Surveillance? – What Surveillance? Part 1 of 2

NATIONAL SECURITY AGENCY UTAH DATA CENTER

“Mass surveillance is different. If you’re truly worried about attacks coming from anyone anywhere,
you need to spy on everyone everywhere.”
-Data and Goliath p.90

Do you have any idea what these Sons of Sea Biscuits have been doing to you – to me – to all of us these past bunch of years? Well, I’m going to lay part of it out for you, hopefully in technicolor and wide screen.

Our NSA (National Security Agency) does not have an open and transparent history. The NSA was created in secret in 1952 not by Congress, but by a pen stroke of Harry Truman in a 7-page document that remained classified for years. Even its name was undisclosed.

And it stayed hidden until finally, in 1971, NSA analyst Perry Fellwock blew the whistle on NSA and their secret program **Echelon** with its vast information gathering technology even back then. This led to the Church Committee hearings and some legislation. *Obviously, it wasn’t enough…..*

WHISTLEBLOWERS

Over the recent years, 6 additional patriotic whistleblowers have come forward at great sacrifice and risk to themselves.

These include Bill Binney, Edward Snowden, Russ Tice, Mark Kline, Thomas Tamm, and Thomas Drake. Click the above link for more information on these men.

NSA TODAY

Bigger: See Wired article from 2012. Written by James Bamford, this is an article that spares no one's feelings in laying out what the NSA is, and does.

Bigger and Nastier: "The NSA is more interested in the so-called invisible web, also known as the deep web or deepnet – data beyond the reach of the public. This includes password-protected data, US and foreign government communications, and noncommercial file-sharing between trusted peers. 'The deep web contains government reports, databases, and other sources of information of high value to DOD and the intelligence community according to a 2010 report.'" -(Quote from the Wired article.)

But don't feel left out. Oh No! They *already have* every keystroke, every conversation, every search (Yes, even *those*), every credit card purchase, every check, every rewards card purchase, every toll gate, every bill, every-everything about you. ***What do you think is filling up those monstrous computers?***

The next two blue links are enlightening wakeup articles from Bruce Schneier. Bruce is a go-to guy on internet security, and author of Data and Goliath, about collecting your data and controlling the world. It was a best selling Amazon Book of the Year in 2015.

The **Utah Data Center** came online in 2014, at a cost of somewhere between one and one-half to two billion dollars for one million-plus square feet. Details are not readily shared with the public.

100,000 square feet will be for data storage. The remaining

900,000 square feet will be for administration and ***"technical support"*****……** ? What, *exactly*, does that mean in spook-talk? Data Mining? More secret programs? Mind Control with DOD's DARPA (Defense Advanced Research Projects Agency)?

It is widely believed that a *large* emphasis at the Utah Data Center will be put on cracking encryption. You know, breaking the private codes. This will done in conjunction with their Oakridge, Tennessee facility which is developing the world's fastest supercomputer.

Currently encryption done at 128 bits, and 192 bits, and most securely at 256 bits has them at bay. But between the vast storage data in Utah and the lightning speed in Tennessee they think they may be able to crack them. *Would it be okay to pray for a large magnetic storm?*

And they're building *another* data center in Fort Meade, Maryland that will be two and one-half times bigger. *Just what are they going to do there?*

Here Are A Handful of the Programs…

ECHELON

Reportedly developed to monitor Russia and the Eastern Bloc, this one has been around since about 1966. "ECHELON was part of an umbrella program codenamed FROSTING, which was established by the NSA in 1966 to collect and process data from communications satellites. FROSTING had two sub-programs:[25]

- TRANSIENT: for intercepting Soviet satellite transmissions, and
  • ECHELON: for intercepting Intelsat satellite transmissions."
  From Wikipedia.

This 1999 article brought more information to the fore.

Echelon's focus is international intercepts. Shrouded in secrecy, Echelon uses large golf-ball shaped facilities (called radomes short for radar-domes which protect delicate radar equipment from the climate) on earth, plus satellites, to listen in on, intercept, and copy any and all transmissions. Echelon includes sites in England (RAF Menwith Hill), Australia, New Zealand, Japan, and others. The satellites used are said to be stationary.

Several years back (+/- the year2000) there was an international flapdoodle as allegations flew that U.S. companies were getting insider information based on intercepted commercial bids, and using them to secure lucrative contracts. This, while believed to be true, was of course denied.

CARNIVORE

This was an earlier FBI e-mail wiretap system that could be set up by the FBI, in conjunction with your ISP (Internet Service Provider), and operated remotely. It was newer technology in the year 2000, unregulated (if you just forget the Fourth Amendment), and extremely prone to *overreach without oversight.*

Carnivore was eventually renamed DCS1000 but that didn't improve its murky reputation nor lessen the FBI's secrecy surrounding the eavesdropping which many believed expanded to intercepting and copying *all* e-mails. *Are we singing Kumbaya yet?*

SNIFFER

This isn't a program but rather a means of creating surveillance. Routers direct internet traffic noting destinations of the "packets" that go through the router. "Packets" are parts of transmissions that have been reduced into smaller parts to make transmissions flow more efficiently.

A sniffer is an intercept monitor that can copy either limited, specific targets, or copy any and every thing that passes by.

HEARTBLEED

This was created through a flaw discovered in an update to the the SSL program. SSL stands for Secure Sockets Layer. SSL has been supplanted by TLS, Transport Layer Security. However, SSL is still widely used.

The SSL is used for security in roughly 2/3 of "secure" Net transactions (think credit card purchases on secured sites). This Heartbleed bug allowed the NSA easier access to our passwords and personal information. The NSA claims it did not know of the Heartbleed bug until 2014. Sources say the NSA knew at least two years earlier. *You think?*

TRAPWIRE

TrapWire is a shadowy overreaching program originated by a corporation known as Abraxos, in Virginia. Abraxos is filled with ex-CIA, ex-Intelligence Community spooks. Its purpose is to film people and study patterns of behavior, pre-assign likely guilt, and call it terror assessment. *Talk about guilty until proven innocent!*

In 2005 an Abraxos officer stated that TrapWire could "collect information about people and vehicles that is more accurate than facial recognition, draw patterns, and do threat assessments of areas that may be under observation from terrorists." TrapWire was exposed in 2012 when a researcher went through a series of hacked e-mails from a company known as Stratfor, aka "Shadow CIA".

It was revealed at that time that literally *millions* of cameras – public, red light, traffic, bridge, commercial, casino, U.S. *and* international – were digitally recording people, encrypting the data, and sending it to places unknown

for storage using face recognition to note **“persons of interest”** in **“Suspicious Activity Surveillance”.**

TEMPEST

This is a program used by the government to reconstruct information data streams by capturing electromagnetic radiation from computers, printers, handheld devices and converting these radiations into their original transmissions. *Unbelievable. Just unbelievable.*

PRISM

Created under George W Bush, PRISM is a secretive tool that co-opts the biggest internet service providers. These include **Google, Microsoft, Apple, Yahoo, Skype (now owned by Microsoft), Facebook, PalTalk, AOL, and YouTube**. It is believed information can be gleaned from the user equipment via back doors; from the internet backbone; or from the corporate cloud database. This may include general data and/or verbatim copies.

- Prism slides released by Edward Snowden. How we learned of PRISM.
- 2013 – 2014 leaks from Edward Snowden. The leaks he provided.

XKEYSTROKE

This is a very developed query program. You can search, or query, using MAC or Microsoft Office or pdf or phone number or e-mail address or type of document or extensions, and more. This classified link is from 2008 – *“The Unofficial XKS User Guide”.*

TEMPORA

This is a British program shared with NSA that collects – for later sorting – internet information carried on fiber optic cables. It went operational in 2011. The cable companies are

aware. I believe all the major cables are now tapped. This matters because much of the international cable traffic flows through the US.

SPECIAL SOURCE OPERATIONS (of the NSA)

This is the division of NSA that collects data from telephone and cable sources. These commercial companies have been coerced (?) into being willing partners with NSA. It is loudly rumored that these companies – *your carriers* – are well paid for their cooperation. (*Are you surprised?*)

Back in the day that worked just fine; they cooperated and no one was the wiser. Then in 2013 Edward Snowden happened and the big Verizon-NSA link became front page news.

Well, it's still going on and all the major companies are in on it.

"SSO also cooperates with private telecommunication providers under the following **four programs**, which are collectively referred to as
Upstream Collection:

– BLARNEY (collection under FISA authority, since 1978)
– FAIRVIEW (cooperation with AT&T, since 1985)
– STORMBREW (cooperation with Verizon, since 2001)
– OAKSTAR (cooperation with 7 other telecoms, since 2004)"
from Wikipedia

"The government does not need to know more about what we are doing. We need to know more about what the government is doing. We need to turn the cameras on the police and on the government, not the other way around." -Ron Paul June 14, 2013

We'll continue in PART TWO with everyday surveillance that is all around us. The scope is breathtaking, and growing.

Part two coming soon.