cement the second term of President Obama.[37]

Obama covertly listed Israel as a national enemy on par with China, Russia, Iran, Pakistan, Cuba, and North Korea.[38] In fiscal year 2011, Obama ordered billions of dollars be spent in trying to destabilize Israel, subvert its government to destroy them. [39]

2016 - The Established Political Structures Begin to Shake

In the Presidential election of 2016, a political earthquake sent tremors throughout the U.S. political establishment. Out of nowhere, a candidate came rolling in, paid his

---

[29] https://www.washingtonpost.com/opinions/woodward-and-bernstein-40-years-after-watergate-nixon-was-far-worse-than-we-thought/2012/06/08/gJQAlsi0NV_story.html?utm_term=.ae70fe3db14e
[30] FY 2013 Congressional Budget Justification, Volume I, National Intelligence Program Summary, February 2012
[31] https://wallbuilders.com/americas-biblically-hostile-u-s-president/
[32] FY 2013 Congressional Budget Justification, Volume I, National Intelligence Program Summary, February 2012
[33] http://www.washingtontimes.com/news/2016/jul/11/obama-tramples-on-high-ideals-of-america-fuels-bla/
[34] http://www.wnd.com/2015/03/how-deep-is-obamas-anti-israel-bias/
[35] Report regarding Technical Surveillance Counter Measures inspection dated July 19, 2012
[36] https://www.nytimes.com/2017/03/04/us/politics/trump-obama-tap-phones.html?_r=0
[37] https://www.nytimes.com/2017/03/04/us/politics/trump-obama-tap-phones.html?_r=0
[38] FY 2013 Congressional Budget Justification, Volume I, National Intelligence Program Summary, February 2012
[39] FY 2013 Congressional Budget Justification, Volume I, National Intelligence Program Summary, February 2012

own way, and promoted a program of *draining the swamp*- a swamp that had been festering for decades.

The Obama administration and self-styled political "experts" did not believe that candidate, Donald Trump, had any possibility of winning. At the time U.S. citizens listened closely to what all of the candidates had to say. American voters rejected candidate Sanders as a bit unconventional; perceived candidate Clinton as being corrupt; and viewed candidate Trump as inexperienced in politics. Nevertheless, Mr. Trump was a powerhouse of a businessman, who knew how to "cut bait" and get things done, and most importantly, how to get things done without playing cute political games or engaging in long useless plots and sub-plots, or in political gamesmanship, or weaving a net or mystery and intrigue. He was the very rare candidate who said what he meant, and who refused to back down, and to his opponents this was a terrifying option.

When it became obvious that candidate Trump led in the polls, a sheer panic spread throughout the beltway crowd. Trump was not merely the front-runner of the Presidential election, but he was projected to win by a wide margin.[40] Trump vowed he would "spay and neuter" the agendas and programs abusing U.S. citizens. Trump would tend to strongly favor Israel: a direct contradiction to Obama's views and machinations. Many career beltway political leaders foresaw their careers and political power come to an abrupt end.

Considering the presidential, political bugging, wiretapping, burglaries, and political dirty trick programs that are historically documented from Truman to Bush, as well and considering the sophisticated surveillance tools available during the Obama administration, is it reasonable to suspect that President Obama exploited these tools and methods for political purposes against Candidate Trump?

Street Wise, and Privacy Astute

Donald Trump is a self-made, streetwise New York businessman, who conducted his business affairs with what the intelligence community would call "good tradecraft" became the candidate, Trump. Trump had decades of experience being subjected to political attacks, business attacks, business downturns, and he himself and his businesses being the victim of illegal eavesdropping, sabotage, espionage, and dirty tricks. Through this crucible of negative experience, Trump learned how to conduct his business and personal matters with a certain level of discretion.

When exploring the possibility of his presidential candidacy, Trump approached it much the same way as his business approach. Trump leveraged a close, tight knit

[40] https://heatst.com/world/exclusive-fbi-granted-fisa-warrant-covering-trump-camps-ties-to-russia/

group of advisors; highly complex advisors who could be trusted not to betray his trust. When Trump announced his candidacy, deep tremors reverberated throughout both the GOP and the DNC in anticipation of a viable threat to the then balance of power- a viable threat envisioned which would rip the power of the status quo out of the hands of the Democrats, and which would also shake up the Republicans.

For the most part, Trump operated his campaign out of Trump Tower. Trump Tower is located in New York City and, yes, in Trump Tower there are several racks of fiber optic multiplexers. These multiplexers were installed when Trump was renovating all of his properties with extremely high-speed fiber optics - for himself, his companies, his tenants and his guests.[41]

Mr. Trump had for years been a firm advocate for the use of fiber optics between his properties and the phone company, investing a small fortune insuring that fiber was established in all properties. The fiber optics installed came with an abundance of extra capacity. These Trump fiber optics had a solid installation with multiple layers of redundancy and security - especially the security. [42]

Anticipating that Trump might be the target of wiretapping (using the broad definition meaning collecting data, voice, video, and location data) Trump had the systems "hardened". A hardened system defends against the possibility that if someone did manage to access his wires and fiber, whatever was collected would have little, if any, value because it would be difficult to decrypt. [43]

The greatest vulnerability of the Trump system; however, was the fiber optic multiplexers in these buildings and matching multiplexers at the phone company- not the fiber cables themselves. If and when these multiplexers were targeted and accessed, they could be used to subvert any cryptographic methods or good tradecraft in use. To do this would require the intervention of governmental entities as they held the secrets of the cryptographic weakness his systems utilized.

Behold, The Emperor is Naked

In the United States, companies that manufacture cryptographic or encryption products share the proprietary secrets of their products with the U.S. government. Possessing this proprietary information enables the government to confect a mechanism to detect and instantly decrypt data or phones calls that were encrypted. This typically boils down to the company advertising an encryption key that is a

[41] http://www.multifamilybiz.com/News/1365/Trump_and_Verizon_Do_Fiber_Optic_Deal
[42] https://www.fiberopticsonline.com/doc/two-of-donald-trumps-super-luxurious-building-0001
[43] https://www.fiberopticsonline.com/doc/two-of-donald-trumps-super-luxurious-building-0001

certain number of bits long. In reality, the encryption key is a pseudo-key with actual variations of only 12 bits.

Huge Steel Box, to Hide a Very Small Key

Putting the technical statements into English for everyone, imagine there is a key to your house. The key is hidden in a very large, steel box. The box is filled with packing materials. The key to your house is the size of an ordinary house key.

On your house you have a door lock that accepts only one key; however, there are 4095 keys that can unlock your lock, but only one key actually fits into the lock. The key can be packed in a very large box with a huge volume of packing materials. No matter how big the box may be, the true key size that unlocks the front door remains the same.

The key size of the true key is actually only 12 bits long. Being 12 bits long results in 4096 variations of the true key regardless of how big a box or how much packing material in jammed inside.

The NSA or GCHQ can very rapidly decrypt communications that have been subject to robust encryption. They merely have a computer try the 4096 keys while completely ignoring the huge steel box and packing material in which the true key is hidden in.

In some cases the true key may be even smaller, and the pseudo key even larger. For example, there is a U.S. made encryption product with uses a 1024 bit key, but the size of the pseudo key and the true key is only 6 bits. This means that there are only 64 variations of the key, which makes it profoundly each to merely have a machine insert each of the keys into a lock and test it until he door opens. Users; however, tend to obsess over the “key size” and not what the key on how strong the lock is, or the weaknesses in the lock, or the fact that a modern computer can merely “brute force” the keys by actually trying all the keys until the lock is tripped, or rather the encrypted data is rendered unencrypted due to the deliberate weakness in the keying system.

Pseudo Scrambling As an Illusion of Encryption

Fiber optic multiplexers utilize data scrambling to help distribute the flashes of light on an equal basis as the lasers that shoot the light into the fiber and to keep things balanced. The fiber only works properly when there is an even number of flashes to the number of non- flashes.

If the laser is on too many times (relative to the period it is off) there will be a spike in errors and a rapid thermal destruction of the laser. To smooth out the heat, a

primitive method of insuring an even number of 1's and 0's (digital binary code) are transmitted, a very standardized formula in Boolean algebra involving exclusive OR gates and fixed points in a feedback loop is used to mix up or scramble the data.

The companies who sell and install fiber optic multiplexers tout this scrambling as a solid security feature. The scrambling might be effective with eavesdroppers on par with elementary school students; however, if the algorithm is known and published, the scrambling scheme can be undone by eavesdroppers on par with middle school students and exploited by eavesdroppers on par with high school students.

While actually tapping a fiber optic multiplexer may be outside the scope of what a high school student can manage (unless they are a quite gifted student), it is not outside the realm of what a typical computer science college student can manage. Without question it is well within the capabilities of a national intelligence or military agency.

Tapping the "Wires" of President Trump

In the 2016 Presidential election, the NSA tapped the fiber optic cables to all of the Trump properties. The cables likely remained tapped right up to the moment he took the oath of office.

Again "tapped" is technically an incorrect word. It is more accurate to say the fiber was rather diverted from the phone company multiplexers to Canada and England, then routed back to the United States and injected back into the phone company switching system in New York City.

The records of the NSA, FBI, and CIA will be mute on the topic since supervision is as sparse as any records by the NSA, FBI or CIA. There are; however, records that do provide concrete evidence: the true holder of records will be the maintenance and system operation control logs for the multiplexers in Trump Tower and the other Trump properties. Additionally the related records in the possession of the phone company also contain the evidence. Most especially the records dated the day of, or the day just before the inauguration is of extreme interest.

The NSA, DOJ, FBI, and CIA are aware of these records. They are also aware that if President Trump asks the right person the right question(s) in the intelligence community to their face, the President will be told that indeed his wires (or more accurately his fibers) were tapped during the Presidential election. But, the President will have to be very direct when this question is asked, and he can not permit the matter to be "researched" as it will ignite a cover-up. Rather, the question has to specifically answer in a 1:1 face to face meeting, as this triggers a specific form of candor.

On the other hand, it would not be unlikely if publically that same person who confesses to the President will tell a different story to Congressional oversight committees, the media and the public. Alternatively, the whistleblower might simply be unavailable having been posted to some far reaches of the globe. It would not be unlikely to encounter a vast smoke screen around who did what, who knew what and to what extent.

Another variable in this morass of political mischief is that there are several government entities whose mere existence is supposed to be classified. For example, there is an entity in the DC area, which is reputed to perform high level political burglaries, bugging and eavesdropping. This entity is a fusion between the NSA and CIA called the *Specialized Collection Service* or SCS in Beltsville, Maryland. [44]

In the past this entity was reputed to have bugged Presidential candidates, merely because they were ordered to do so by the incumbent President. As an amusing aside, the employees of this entity are career intelligence officers and technicians. When provided liberal amounts of alcohol tongues wag. Many of them are very discontent in their positions and are "ETOH" vulnerable (ethanol alcohol), to say the least.

Washington DC Plumbers

There are also dozens of companies (most likely hundreds) in the Washington, DC area, that "do plumbing" (an old Watergate-era joke), in which the spy who formerly worked for the U.S. government performing illegal break-ins, burglaries, wiretapping, and other prohibited acts, at the direction of the President, or at the direction of his Chief-of-Staff, or party director.[45] As they are outside of the U.S. government, if/when they get caught, the government can officially deny any involvement, while handing over proverbial briefcases of cash. The prime example is the Watergate minions who got caught in the middle of an illegal bugging, ordered by the White House: a bugging that was done strictly for political gain, unlawfully… and the tradition goes on.[46]

One Foreigner in the Building

Because fiber optic multiplexers are shared by all occupants of a building, as soon as one non-U.S. citizen steps foot onto a Trump property or into Trump Tower, the NSA

[44] Vest, Jason; Madsen, Wayne (March 2, 1999). "A Most Unusual Collection Agency". The Village Voice.
[45] G. Gordon Liddy deposition in Maureen K. Dean and John W. Dean v. St. Martin's Press et al., United States District Court for the District of Columbia. Case No. 92 1807 (HHG)
[46] The Watergate Files presented by The Gerald R. Ford Museum & Library

and FBI can justify penetration and reprogramming of the multiplexers at either the Trump Property or the phone company or both. It is likely they will justify a full collection of everything on the fibers (or wires) looking for at least one instance of the foreigner engaging is some sort of activity. Considering the Obama administration Call Chaining and its application to innocent U.S. citizens, this justification within present intelligence parameters is far, far from far fetched.

While the NSA is supposed to destroy the data and phone calls of the U.S. citizens in the building, whistleblowers report they do not and will not. Rather the NSA simply gives lip service. There is high confidence that the director of the NSA will not lie directly to the President's face to a direct demand for a truthful answer to the right question. The origination of the March 4th tweet suggests the President did ask the appropriate question to someone's face and got a direct answer that someone did not wish to give.

In Time, the Details Will Be Told

The Truth Will Set Your Free – It's Just a Bitch Getting There

In time, the full details of the 2016 election machinations, whether they were *Call Chaining*, *New York Reach Around*, re-programming of Trump multiplexers or the phone company's mirror multiplexers, or just plain wiretapping will come to light. Shadow warriors thrive with deception, false flags, parsing of words, equivocation and sometimes just plain lying. The light of public disclosure is the mortal sin of the intelligence community from which every possible ploy, deception, and double talk will be deployed to obscure, manipulate, and hide the real reality of the depth and breadth of abuses arising from slick manipulations of the Constitutional guarantees that are revered as the "rule of law" in the United States since 1789.

Assuming Congress decides to conduct a viable investigation rather than a bread and circus show investigation, political carnage can certainly be anticipated.

A Historical Pattern of Motive and Practice

The Church Committee report is replete with documentation of presidential political electronic surveillance operations conducted by intelligence agencies of the government originated by presidential mandate. Within that documented, historical tradition, one might begin with who might be unhappy with Mr. Trump being elected President and how far those persons would go to insure Trump would not be elected President.

President Richard Nixon's political tricks, political spying, and campaign sabotage was eventually unmasked. It was unmasked; however, after a consistent cover-up, laced with vehement denials from every entity involved (including denials from Mr. Cheney). It deserves mention that Hillary Clinton was involved in the Watergate

debacle. She was involved in trying to engage in dirty tricks and to subvert the investigation by leaking highly restricted information to reporters; an act that got her fired. [47]

Spies at Holmdel, Middleton and North Andover

AT&T had a special division called "AT&T Bell Laboratories" where they invented devices and technologies that would be deployed by the phone company both nationally and globally. There was a small group in Holmdel and Middleton, New Jersey which included the primary scientists tasked with designing fiber optic systems, fiber optic multiplexers, fiber optic switches, routers, and the integration of fiber optics into every element of the phone system that could be managed.

There was also a huge fiber optic multiplexer factory in North Andover, Massachusetts, that held part of a special lab for this sort of product design and research. While the primary research was performed in Holmdel and Middleton, the lab in North Andover provided a test bed so that engineers floated between these three facilities.

In Middleton, there was a curious portion of the research lab where the AT&T engineers working on the ECI programs laid out maps of undersea and transnational fiber optic cables. They also used test equipment to simulate traffic typical to the particular cables. By attaching this test equipment to this network; the AT&T or other companies' fiber optic multiplexers, as the case may be, they would invoke commands to reroute traffic to create and test the *New York Reach Around* affirming its viability. These scientists took the originally developed source code (computer program) used to control these devices, spliced in backdoors and other commands to allow routine version updates to propagate a series of backdoors into these multiplexers. Their work culminated in the DDM-2000, which was the pinnacle of their success.

There was a scientist in these AT&T Bell Laboratories facilities who formerly had been a spy for a foreign country who was recruited by the U.S. Government that placed him in Bell Labs. The government tasked him with developing backdoors and other means to subvert the privacy on AT&T products. His allegiance was to his CIA handlers, not AT&T Bell Labs. This episode was a successful domestic espionage program within the Specialized Collection Service or SCS (the NSA and CIA fusion entity, for just this sort of thing). [48]

---

[47] Zeifman, Jerry, "Hillary's Pursuit of Power"

[48] Aid, Matthew (September 21, 2012). "The Spies Next Door: The Top 10 Beltway Intel Centers Hiding in Plain Sight" and

He was not the only imbedded spy. There were many more, given the task of developing weaknesses in AT&T products that would allow exploitation by the CIA, NSA, and SCS.

Room 641A in San Francisco

In 2002, the National Security Agency "rented" A 24 by 48 foot space from AT&T. In 2003, the NSA built a special room into which they installed fiber optic devices to include routers, multiplexers, computers, and other equipment. This special room was actually deep inside the AT&T facility. The fiber optic cables in this building were rerouted to appear in this room where they were tapped and then passed out into the normal portion of the AT&T facility. There are over 30 similar rooms across the United States where major fiber optic cables are tapped with the knowledge, consent and cooperation of the various fiber optic operators like Verizon, SBC, AT&T and others. These "rooms" render a huge revenue stream for these companies.

In 2006, Mark Klein, an AT&T Technician, obtained documents from his work. Klein wrote down the configuration of these rooms' contents. Through the Electronic Frontier Foundation (EFF), Klein filed a class action lawsuit in which he exposed to the public Room 641A and the illicit eavesdropping taking place. The case was dismissed in 2011. Part of the ECI agreement allowing the installation of these systems and eavesdropping equipment contained a grant of immunity from civil suits for the cooperating companies. This provision was added to the contracts in 2001 and subsequent versions granting complete immunity for the entire program and involved companies.

San Francisco was of particular interest since it was a major west coast juncture for both domestic Internet traffic as well and telephone traffic. But, there are 12 other major junctures to include New York, Boston, Cambridge, Miami, New Jersey, Mississippi, Portland, and others.

ECI FAIRVIEW and BLARNEY

AT&T started to collaborate with the NSA to take part in unlawful eavesdropping on American citizens in 1984, shortly after (literally minutes) the court ordered division of what was AT&T took place that year. It is important to note that well prior to 9/11, the NSA was already eavesdropping on U.S. citizens using domestic communications networks of AT&T, MCI, Sprint, EDS, Qualcomm, IBM, Oracle, Verizon, Intel, Microsoft, Motorola, Q-West, Facebook, Google and others.

MCI Communication Corp (MCI) started to collaborate with NSA starting in 1983, and was fully online with the NSA, for covert domestic eavesdropping by late 1984. Later, this would become MCI WorldCom, and they would control the Tier 1 ISP UUNET, which provided the NSA with access to a very important domestic Internet

backbone network. It does bear mentioning that in 1999 and 2000, the then CEO, Bernard Ebbers, grew increasingly opposed to the NSA scooping up all of the Internet traffic flowing through MCI controlled networks, and suddenly thereafter, the U.S. government ripped into both MCI and Ebbers, eventually destroying both. MCI changed its name to *Worldcom* after Ebbers was ousted; eventually going to prison. With Ebbers imprisoned, the company returned to a new NSA eavesdropping ECI agreement. In 2002, it changed its name merely to MCI, which would later (2005) be absorbed into Verizon (who already had an ECI agreement in place with the NSA).

Due to the ECI relationship, the technicians for AT&T, Verizon and MCI had to possess a Top Secret security clearance to be able to access their own fiber, because they might "accidentally" discover the tap, or discover data being diverted out of the fiber optic multiplexers or beam splitters.

"ECI" means that the company is given a code name to conceal its involvement in illegal activities. For example, AT&T has a code name; MCI has a code name; Sprint has one, and so on. The ECI codename for AT&T is "FAIRVIEW" and also US-990; but pay attention to the US-990 SIGAD code, as it tends to indicate or index when a code and alias was initiated. US-990 dates from the day AT&T was broken up. On that date, each of the "baby bells" was given a different ECI codename and SIGAD code name in the same manner of that of AT&T.

The ECI BLARNEY was initiated on AT&T prior to the breakup. It refers to the 1977 and 1978 era fiber optic switches that serviced regions, but which also routed international calls to undersea cables. BLARNEY was the pre-AT&T break up network to pass undersea cables to the NSA. After the AT&T break-up, BLARNEY remained in place for FISA reasons; then a new ECI was created called FAIRVIEW for the newly-born AT&T that handles undersea fiber optics. But, BLARNEY was still the overall cable tapping program for FISA intercepts on AT&T until the Clinton Era CALEA program. Of course, by that time, MCI and Sprint were major carriers, and both were assigned their own ECI codenames for domestic facilities, with a different ECI codename for undersea fiber optics.

As each fiber optic company sought a new undersea cable-landing license from the FCC, they were required by the NSA to enter into a classified ECI contract for at least TWO access points for each undersea cable. The first access point had to be right at the optical multiplexer, which duplicated the optical pulse into the undersea cable; and then a second into a fiber optic cable that fed NSA gear. Then, another behind the multiplexer and the switching systems a second access point where the signals exited the cable station to enter the AT&T, Sprint, MCI, *et al.* backbones.

Alas, poor Yorick! I knew him, Horatio…

In this manner the NSA besides having access to all data entering or exiting the cable landing station from the United States (illegally), but also access to the cable as it left the United States. The reason for TWO access points is that data can be relayed from cable station to cable station without exiting the cable station other than to hop through the cable station and the data, in this case, never hits the backbone.

After the above sequence, the data is sent to a cable station via an ocean route that is routed from another cable station; but without accessing the network backbone. In each case it creates a "relay effect" where the cable stations are not "routing through" the station as normal traffic, but are going round-robin from station to station.

For example, someone in England can launch data out of London, to an undersea cable to Long Island, which bounces it undersea to New Jersey; and then undersea to Florida; and thence to Cuba without the packets ever entering the domestic backbones of the carriers. So, for the NSA to operate the most effective network access, they have to hit both the front side and the back side of the undersea cable stations. More specifically, they access the cable by means underwater and landing taps, or they siphon it up at one of the interconnecting sites.

Since there has been some resistance from the carriers from time to time, the NSA, operating through fake FBI search warrants issued under FISA, has had installed on domestic backbones a fiber optic tap on each side on the cable landing stations. These intercept points were only suitable when the 1983 to 2001 era carriers were "uncooperative" by asking 4th Amendment related questions. For example, look what happened to the President of MCI when he started pushing back the NSA after they overstepped his original permission to penetrate the networks he controlled.

There were FIVE companies who just after 9/11 were blackmailed by the Oversight Committee on Intelligence into cooperating with the NSA without ANY warrants being issued. AT&T is one, then MCI, SPRINT, Verizon, and so on.

The end result was the creation of 12 “Program Cable Stations” at major interconnection points, performed with the assistance of the respective companies; and then secondary tap points performed without the cooperation of the respective companies.

Of course, this was merely the junction point on the backbones. There were other programs to target 26 VOIP routing facilities in the United States, plus 16 submarine landing stations (with very impressive NSA listening posts nearby), and close to two dozen 4ESS and 5ESS switching station as of Spring 2005.

In addition, under the FAIRVIEW ECI agreement, AT&T built backdoors into all of the DDM products for the NSA (DDM means Digital Division Multiplexing), in a program which predated 9/11; dating back into the 1970’s.

Speaking of the 1970 – William Binney

In 1970, a technological genius by the name of William Binney graduated college and went to work for the NSA as a career intelligence officer. He started his NSA experience while in the Army from 1965 to 1969. After college he, joined the NSA directly. During the 30 years he was with the NSA, he rose from being a technical analyst to the position of Technical Director and Technical Leader.

After 9/11, many hundreds of career intelligence professionals were offended by the U.S. government initiating systems to spy on the general public, as well as being upset over programs of one sort being turned on the public rather than foreign national security adversaries. Mr. Binney resigned from the NSA as a form of protest after the organization implemented a massive totalitarian program against the U.S. public; a program that has been described elsewhere in this paper, and which offends the Constitution of the United States.

In 2007, the NSA and FBI confected a case against Mr. Binney as a means of harassing him into silence, unlawfully raided his home and stole computers disks and records. The FBI and NSA also targeted Thomas Drake (another NSA executive) in the same manner. The misconduct by the FBI and NSA was based on the fact that many intelligence professionals had filed complaints with the U.S. Department of Defense Office of the Inspector General, and what took place from 2007 to 2011 was against nothing less then whistleblower retaliation and an attempt to harass and intimidate him into silence.

Unbeknownst to the NSA, there was trouble brewing for the NSA a great deal of trouble, actually, and it was coming from the CIA, and about to explode NSA surveillance programs.

The Worst Nightmare of the NSA, And An Epic Disaster

Spies do not "just happen," but rather, something happens at some point where a person with trusted access, betrays the trusted access and becomes a spy by either stealing and sharing secret information; or by doing this as an agent of a foreign government.

The CIA hires a lot of people, and they like to go after fairly young people since it is easier to get them to fall in line behind policies. Also, their ethics are still malleable at that age. The agency does like college graduates; as they can be formed into intelligence officers. The CIA still needs a small army of people who never made it out of high school; or who made it out of high school; but never got through college. Quite a few career CIA officers have never even completed middle school; however, these individuals had other skills of abilities useful to the agency, so the CIA did not care about a higher level of education.

In 2006, the CIA recruited an unemployed security guard from a local college (essentially a mall cop) by the name of Edward Snowden and sent him to school for six months to become a computer technician. The former security guard was then assigned to a support role in Switzerland in March 2007. He resigned in February 2009 after working only three years for the CIA. He left to go to work for Dell Computer as a contract worker at NSA facilities; basically doing tech support on Dell systems in Japan.

Even though his background investigation revealed a history of fraud, the fact that the majority of his family worked for the government allowed him to gain a Top Secret security clearance (5-year), which he otherwise would not have been able to obtain at this point in his life.

While at Dell, he began downloading huge volumes of classified documents and smuggling them out of the NSA facility. From Dell he resigned and then took up a similar position with Booz Allen Hamilton as a systems administrator (essentially a very low position on the computer profession totem pole). He was assigned to an NSA listening post in Hawaii. While in Hawaii, he increased his volume of classified document theft and hording. After 15 months in Hawaii, he unleashed a huge trove of stolen documents to foreign newspapers, trying to drastically damage national security, while claiming he did so to stop illegal NSA eavesdropping.

His position in Hawaii, working for Booz-Allen-Hamilton as a contractor for the NSA required that his security clearance undergo a new background check, and the thumb-up on his background due to the security contractor who was being paid for these background checks, was merely "pencil whipping" the background, and not actually performing a legitimate background investigation. Thus, a person who had a pile of disqualifiers in his background investigation was able to improperly obtain a Top Secret security clearance, and in turn get into a high risk position, with access to Top Secret materials.

One of the problems with spies is that many of them become spies or rather "betrayers" because they feel powerless in their lives; and wish to have access to classified information merely to make themselves feel more important. When they disclose the secrets entrusted to them; it raises their self-image in the short term; that in and of itself is a major goal. If they are granted access to some sort of vice or tangible thing like hookers, cocaine, and hard cash; the internal rewards they experience is increased ever more.

The Wrinkle

These thefts detailed above spanned many years, involved multiple agencies, multiple contractors, and tens of thousands of classified documents. More likely the purloined documents range in the hundreds of thousands. Indeed, at one point the

U.S. government estimated the theft was in excess of 1.7 million files; including highly classified documents from the Australian, Canadian, New Zealand, and British governments.

There is a bit of a wrinkle in U.S. law that stated a document cannot be deemed classified if that document discloses unlawful activity of the government, or government employees. The trouble is, only a very miniscule number of the stolen documents fit the loophole of "illegal activities". Rather, the majority of what was stolen involves perfectly lawful activities against foreign entities (not on U.S. soil). The pages which do fall into this exclusion reveal mammoth illegal violations of the 4th Amendment.

This spy needed to stroke his ego by craving attention. To do so, he collected and hoarded classified computer files for years. In 2012, he began shopping for a journalist who would stroke his ego in exchange for a virtually endless stream of classified documents.

A congressional investigation into the spy noted that shortly after his initial recruitment as a CIA employee; he exhibited notable security risks; he did things that should cause his new employer to suspect his loyalties. As time went on, the Congressional investigative report reveals he repeatedly had disciplinary problems. Since he never really worked at one place for any length of time, the counter-intelligence machine was unable to garner sufficient materials to yank his security clearance.

In 2013, the flood of documents into the public eye started. For four years it has been an endless stream coupled with much ego stroking to get the spy to reveal increasingly juicer and juicer classified data; all while digging himself into a deeper and deeper hole.

At various times, he would claim he did it in retaliation for the NSA harassing William Binney. Other times, he would claim he did it because the head of the NSA lied to Congress. Ultimately his conduct was all about getting his ego stroked for a few years.

Nevertheless, the documents disclosed by him do provide a partial insight into the global scale of the NSA operations. Of the greatest interest in the documents is the details of how the NSA, CIA, and SCS set up unlawful eavesdropping programs right after 9/11 in order to target NSA surveillance against U.S. citizens; or rather, anyone and everyone who was on U.S. soil.

The conundrum evolved into two possible choices: 1) should the country be upset with the spy who spilled the secrets; or 2) should citizens be livid with their government who went well beyond the limits set down in the Constitution by spying on everyone.

Either way, there is now highly classified and ECI documentation in public circulation that the NSA has a massive eavesdropping operation going inside the United States which targets the entire U.S. population (with no warrant). Given that in the past the NSA has been proven to conduct illegal bugging, wiretapping and eavesdropping during political campaigns by the sitting President; it is not unreasonable to maintain the premise that President Obama did so during the 2016 election; just like has been proven he did in the 2012 Presidential election.

NSA Regional Data Centers

The NSA operates a number of massive facilities that provide a massive data center at each location. Each is connected to all of their other data centers. In combination the result is an utterly astronomical capability which siphons up every phone call, every Netflix account, every Facebook post, every browser click, and every E-Mail of every single American in real time. While crunching this data, NSA also gobbles everything from international fiber optic taps, manipulated fiber optic multiplexers, fiber splitters/bam splitters, bank computers, cute cat videos, and the most intimate of details of every U.S. citizen; all contrary to the Bill of Rights.

These Data Centers exist in many venues; like the one near Atlanta, Georgia; Salt Lake, Utah; Hawaii, Texas or under several mountains, or right at Ft. Meade, and dozens of other US locations and in foreign countries. All of these locations are interconnected to create the largest storage facility of computer-based information in the world.

Let's Talk About Cloud Computing

A "cloud" is an interconnected series of geographically separate computer servers that when viewed from the outside world appears to be merely one giant computer with a virtually unlimited about of online storage. In fact, they tend to be huge buildings with hundreds of thousands of really cheap disposable computers, an array of really cheap hard drives, and really cheap memory.

The key is to only use cheap computers, and to conceal the flaws and vulnerabilities of the use of cheap computers and hard drives to create an illusion of reliability, and this is done by predicting outages, and by having automatic cross over to redundant systems so the customer never sees the chaos of a massive server crash or hard drive array outage.

Internet Clouds are created by constructing huge buildings with an abundance of electrical power with the ability to remove the loads of generated thermal heat in order to keep the servers at a stable temperature. Really progressive companies have racks of servers delivered to them in prebuilt international shipping containers which they can buy or lease as needed.

Cloud providers need to build in a tremendous amount of excess storage space. These providers assist their budgets by selling storage space to various governmental entities as cloud storage which can be drastically cheaper than local storage. Granted cloud storage is not needed for anything less than 64 terabytes of data; however, when one single data set can run into the petabyte level or larger; then cloud computing service start to become very attractive. While this sort of arrangement also facilitates wide scale collection; it also concentrates considerable risk of spies spying on the spies. This spying upon spies is a process that circles around itself into an ever tightening spiral.

Amazon Web Services, and Front Companies

It is a little known fact that Amazon obtains profits through a host of front companies which host pornographic websites. Amazon also makes a small fortune hosting data for the NSA and CIA. Although Amazon and the NSA go to some astounding efforts to conceal this; it is a matter of public record and generates tens of million of dollars.

Amazon provides part of the NSA/CIA cloud so that illicitly captured phone calls can be hidden next to hard-core pornography; light bulbs, bibles and things people spend their disposable income on. It is not a bad business model, other than for the significant ethically questionable activities for which heir servers are sometimes used.

For example, a front company will show up in the GSA logs that is reselling Amazon Web Service to the Patent office, but only a small sliver of that contract is actually the PTO. A rather large pool of various front companies is used to build up a vast segment of AWS bandwidth and server space for NSA intercepts against U.S. Citizens. If anyone sues Amazon for any of this; Amazon will invoke the ECI immunity just as was done by AT&T when they got sued over the eavesdropping rooms in San Francisco.

What is an NSA Regional Signals Operations Center – RSOC?

A National Security Agency (NSA) Regional Signals Operations Center (RSOC) is a location where multiple eavesdropping and hacking efforts are undertaken and overlapped. The RSOC siphons all the collected intelligence for a region and injects it into the various NSA Broadband circuits, usually being fiber optics.

For example on the Island of Oahu in the Hawaiian Islands there is a mammoth underground facility where the NSA fiber optic tapping point resides on Ka'ena Point, along with the NSA satellite dish facilities nearby funnel into the Kunia RSOC.

This is all injected into the NSA fiber optic cable and circulated to all other RSOC's and analysis centers.

An RSOC essentially sits in the middle of a geographic collection point, which in the case of Kunai, is the satellite dishes and fiber at Ka'ena Point arriving from Asia. On the topic of satellites, there are several families of NSA eavesdropping satellites with code names of: ONYX, TOPAZ, RAVEN, ORION, NEMESIS, CRYSTAL, INTRUDER, QUASAR; all of which feed into this massive NSA fiber optic network by way of these and other satellite dishes.

The various RSOC's all over the globe are the key to the collecting intelligence abroad and funneling the collected intelligence back to the NSA for exploitation. The only wrinkle is that there are numerous RSOC's inside the United States that focus their technology on U.S. Citizens engaged in communications with other U.S. Citizens, in contravention to the 4th and 14th Amendment.

Technically, there is only two legal means by which the intelligence agencies can eavesdrop. One is under FISA and the other is under Executive Order 12333 (or the classified annex to Executive Order 12333). But, that assumes the eavesdropping is actually legal. Historically, documentation has been uncovered that the NSA and other intelligence agencies routinely violate these legal means and step well outside the 4th Amendment and spy on U.S. citizens with impunity for political gain or political power (or in some cases, just for sexual voyeurism). [49]

When questioned by Congress, NSA or whatever intelligence agency is on the "hot seat", each will pronounce how ethical the agency is detailing at great lengths the agency's tremendous effort NOT TO eavesdrop on U.S. citizens. The heads of all of the U.S. intelligence agencies have the same shtick and the same song and dance routine when questioned under oath on this sort of matter. Whenever it is suggested they have offered false testimony under oath supported by documents showing same, a new chapter begins in which testimony claims they never knew, were never briefed, or never had any involvement in such things, and so on. Eventually, sacrifices of some low-end staffers are thrown on the coals as sacrifice to end the inquiry. At the end of the day, the actual architects and management return to their mahogany paneled office to take more requests to continue the daily routine of eavesdropping.

Under Executive Order 12333, the NSA gains access to any fiber optic cable that enters or leaves the United States, through a device called a *fiber splitter* installed at the phone company fiber optic appearance point. This *splitter* can be in the central office; at a transmission plant; at the manhole where the fiber optic cable first hits

[49] http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo 27 February 2014

land; or, in some cases, underwater as a glass to glass fusion splice; or a splice right at the underwater repeaters.

Conclusions

1) Historically, incumbent Presidents order espionage (to include eavesdropping) against the candidate of the party that opposes them.
2) This election linked espionage may include illegal eavesdropping from one political party against the other party, or it may involve espionage inside the respective parties.
3) Historically, the NSA has been used for this sort of eavesdropping, but other agencies may be involved as well.
4) It would have been astoundingly unusual for President Obama not to order the eavesdropping of Candidate Trump, or Candidate Sanders.
5) The NSA has a partnership agreement with the intelligence services of four other nations, to include the British GCHQ through the Five Eyes partnership.
6) By performing a "Reach Around" the NSA can provide GCHQ with access to the private communications of a Presidential candidate, so that GCHQ writes up the information contained in the intercept, which GCHQ then leaks through various deniable sources to the media in order to control U.S. elections.
7) President Trump has a legitimate claim that the NSA eavesdropped on him during the Presidential campaign of 2016.
8) President Trump has a legitimate claim that the NSA routed signals out of Trump Tower to GCHQ, who were an integral mechanism to attempt to manipulate the U.S. Elections.
9) President Trump claims that President Obama had his wires tapped are legitimate, credible, and viable.
10) It is highly probable that President Obama did in fact violated the Fourth Amendment and attempted to sabotage the Presidential Campaign of Donald Trump by using the NSA and its various eavesdropping programs.

About the Authors

James M. Atkinson

Mr. Atkinson is the industry leader in Bug Sweeps, Wiretap Detection, Detection of Covert Video Cameras, Detection of Covert Microphones, and related inspections, TSCM, TEMPEST, NONSTOP, Emissions Security (EMSEC), Signals Intelligence and related fields. He has forty years of hands-on experience on a wide range of computer systems, involving multiple generations of technology, including huge, highly secure, and highly classified mainframe systems, to modern desktop, laptop, and handheld computers. Well experienced in the design and development,

prototyping, and production of specialized electronic devices and instrumentation. He is also a skilled photographer, computer programmer and artist.

He is a recognized expert technical, analytical and research for the detection, nullification, and isolation of eavesdropping devices, technical surveillance penetrations, technical surveillance hazards, and physical security weaknesses. Mr. Atkinson is highly skilled in intelligence Analysis and activities to determine the existence and capability of surveillance equipment being used against the governments, corporations, establishments, or persons. He is also formally trained in technical, forensic skills to include computer forensics, network forensics, hard drive forensics, Wi-Fi forensics, WAN forensics, and cell phone forensics. He has testified as an expert witness is numerous courts, and has been called to testify before Congress three times as an expert witness. Mr. Atkinson is considered to be the "Leonardo da Vinci of Bug Sweeps."

Mr. Atkinson may be reached by E-mail at jmatk@tscm.com, or by phone at (978) 381-9111. His website about technical counterintelligence can be found at: http://www.tscm.com/

Stan Spring

Stan Spring is an active member of the Association of Former Intelligence Officers, former TSCM operator, instructor and litigator. Presently he is active as a screenwriter, actor, film producer and director living in Baton Rouge, Louisiana.