A Review of Intelligence Oversight Failure: NSA Programs that Affected Americans

by Major Dave Owen

The views and opinions expressed here are those of the author and do not necessarily reflect the official policy or position of any agency of the U.S. Government.

Introduction

After World War II, the National Security Agency (NSA) established and directed three programs that deliberately targeted American citizens' private communications. Despite ethical and legal concerns, these programs continued through the early 1970s. This intelligence oversight failure, once it was identified, resulted in a thorough U.S. Senate investigation. Out of this investigation came the 1976 document *"NSA Surveillance Affecting Americans,"* which led to legal restrictions on the agency and robust intelligence oversight processes to ensure that it continued to adhere to these restrictions.[1] This article will summarize the programs that led to this situation, review the legal decisions that affected these programs, and discuss the impact that is still felt within the NSA today.

Background

The NSA rose after World War II in order to centralize and manage U.S. cryptologic efforts. Prior to and throughout the war, these efforts were mostly spread among the military services, and were poorly coordinated, controlled, and understood. In fact, the success of Japan's attack on Pearl Harbor was largely due to this confusing cryptologic situation, as the U.S. had clear warnings through Signals Intelligence (SIGINT) but failed to act.[2] In 1949, the Department of Defense (DoD) attempted to remedy this situation by creating the Armed Forces Security Agency (AFSA). Under the command of the Joint Chiefs of Staff, this agency combined the separate efforts underway in each service. However, the AFSA was ineffective, as continued inter-service rivalries, coupled with poor coordination basically maintained the situation of divided, independent cryptologic efforts. Additionally, as an agency of the Joint Chiefs of Staff, AFSA was not responsive to the SIGINT needs of elements outside of DoD, such as the State Department or the Central Intelligence Agency (CIA).[3]

President Truman created NSA in 1952 to remedy this situation. He issued a classified memorandum to do this, and followed it up with National Security Council Intelligence Directive 9. This classified directive explicitly stated that the NSA would be the "executive agent" for foreign communications intelligence for the entire government.[4] However, this directive did not establish any limitations within the foreign SIGINT mission. Even as late as the 1970s, according to the NSA's general counsel, "no existing statutes control, limit, or define the signals intelligence activities of the NSA."[5] Since foreign intelligence can be derived from American citizens' private communications, and since domestic issues can affect foreign policy (requiring 'foreign intelligence' support for these domestic issues), this situation resulted in minimal control of NSA activities. Additionally, since both the memorandum and directive which led to its creation were classified, the NSA was generally unknown to the public.

As a result, the agency existed in an environment of unquestioned SIGINT authority, minimal intelligence oversight, and no statutory limitations. This environment was exacerbated by a marked appreciation for SIGINT capabilities, especially due to the "demonstrated wartime value of breaking enemy codes, particularly of the Japanese."[6] These factors resulted in a situation which could easily have led to the NSA exploiting American citizens' private communications. However, one additional factor made this possibility a certainty, and also shaped the SIGINT culture so that exploiting American citizens' communications seemed to be a normal part of operations: Project SHAMROCK.

Project SHAMROCK (1945 to 1975)

Project SHAMROCK began in August 1945, shortly before the end of World War II and over seven years prior to the establishment of the NSA.[7] This time frame is important to note when considering the

culture of the SIGINT enterprise. By the time NSA was established, Project SHAMROCK was a long-standing, well-accepted program.

Project SHAMROCK originally started as an effort to improve wartime intelligence activities and was continued after the war due to its intelligence value. It consisted of access to telegraph communications that transited networks owned by several U.S. companies which then provided daily microfilm copies of all traffic. Though this traffic included foreign communications, it also included a vast amount of communications from or to American citizens.

The companies involved in Project SHAMROCK questioned the legality of these activities, especially in peacetime. In fact, they only agreed to support it "provided they received the personal assurance of the Attorney General of the U.S."[8] Additionally, representatives of the companies met with the Secretary of Defense in 1947 to discuss their continued participation. The Secretary of Defense assured them that Project SHAMROCK was "in the highest interests of national security" and that both the Attorney General and the President approved.[9] The companies again brought up this issue in 1949, with similar results. However, though the companies did fear that Project SHAMROCK was illegal, they "never sought assurances that that the NSA was limiting its use to the messages of the foreign targets."[10]

At its peak, Project SHAMROCK collected approximately 150,000 messages per month. NSA generated reports based on this collection to customers including the DoD, the CIA, the Federal Bureau of Investigation (FBI), the Secret Service, and the Bureau of Narcotics and Dangerous Drugs (a precursor of the Drug Enforcement Administration). The inclusion of the FBI and the Bureau of Narcotics and Dangerous Drugs is especially noteworthy, as their mission included mostly domestic targets.

The Director of the NSA terminated Project SHAMROCK in 1975 amongst increasing Congressional concerns that this collection was in violation of the Fourth Amendment which guards against unreasonable searches and seizures unless authorized by a warrant. A previous Supreme Court decision (Katz v. the United States, 1967) identified private communications as protected by Fourth Amendment rights. However, even as late as 1976, the NSA continued to claim that "the Fourth Amendment does not apply to the NSA's interception of Americans' international communications for foreign intelligence purposes."[11]

Though Project SHAMROCK undoubtedly collected and analyzed American citizens' private communications on a large scale, this effort still focused on foreign intelligence. The project was created as an effort to improve the foreign communications intelligence mission, and that purpose continued to be the primary reason for its existence.

Project SHAMROCK was just one of three major programs that infringed on Americans' privacy. The other two programs more directly pursued the private communications of American citizens. The first of these two remaining programs was Project MINARET.

Project MINARET (1960 to 1973)

Project MINARET was essentially the NSA's watch list. It used existing SIGINT accesses (to include information from Project SHAMROCK), and searched for terms, names, and references associated with certain American citizens.

Though Project MINARET officially started in 1969, the watch list itself existed at least as early as 1960.[12] Originally, this list had nothing to do with American citizens. According to the 1975 testimony of a senior NSA official, "the term 'watch list' had to do with a list of names of people, places or events that a customer would ask us to have our analysts keep in mind as they scan large volumes of material."[13] However, starting in 1967, the NSA started adding selectors associated with American citizens to the watch list, establishing a 'civil disturbance' watch list. This was due to requests from the White House, the FBI, and the Attorney General.[14] These requests included:

- "Indications that foreign governments... are controlling or attempting to control or influence the activities of U.S. 'peace' groups and 'Black Power' organizations."
- "Determining whether or not there is evidence of any foreign action to develop or control these anti-Vietnam and other domestic demonstrations."
- "Identities of individuals and organizations in the U.S. in contact with agents of foreign governments."[15]

The Secret Service also requested support through the 'civil disturbance' watch list program, submitting "names of individuals and organizations active in the antiwar and civil rights movements."[16] Finally, the CIA asked for "The activities of U.S. individuals involved in either civil disorders, radical student or youth activities, racial militant activities, radical antiwar activities, draft evasion/deserter support activities … where such individuals have some foreign connection."[17]

After receiving these requests, the Director of the NSA sent a cable to the Director of Central Intelligence and every member of the U.S. Intelligence Board. In this cable the Director informed them that the NSA was "concentrating additional and continuing effort to obtain SIGINT" in support of these requests.[18] Though there is no record that the U.S. Intelligence Board took any action in response to this message, the Board also did not validate these collection requirements. The lack of a response resulted in the continuation of the 'civil disturbance' watch list program.

NSA realized that the 'civil disturbance' watch list was significantly different from their other intelligence missions. First, it dealt with sensitive subjects to include protection of the President, terrorism, and civil disturbances. Second, the SIGINT sources could easily be compromised if information about this program was released. Finally, the sensitive nature of the subject material was on the edge of what the NSA considered legally permissible. One NSA official called it "unprecedented," while another said it was "different from the normal mission of the NSA."

Because of the sensitivity of this program, NSA decided to implement additional safeguards. When intercepts were used where one of the communicants was an American citizen, the resulting serialized product was only disseminated to a limited, by-name distribution. When both communicants were American citizens, the NSA removed itself as the source, the report was labeled "For Background Use Only," it was not serialized, and it was not filed with other SIGINT reports. The Deputy Director of NSA, commenting on these safeguards, said that this was done so that "there would not be any record of this material held in other places within the Agency." [19]

In 1969, due to the growth of the 'civil disturbance' watch list and concerns over the security controls, NSA established Project MINARET. This project contained the entire program, and increased the security requirements. Prior to Project MINARET, only intercepts where both communicants were American citizens were held to the tighter security practices detailed in the preceding paragraph. With the establishment of Project MINARET, all communications "to, from, or mentioning U.S. citizens" were held to this higher security standard.

After the NSA established Project MINARET, the FBI sent the agency two memoranda in an effort to ensure that this activity continued. In these the Director of the FBI stated "this Bureau has a continuing interest in receiving intelligence information obtained under MINARET…There are both white and black racial extremists in the U.S. advocating and participating in illegal and violent activities for the purpose of destroying our present form of government. Because of this goal, such racial extremists are natural allies of foreign enemies of the U.S."[20] This demonstrates the continued effort to classify the Project MINARET activity as foreign intelligence, which would enable its continued existence.

Project MINARET continued until 1973, when it was terminated by the Director of the NSA. Throughout its course, this program targeted a cumulative total of approximately 1,200 American citizens. Targeted individuals included "members of radical political groups, to celebrities, to ordinary citizens involved in protests against their Government."[21]

Though Project MINARET clearly targeted the private communications of American citizens, it did this through existing collection efforts that were originally established to pursue foreign intelligence information.

There is one more NSA program that affected American citizens. In addition to targeting, exploiting, and reporting on the private communications of American citizens, this program also established new collection sources solely to improve access to the private communications of American citizens: the Drug Watch Lists.

Drug Watch Lists (1970 to 1973)

In 1970, the Director of the Bureau of Narcotics and Dangerous Drugs sent a memorandum to the

Director of the NSA requesting "any and all communications intelligence information which reflects illicit traffic in narcotics and dangerous drugs."[22] The Bureau of Narcotics and Dangerous Drugs made this request primarily due to the 1967 Supreme Court decision 'Katz v. the United States.' Because of this decision, the Bureau of Narcotics and Dangerous Drugs believed that it did not have the legal authority to collect this information for law enforcement purposes. However, they also believed that the NSA could collect this information for foreign intelligence purposes, and then share it with them.

The NSA responded to this request by establishing the 'Drug Watch' Lists. These watch lists consisted of individuals and organizations with a history of illegal drug activities. Unfortunately, many of the individuals on these lists were American citizens, and in order to target their private communications the NSA established new collection accesses for that specific purpose.

The CIA joined the Drug Watch Lists effort in 1972, believing that it may have a role separate from the law enforcement perspective (or perhaps believing that the Bureau of Narcotics and Dangerous Drugs was attempting to intrude on a foreign intelligence area). However, after participating in the program for three months, the CIA decided that this effort solely supported a law enforcement function (vice a foreign intelligence purpose) and they ended their participation. Because of this, NSA conducted its own review and came to the same conclusion, ending the program in 1973. To date, this program represents the only occasion where NSA established new collection accesses for the purpose of targeting American citizens.

Legal Considerations: 'Katz v. the United States' (1967)

One of the most significant cases that impacted NSA's programs is 'Katz v. the United States.' In this case, Charles Katz used a public phone booth to relay gambling wagers. This action is illegal according to the Wire Act. The FBI, targeting Katz in their investigation, used an electronic listening device attached to the outside of the phone booth. Based on the evidence from this device, Katz was convicted of violating the Wire Act. However, he appealed his conviction, claiming the listening device violated his Fourth Amendment rights.[23]

Katz believed the listening device constituted an 'unreasonable search and seizure'. He argued that because the FBI did not have a warrant, the recordings should not be admissible in court. The FBI argued that since there was no physical intrusion into the phone booth, this was not an 'unreasonable search and seizure.' Additionally, the FBI argued that previous Supreme Court cases ruled along similar lines:

- In 'Olmstead v. the United States' (1928), the Supreme Court ruled that phone conversations obtained by warrantless wiretaps were legal. In this case, Chief Justice Taft commented "The (Fourth) Amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing, and that only."[24]
- In 'Goldman vs. the United States' (1942), the Supreme Court ruled that conversations were not protected under the Federal Communications Act (1934) when the means of intercept was not through the phone system. The Federal Communications Act protected American citizens against warrantless wiretaps, but in 'Goldman vs. the United States' the Supreme Court ruled that the communications were only protected "throughout the course of its transmission."[25]

Based on these arguments, the Court of Appeals ruled for the FBI. However, the Supreme Court decided to conduct a judicial review. In this review, the Supreme Court overturned the Court of Appeals decision, and ruled in favor of Katz. Justice Harlan summarized the ruling by stating "an enclosed telephone booth is an area where, like a home, and unlike a field, a person has a constitutionally protected reasonable expectation of privacy…An invasion of a constitutionally protected area by federal authorities is, as the Court has long held, presumptively unreasonable in the absence of a search warrant."[26]

The Supreme Court decision in 'Katz v. the United States' established a new legal precedent for the Fourth Amendment. This precedent defined "unreasonable searches and seizures" as applying to any situation where a person has a "reasonable expectation of privacy." Though this decision clearly could apply to Project SHAMROCK, this program was well established by that point. Additionally, it

was unclear if this ruling even affected the 'foreign intelligence mission,' or if it just applied to law enforcement collection.

Legal Considerations: 'The Keith Case' (1972)

Another noteworthy legal decision is 'United States v. United States District Court.' This case, better known as 'The Keith Case', was named after the presiding judge for the U.S. District Court, Judge Damon Keith. In this case, the U.S. charged three individuals with 'conspiracy to destroy government property.' Additionally, one of these individuals was also charged with bombing a CIA office.[27]

In the 'Keith Case', much of the evidence came from warrantless wiretaps. However, the Attorney General argued that these wiretaps did not fall under the authority of the Federal Communications Act. The Attorney General argued that the wiretaps were authorized under Title III of the Omnibus Crime Control and Safe Streets Act (1968), which allows warrantless wiretaps when there is a "clear and present danger to the structure or existence of the Government."[28]

After reviewing the arguments, Judge Keith did not concur with the Attorney General's request to keep the sources confidential, and ordered the U.S. to disclose all sources and intercepts. Following this ruling, the U.S. appealed to the Sixth Circuit Court. However, the Sixth Circuit Court concurred with Judge Keith's original decision. The Attorney General appealed yet again to the Court of Appeals. At this point the Supreme Court decided to hear the case.

The Supreme Court debated the case for almost four months before they ruled in favor of the lower courts. When explaining their decision, Justice Powell stated "The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power…For private dissent, no less than open public discourse, is essential to our free society."[29]

This ruling reinforced that wiretaps and other means of intruding upon a person's 'reasonable expectation of privacy' can only be conducted with a warrant. However, just like the ruling in 'Katz v. the United States,' it was unclear if the 'Keith Case' ruling just applied to law enforcement collection, or if it also affected the 'foreign intelligence mission.'

The Church Committee (1975 to 1976)

'The U.S. Senate Select Committee to Study Governmental Operations with respect to Intelligence Activities,' better known as the 'Church Committee' investigated the NSA's programs that affected American citizens. This thorough investigation resulted in the report "National Security Agency Surveillance Affecting Americans." In this report the Senate Select Committee argued that the lack of a statutory charter or other significant control mechanism constituted an unacceptable risk to American citizens' Fourth Amendment rights.[30]

The Committee viewed the NSA situation through the lens of 'The Keith Case,' and their perspective is best summed up by Justice Powell: "History abundantly documents the tendency of Government–however benevolent and benign its motives–to view with suspicion those who most fervently dispute its policies…The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect 'domestic security'."[31] Because of this perspective, the Church Committee seemed genuinely surprised by much of the testimony, even though most of the programs they investigated had been in place for over a decade.

The Church Committee reviewed thousands of pages of statements and testimony, and presented a coherent, thorough view of the programs that affected American citizens. In order to be as persuasive as possible, the Committee did not include any differing perspectives which would have made this report less impacting. It was careful to avoid any reference to noteworthy intelligence that resulted from these programs, and only provided details that supported its arguments.

The report was undeniably effective. It clearly demonstrated the negative results that can come from an unrestrained SIGINT agency, even when the individuals within this agency have good intentions. Additionally, this report led to legal restrictions on the NSA's foreign intelligence authorities, as well as robust intelligence oversight processes to ensure that NSA continued to adhere to these legal restrictions. The most notable of these results was the Foreign Intelligence Surveillance Act.

Legal Considerations: The Foreign Intelligence Surveillance Act (1978)

The Foreign Intelligence Surveillance Act formally defined the rules and procedures required for phys-

ical and electronic surveillance in support of the foreign intelligence mission. Prior to this act, this mission was largely unregulated with minimal oversight. Even though there were many developments in the rules required for law enforcement purposes, it was not clear if these developments also affected the foreign intelligence mission. Additionally, since this mission was out of sight of the public eye, it did not receive the same scrutiny.

The act limited the scope of the NSA's foreign intelligence mission, and also implemented strict, warrant-based procedures that all U.S. agencies had to follow for foreign intelligence issues. As well, it implemented thorough and mandatory intelligence oversight processes. These processes ensured that U.S. government agencies would conduct their foreign intelligence missions while protecting American citizens' Fourth Amendment rights.[32]

The Lasting Impact on the NSA

The current intelligence oversight processes are a testament to the impact of the Church Committee, and are a lasting legacy of the Foreign Intelligence Surveillance Act. In addition to mandatory annual intelligence oversight training and quarterly intelligence oversight reports, there is a requirement to identify and quickly report possible intelligence oversight violations. These processes have formed and continuously reinforce an NSA culture that is extremely adverse to any issue that may be construed as collecting on American citizens. Though this culture has shifted slightly over the last decade, most NSA employees are, at best, uncomfortable around these issues. Though the NSA culture will slowly shift, especially as new global technologies continue to blur the communications environment, NSA employees will continue to be exceptionally aware of their intelligence oversight responsibilities.

Summary

Due to the background of the NSA and the lack of statutes that controlled, limited, or defined its SIGINT activities for 30 years, the agency existed in an environment of unquestioned SIGINT authority with minimal intelligence oversight. This situation led to several programs that directly affected American citizens' Fourth Amendment rights. Though several associated Supreme Court decisions affected similar law enforcement situations, NSA continued to operate these programs under the cover of its undefined foreign intelligence mission. This led to the Church Committee investigation, and eventually to the establishment of the Foreign Intelligence Surveillance Act. As a result, NSA now includes robust, mandatory intelligence oversight processes as part of its regular operations. These processes have created and continuously reinforce a culture that is extremely adverse to any issue that may be construed as collecting on American citizens. NSA will continue to operate with this culture for the foreseeable future as it pursues its legitimate foreign intelligence mission.

Endnotes

1. U.S. Senate, *"Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities: National Security Agency Surveillance Affecting Americans,"* 23 April 1976.

2. John Hughes-Wilson, *"Military intelligence Blunders and Cover-Ups,"* (New York: Carroll and Graf Publishers, 2004), 60-101.

3. Thomas L. Burns, *"The Origins of the National Security Agency 1940-1952"*, Center for Cryptologic History, NSA, 1990, 59-81.

4. Ibid., 3, 97-112.

5. Disposition of Roy Banner, NSA General Counsel, 4 February 1976.

6. Ibid., 1.

7. Ibid., 1.

8. Ibid., 1.

9. Testimony of Robert Andrews, Special Assistant to the General Counsel, DoD, 23 September 1975.

10. Ibid., 1.

11. Ibid., 5.

12. Ibid., 1.

13. Ibid., 1.

14. Testimony of General William Yarborough, Army Assistant Chief of Staff for Intelligence, 10 September 1975.

15. Cable from General William Yarborough to General Marshall Carter, 20 October 1967.

16. Secret Service response to the Senate Select Committee, 12 October 1975.

17. Ibid., 1.

18. Cable from General Marshall Carter to General William Yarborough, 21 October 1967.

19. Testimony of Benson Buffham, Deputy Director, NSA, to the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, 12 September 1975.

20. Memoranda from J. Edgar Hoover to Director, NSA, 3 June 1970, 6 November 1970.

21. Ibid., 1.

22. Memorandum from John Ingersoll to Noel Gaynor, 10 April 1970.

23. U.S. Supreme Court Case Law: Katz v. United States, 389 U.S. 347. Argued 17 October 1967, decided 18 December 1967.

24. U.S. Supreme Court Case Law: Olmstead v. United States, 277 U.S. 438. Argued 20-21 February 1928, decided 4 June 1928.

25. U.S. Supreme Court Case Law: Goldman v. United States, 316 U.S. 129. Argued 5-6 February 1942, decided 27 April 1942.

26. Ibid., 23.

27. U.S. Supreme Court Case Law: United States v. United States District Court (The Keith Case), 407 U.S. 297. Argued 24 February 1972, decided 19 June 1972.

28. The Omnibus Crime Control and Safe Streets Act, Public Law 90-351, 82 Statute-at-Large 197, Title 42 U.S. Code 3711, 19 June 1968.

29. Ibid., 27.

30. Ibid., 1.

31. Ibid., 27.

32. Foreign Intelligence Surveillance Act, Public Law 95-511, 92 Statute-at-Large 1783, Title 50 U.S. Code Chapter 36, 25 October 1978.

MAJ Owen has worked in the SIGINT community for over a decade and is currently assigned as the Operations Officer for the 709th MI Battalion. He holds a Bachelor's Degree in Applied Mathematics, with a minor in Physics, and is currently pursuing a Master's Degree in Strategic Intelligence. Additionally, he is a graduate of the Junior Officer Cryptologic Career Program.