

# Literal intelligence collection

[Law](#), [Security](#)



Literal Intelligence Collection: National Intelligence and the NSA wireless intercept program Intelligence Collection: Sources and Challenges February 13, 2012 In the aftermath of 9/11 the intelligence community (IC) felt pressure from all directions. Employees of the IC, Congress, and the general public wanted questions answered as to why our nation didn't know an attack was imminent. This "failure" of intelligence caused a shake up within the entire IC, leading to many future changes. One such change was in communications intelligence (COMINT) collection.

According to Cummings (2006), " President George W. Bush said that he authorized NSA to intercept the international communications of people with known links to al Qaeda and related terrorist organizations in the weeks following the September 11th terrorist attacks" (p. 6). The President's decision had many repercussions. I will discuss the parameters of the decision, the management issues associated with it that lead to such controversy, and the impact it had on national intelligence and the NSA.

What led to this drastic decision by the U. S. President? The United States was blind-sighted in the September 11, 2001 terrorist attack which resulted in the death of 2, 977 innocent Americans. This was the largest attack in the history of the U. S. on our soil and although the signs were there for the intelligence community to see, it was mistakenly not put together. Much of the attack stemmed from communications between terrorist or those connected and working with terrorist within our Country, and this was unacceptable.

In order to defend against such communications, according to Lichtblau & Risen (2005), " Under a presidential order signed in 2002, the intelligence <https://assignbuster.com/literal-intelligence-collection/>

agency has monitored the international telephone calls and international e-mail messages of hundreds, perhaps thousands, of people inside the United States without warrants over the past three years in an effort to track possible ‘dirty numbers’ linked to Al Qaeda, the officials said. The agency, they said, still seeks warrants to monitor entirely domestic communications”.

The sole purpose of the NSA program was to safeguard our national security in a more expansive, efficient manner. The center on law and security (2007) states “...this requirement to demonstrate all of the substantive and procedural elements of FISA to the Attorney General's satisfaction before any surveillance can begin, would fatally impair the President's ability to carry out his constitutional responsibility to collect foreign intelligence to protect our Nation from attack” (p. 9).

Any implementation involving citizen's privacy is assured to draw controversy, and the root of the problem with this program was a management issue. The President, DCI, and the Director of the NSA should have informed the head of the Senate Select and Congressional oversight committees with a more in depth understanding of the changes and the secrecy. A plan should have been in place to deal with leaks to the public of the changes, and a more detailed description of the amendment to the policy should have been created and kept under lock and key.

Intelligence collection involves many activities that citizens (lacking all of the facts), may deem unconstitutional. The problem with this is most of the time the facts are not available to the general population, media, and even certain members of the Congressional oversight committees, for fear of an operation leak. Much of what the IC does must remain secret, at least until

the aftermath (which could be years later). In regards to the topic at hand, authorization of warrantless wireless intercept by the NSA, the main problem arose due to management failures in the implementation of such a controversial topic.

The center on law and security (2007) states, “ Critics of the NSA program do not necessarily object to the type of surveillance, but rather to the way in which it has been authorized, and to the absence of any oversight” (p. 10). The Congressional oversight committees serve as a checks and balance to the IC and the President informed the heads of the committees (Gang of Eight) of his plan to authorize wireless intercepts on Americans. Cummings (2006) states, “...the executive branch had limited its briefings of the legislative branch to the Gang of Eight.

They further asserted that the executive branch had prohibited them from sharing any information about the program with congressional colleagues” (p. 7). In the aftermath, it seems the Gang of Eight did not understand the necessity of secrecy behind this information. The President should have explained the reasoning behind the secrecy and why the information was limited to the Gang of Eight. If the Gang of Eight understood the parameters and restrictions in place, they could better defend the plan when future problems arose. Preparations should have been in place for dealing with the public if and when the time came that the media caught wind of the wireless intercept. At some point the President should expect that the public would have to be addressed with some details defending his actions. There should have been regulations in place, describing the limits the NSA still had to endure when it came to U. S. citizens. When reports came out in 2005, there

was much confusion as to what exactly the President had authorized, and if there were limits in place for the NSA. A failure to properly address the issue allowed the media to run wild with stories, further outraging critics.

Silence and secrecy only added to the problem of distrust of the IC. In preparation, President Bush should have had a detailed description of the amendment to the policy, with restrictions still in place for the NSA. This policy should have been dated at the time it went into effect, signed by the President, the DCI, the Director of NSA and the Gang of Eight and kept in the possession of the Director of the NSA. Having a signed document would serve the future purpose of showing there was knowledge of the parameters of the amended policy.

If this policy had to become public (open source) at some point, it would hopefully show that Management had made an organized effort of implementing change and involved as many officials as possible under the current circumstances. The National Security Agency (NSA) has the task of protecting U. S. national security systems through the use of signal intelligence (SIGINT), to include COMINT. Prior to the President giving authorization to warrantless domestic eavesdropping following 9/11, the NSA had to obtain a court approved warrant in order to eavesdrop on a U.

S. citizen's communications, otherwise known as a FISA (Foreign Intelligence Surveillance Act) warrant. According to the center on law and security (2007) " FISA warrants require ' probable cause' to suspect that an individual is acting either for a ' foreign power' (including terrorist organizations) or as an ' agent of a foreign power,' a target (a cell phone, a computer, a BlackBerry, or a landline phone, for example), and that foreign intelligence be a ' "

significant purpose’ of the warrant” (p. ). NSA is no stranger to negative public perception regarding their unconstitutional practices. This wireless intercept program put the agency’s reputation at stake once again. Reports of the NSA having access to most American’s phone records detailing their calls and communications is cause for concern for critics. Due to a lack of proper implementation, notifications and opportunity for oversight, the NSA and the IC has to climb another uphill battle to win back the trust of Americans.

Dilanian (2011) states, “ U. S. intelligence officials insist that the new surveillance powers have been crucial to stopping terrorist plots”. Hopefully, some of the more recent successes in the community can erase the impact of failures and the intelligence community can improve their reputation once again. References Cummings, Alfred (2006). Statutory procedures under which Congress is to be informed of U. S. intelligence activities, including covert actions: NSA domestic surveillance.

Congressional Research Service Dilanian, Ken (2011). 9/11, ten years after, more surveillance; A legacy of watchful eyes; The government eavesdrops on U. S. citizens as never before. Los Angeles Times Aug 30, 2011. Tuesday Home Edition. Lichtblau, E. & Risen, J. (2005). Bush lets U. S. spy on callers without courts. The New York Times, Dec 16, 2005. doi: 942423341 The Center on Law and Security at the NYU school of Law (2007). The NSA wiretapping program. For The Record, 1(Jan) 1-16.