A Chronology

How Obama Expanded and Consolidated The Bush-Cheney Domestic Spy Dragnet

by Edward Spannaus

What follow are some of the known critical nodal points in the process of the consolidation of the dragnet surveillance and data-mining program over the post-Franklin Roosevelt years; much more is still unknown and hidden behind classification barriers.

1940s: The British-U.S. Arrangement

1943: The U.S. and Britain formalize wartime signals intelligence cooperation, with the **BRUSA** (Britain-USA) agreement, providing for sharing of information.

1945: **Operation SHAMROCK** is inaugurated, a program under which the three largest U.S. cable companies—Western Union, ITT World Communications, and RCA Global—provided to the **National Security Agency** (the U.S. military's signals intelligence agency), and its predecessors, copies of all cable traffic entering and leaving the United States. Western Union and ITT gave the NSA microfilms of cable messages; RCA provided NSA with complete copies of all cables, and later, magnetic tapes, when its operations were computerized.

1947: Britain and the United States signed the **U.K.-U.S.A. Security Agreement,** also known as "UKUSA," or the "Secret Treaty." This represented President Harry Truman's treasonous policy of establishing an Anglo-American "special relationship"—a repudiation of FDR's policy. With a year, the other signatories—Canada, Australia, and New Zealand—had joined. Subsequent agreements provided for standardized codewords, security agreements, and procedures for dissemination of information. The two principal agencies involved are the U.S. NSA and Britain's Government Communications Headquarters (GCHQ) at Cheltenham.

All of the above arrangements continued and expanded throughout the 1950s, and up to the present day.

1960s: NSA Operations Expand

In the early 1960s, the U.S. Justice Department and FBI started providing the NSA with names of Americans whom the FBI believed to be involved in certain domestic criminal and political activities, so that NSA could expand its "watch list." In 1967, **Maj. Gen. William Yarborough,** the Army's Assistant Chief of Staff for Intelligence, requested information pertaining to civil disturbances, and during the late 1960s into the mid-1970s, the Army, CIA, FBI, and DIA all were sending requests for intercept intelligence to the NSA, the subjects of which included domestic anti-war and civil rights activists, including Dr. Martin Luther King.

In 1969, the domestic surveillance program was formalized under the code name **MINARET,** pertaining to, *inter alia,* "individuals who may foment civil disturbance or otherwise undermine the national security of the United States." British Intelligence's GCHQ Cheltenham also provided intercepts to the NSA which were then passed on to other U.S. intelligence agencies.

1970s: Military Spying Exposed

1971: Congress began investigating military spying on U.S. citizens.

1972-74: the **"Watergate"** scandals exposed Nix-

on's use of domestic intelligence agencies and the IRS to surveil and target his political enemies.

In 1972, the U.S. Supreme Court, in the landmark case *U.S. v. U.S. District Court*, held that the President's Executive Powers cannot override the Fourth Amendment's requirement for a warrant, in a case involving domestic electronic surveillance.

In August 1975, the House Select Committee on Intelligence Activities, headed by **Rep. Otis Pike** (D-N.Y.), held hearings on NSA domestic surveillance, in the course of which CIA Director William Colby disclosed NSA's interception of international communications, and during which NSA Director Lt. Gen. Lew Allen testified in an open hearing for the first time.

In October 1975, the Senate Select Committee on Intelligence Activities—known as the **"Church Committee"** for its chairman, **Sen. Frank Church** (D-Id.)—publicly identified the SHAMROCK AND MINARET programs by name for the first time.

U.S. Navy/Johnny Bivera

Dick Cheney's drive for dictatorship goes back to the 1980s when, as a Congressman, he commissioned a report stating that Congress may not infringe on Executive power, in matters of war and national security.

Church opened the hearing on Oct. 29, 1975 by stating that "Just as the NSA is one of the largest and least known of the intelligence agencies, it is also the most reticent. While it sweeps in messages from around the world, it gives out precious little information about itself.... Today, we will bring the agency from behind closed doors." On Nov. 6, 1975, the Church Committee made public its report on SHAMROCK.

After the release of the Committee's Final Report in 1976, Senator Church warned that tyranny would result if the NSA "were to turn its awesome technology against domestic telecommunications." Were this to happen, Church warned, "That is the abyss from which there is no return."

1978: In response to the Church and Pike Committees' findings of abuse, including widespread violations of the Fourth Amendment's prohibition against unreasonable searches and seizures, Congress passed the **Foreign Intelligence Surveillance Act (FISA),** which confirmed, once and for all, that the Fourth Amendment does apply to domestic electronic surveillance. FISA required a particularized showing of probable cause before an individual in the U.S. could be subject to electronic surveillance, or his records seized, in a foreign intelligence or national security case.

1980s: Cheney Rejects Controls

Rep. **Dick Cheney,** the senior Republican on the Joint Congressional **Iran-Contra Committee,** commissioned a "Minority Report," written largely by his aide and future legal counsel **David Addington,** proclaiming that Congress has no power to infringe on Executive power in matters of war and national security. It was well-known that Cheney never accepted the findings of the Church Committee, and looked for any and every opportunity to repudiate them.

When Cheney became Secretary of Defense (1989-93), and later Vice President (2001-09), he had his chance to put these views into action.

1990s: Emergence of Data-Mining

In the late 1990s, the U.S. Army's **Intelligence and Security Command (INSCOM)**, in conjunction with the **Defense Intelligence Agency (DIA)** and other agencies, developed a data-mining program using "link analysis" also known as "associational analysis," for use in terrorism investigations and other matters, such as technology transfers and espionage related to China. This program became known generically as **"Able Danger"**—although Able Danger was reportedly a narrower program, feeding "actionable" intelligence into the military's **Special Operations Command (SOCOM)** for hunting down and killing terrorist suspects.

In early 2000, the data-mining program was shut down by the Pentagon, because it had been retaining

information on U.S. citizens. However, according to various reports, SOCOM simply relocated the program to a private contractor where it continued.

EIRNS/Stuart Lewis

The Total Information Awareness (TIA) Office, created in 2002 by Adm. John Poindexter (of Iran-Contra infamy) established a massive data-mine, collecting bank, credit card, telephone, and travel records, etc.

9/11 and Its Aftermath

2001: **The Patriot Act-Plus**. Shortly after the Bush-Cheney Administration took office in early 2001, it began approaching the top telecommunications companies, seeking NSA access to their customer records. Dick Cheney personally sought the participation of Qwest Communications in the program, but Qwest refused, after finding out that the NSA had no warrant from the FISA Court or any other legal authority to obtain such records.

On Oct. 4, less than four weeks after the Sept. 11 attacks, President George W. Bush signed an order authorizing the NSA's domestic wiretapping program, which went operational on Oct. 6. Quickly, the NSA made new approaches to the telecommunications companies, seeking access to all their traffic. These included the three largest: **AT&T, Verizon, and BellSouth.** The legal justification was cooked up by Cheney's lawyer David Addington and second-rank Justice Department attorney **John Yoo,** bypassing normal channels. It is thought that these still-secret legal opinions reflected Cheney's longstanding dogma that the President's war powers, under Article II of the Constitution, override any legislative restrictions such as FISA.

On Oct. 23, **Rep. James Sensenbrenner** introduced the USA Patriot Act, junking a previous bi-partisan bill. The bill was rapidly passed by the House and Senate, over heavy Democratic opposition, and was signed into law by President Bush on Oct. 26. Among its most notorious provisions are those allowing the FBI to obtain records without a court order or a subpoena, through the use of National Security Letters, and its Section 215, which allows the FBI and others agencies to obtain records and other materials through secret warrants issued by the FISA Court.

2002: Secret Presidential Order

A secret Presidential order authorized the NSA to conduct domestic surveillance, overturning 25 years of law and regulations. Congressional leaders were summoned to Cheney's office for a secret briefing on the program. This was what is known as a "special access program," so sensitive that relatively few people even know about it. According to some sources, the program was code-named **"Stellar Wind."**

In a parallel development, the Defense Department's **Defense Advanced Research Projects Agency (DARPA)** created the Information Awareness Office, also known as the **Total (or Terrorist) Information Awareness (TIA)** Office, a data-mining program run by **Adm. John Poindexter,** best known for his role in the Iran-Contra affair. The idea of TIA was to create a huge, centralized database consisting of government and commercial records, including bank records, credit card and telephone bills, travel records, and so on, and then to look for "suspicious" associations and patterns.

In the Summer of 2002, AT&T technician Mark Klein learned of secret rooms being constructed at two AT&T switching facilities in San Francisco, from which the NSA tapped into fiber-optic cables connecting AT&T's WorldNet service to other Internet providers. Klein thought the arrangement was part of TIA. Only persons with an NSA security clearance were allowed to enter the secret room. Similar NSA secret rooms were being built in other AT&T facilities around the country.

2003: Under Congressional Pressure, a Shift

After a public uproar, Congress pretended to shut down the TIA program, but in fact, the program was

shifted into the Pentagon's classified ("black") budget, and continued to operate within the NSA, and under the auspices of DOD contractors such as **SAIC** and **Booz Allen Hamilton.** In 2002, former NSA Director **Mike McConnell,** then heading Booz Allen's intelligence division, wanted Poindexter to give the entire TIA program to Booz Allen, but Poindexter was reportedly reluctant to give one firm so much control over it, so Booz Allen got part of it, as did other private contractors, where the TIA program carried on—as it continues to do up to the present. The unprecedented amount of data which the NSA collects today, sweeping up all telephone and Internet traffic, is useless unless the agency has the means to mine through it and analyze it—and that's what Poindexter's TIA and its offshoots were designed to do.

DOJ

In March 2004, Attorney General John Ashcroft, then ill and sedated in hospital, was accosted by Cheney-directed White House lawyers demanding that Ashcroft recertify the NSA surveillance program.

(Former NSA Director Michael Hayden told the *National Journal* on June 10, 2013, that the NSA's massive data-collection and surveillance system was developed by, and is almost entirely run by, private defense contractors. According to author and NSA expert **James Bamford,** these contractors include at least two Israeli firms: Narus, which processes the information obtained from AT&T for the NSA, and Verint, which does the same for Verizon data.)

On July 17, 2003, **Sen. Jay Rockefeller** (D-W.Va.) the senior Democrat on the Senate Intelligence Committee, was so alarmed by a secret White House briefing on the NSA program, that he sent a private, handwritten letter to Cheney, expressing his concerns over the surveillance program, and saying it reminded him of Poindexter's TIA program. Neither Cheney nor anyone else ever answered Rockefeller's letter.

2004: An Open Battle

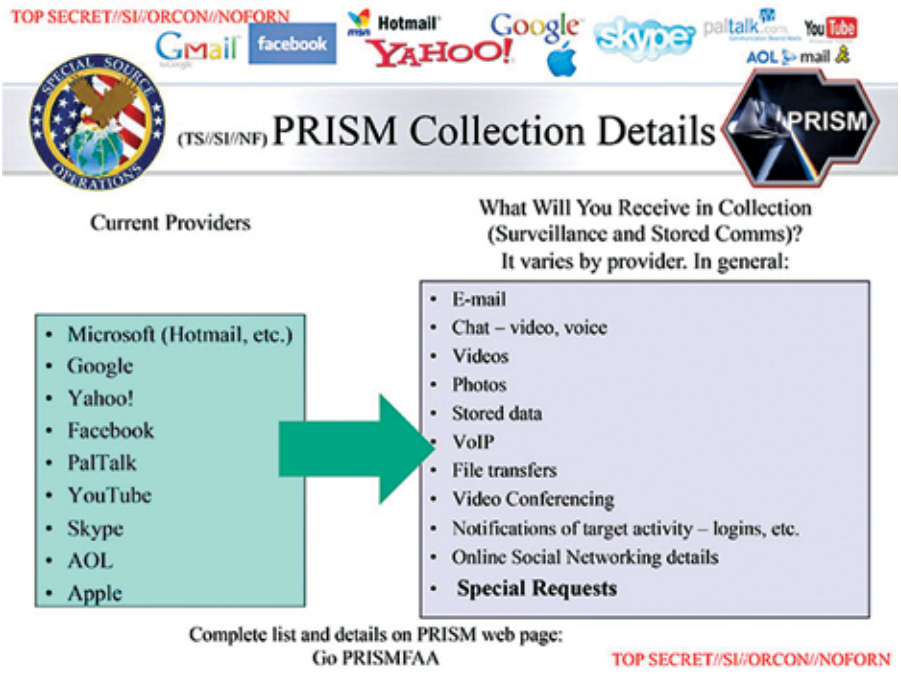
By March 2004, Justice Department lawyers were becoming so concerned about the legality of the NSA surveillance program that they were considering refusing to re-certify it. The new Deputy Attorney General, **James Comey**, told Attorney General **John Ashcroft** that the program might be illegal. The Justice Department's balking over recertification led to the dramatic confrontation in Ashcroft's hospital room on March 10, where White House lawyers, acting at the direction of Cheney, attempted to get an ill and sedated Ashcroft to reauthorize the program, but were blocked by Comey and FBI Director **Robert Mueller.** When the White House reauthorized the program the next day, without DOJ approval, Comey, Ashcroft, and all the top DOJ leadership threatened to resign *en masse* unless the program was changed.

Apparently overriding Cheney, Bush agreed to some modifications. There are many indications that Comey's concern was not just with the publicly acknowledged Terrorist Surveillance Program, but with a much broader NSA program—probably Stellar Wind, the dragnet sweep of all telecommunications. Administration officials have said in public testimony that there are other, secret programs which they cannot discuss in open hearings.

2005: More Exposure

In a series of articles in December 2005, the *New York Times* exposed the Bush Administration's surveillance and eavesdropping on U.S. citizens without a court order. The warrantless surveillance program, operating since 2002, represented a sharp break with the previous practice of obtaining FISA Court war-

rants for any domestic spying. The *Times* reported how the NSA had obtained access to the communications streams of the major telecommunications companies.



The "Protect America Act of 2007" allowed the FISA Court to issue blanket authorizations, rather than individual warrants, for surveillance, thus overturning the 4th Amendment.

2006: More Uproar

As the uproar over the warrantless wiretap program continued, the *Washington Post* reported that the NSA was sharing this information with the FBI, CIA, the Department of Homeland Security, and other military agencies. *USA Today* named the private telecommunication companies involved.

In February, a long-time NSA employee, Russell Tice, told a House Government Reform subcommittee that he was concerned about the legality and constitutionality of another "special access" program being conducted by the NSA. Tice said this program was different and more far-reaching that the one disclosed by the *New York Times*, but he said he could not discuss it because of its highly classified nature.

2007: FISA Court Gets Right To Violate 4th Amendment

In January 2007, the Bush Administration announced that, henceforth, the FISA Court would authorize any surveillance previously conducted under the President's Terrorist Surveillance Program. If this were true, it constituted a narrowing of the program.

But, in August, Congress passed the **"Protect America Act of 2007,"** which expanded Executive power to conduct international surveillance, and allowed the FISA Court, for the first time, to issue blanket authorizations rather than individualized warrants—thus completely obliterating the protections provided by the Fourth Amendment. It also eliminated the previous requirement to show that a target was an agent of a foreign power; now the collection simply had to be related to foreign intelligence gathering. It legalized the ongoing NSA tapping into telecommunication facilities.

Within a month, the Bush Administration obtained access to **Microsoft's** Internet traffic, under the newly launched **PRISM** program.

2008: Obama Weighs in for Spying

In July, then-Sen. Barack Obama reversed his previous stance, and voted for the FISA Amendments Act of 2008, which made most of the 2007 "Protect America Act" permanent, and which also gave retroactive immunity to the telecommunications companies which had been handing over customer records and data to the FBI and other agencies through the NSA.

2009: Obama Protects Warrantless Wiretapping

At the beginning of January, Federal courts started dismissing civil suits that had been brought against telecommunications companies, citing their immunity under the 2008 law.

In April 2009, the Obama Administration moved to have another civil suit thrown out of court, on the grounds that any litigation over the Bush Administration's warrantless wiretapping program would require the government to disclose "state secrets." The Administration aggressively invoked "state secrets" in other

Wikimedia Commons

The NSA's new $2 billion data storage and analysis center in Bluffdale, Utah, shown here under construction in April 2013.

cases to defend the NSA surveillance program, and fought for the broadest immunity for telecommunications providers.

2010: Still Sharing with the British

By 2010, and probably before, the British GCHQ was given access to PRISM's sweep of Internet traffic, enabling British Intelligence to circumvent British law. Between June 2010 and May 2012, GCHQ generated 197 intelligence reports for MI5 and MI6, according to the June 7 *Guardian*. (It has been reliably reported that, for decades, U.S. and British intelligence used each other to spy on their own citizens, thus circumventing their own country's prohibitions against domestic surveillance.)

2011: Extending the Patriot Act

On Jan. 6, 2011, NSA officials and others broke ground for the construction of the NSA's new $2 billion data storage and analysis center in Bluffdale, Utah.

In the Spring, with key parts of the Patriot Act up for renewal, President Obama demanded a longer extension of the law (until December 2013), than did the Republicans (who wanted it extended only to the end of 2011). Obama's White House claimed that this was needed to provide "certainty and predictability" to the intelligence agencies. In May, Obama signed the bill which extended key provisions of the Patriot Act—including Section 215—until 2015.

2012: Massive Expansion of Surveillance

In April, the *New York Times* reported that the NSA was still engaged in intercepting purely domestic communications, beyond the limits set by Congress.

That same month, NSA whistleblower William Binney said that surveillance had increased under Obama, and that the NSA's data-mining program has become so vast that the government has assembled *20 trillion* transactions of U.S. citizens with other U.S. citizens, including phone calls, e-mails, credit card purchases, and Internet searches.

In June, at the insistence of Obama and the intelligence agencies, Congress passed a five-year extension of the 2008 FISA Amendments Act. Senators **Ron Wyden and Mark Udall** warned of "a loophole in the law that could allow the government to effectively conduct warrantless searches for Americans' communications" (see Wyden's remarks, previous article).

2013: The Latest Revelations

On June 5-6, the London *Guardian* revealed a secret FISA Court order requiring Verizon to turn over all customer records to the NSA on a daily basis. "The unlimited nature of the records being handed over to the NSA is extremely unusual," the *Guardian* reported, and also cited the "numerous cryptic public warnings" by Wyden and Udall, that the Obama Administration was relying on "secret legal interpretations" of its spying powers, so broad that the American public would be "stunned" to learn the scope of it.

On June 6-7, the *Guardian* and the *Washington Post* revealed the existence of the PRISM program involving the leading Internet firms and providers.

On June 7, the *Guardian* reported that the British GCHQ Cheltenham has had access to the NSA's PRISM system since at least June 2010.

On June 7, President Obama acknowledged the reported activities and fully defended them, in terms almost identical to those used by George W. Bush after the disclosure of the NSA spying program in 2005.

The London *Daily Telegraph*) reported on June 8 that members of the British Parliament's Intelligence and Security Committee, which monitors the work of MI5, MI6, and GCHQ, would be coming to the U.S. to meet with senior figures from the NSA and the CIA.