

**From:** "Gerry, Brett C."  
**To:** "Kavanaugh, Brett M."  
**Subject:** FW: [Fwd: Final Version of the Speech]  
**Received(Date):** Tue, 24 Jan 2006 17:02:58 -0500  
[NatIPressClub--23Jan--0915.doc](#)

This is the final, to my knowledge. Hayden quote is at top of p. 8.

---

**From:** b3 50 USC 3024 (m)(1)

**Sent:** Monday, January 23, 2006 9:26 AM

**To:** Bartlett, Dan; Kavanaugh, Brett M.; Miers, Harriet; Kelley, William K.; Addington, David S.; Bellinger, John B(Legal); Courtney.Elwood@usdoj.gov; Drummond, Michael; Perino, Dana M.; Rachel.Brand@usdoj.gov; Roebke, Heather M.; Wanda.Martinson@usdoj.gov; Allen, Michael; Coffin, Shannen W.; Gerry, Brett C.; Kyle.Sampson@usdoj.gov; Larry Pfeiffer; McClellan, Scott; McDonald, Matthew T.; Steve.Bradbury@usdoj.gov; West, Christal R.; Wolff, Candida P.

**Subject:** [Fwd: Final Version of the Speech]

final version prepared for delivery.

----- Original Message -----

**Subject:** Final Version of the Speech

**Date:** Mon, 23 Jan 2006 09:16:26 -0500

b3 50 USC 3024 (m)(1)

**Principal Deputy Director of National Intelligence**  
**Address to the National Press Club**  
**23 January 2006**

Good morning. I'm happy to be here to talk a bit about what American intelligence and especially NSA have been doing to defend the Nation.

I'm here today not only as Ambassador Negroponte's deputy in the Office of the Director of National Intelligence. I'm also here as the former Director of the National Security Agency, a post I took in March of 1999 and left only last spring.

Serious issues have been raised in recent weeks. And discussion of serious issues should be based on facts. There is a lot of information out there—some of it is frankly inaccurate, much of it is simply misunderstood. I'm here to tell the American people what NSA has been doing and why. And, perhaps more importantly, what it has not been doing.

Admittedly, this is a little hard to do while protecting our country's intelligence sources and methods. And people in my line of work generally don't like to talk about what they've done until it's a subject on the History Channel.

But let me make one thing very clear: as challenging as this might be, this is the speech I want to give. I much prefer being here with you today telling you about the things we have done when there hasn't been an attack on the US Homeland.

This is a far easier presentation to make than the ones I had to give four years ago—telling audiences like you *what we hadn't done* in the days and months leading up to the tragic events of September 11<sup>th</sup>. Today's story is not an easy one to tell in this kind of unclassified environment, but it is by far the brief I prefer to present.

We all have searing memories of the morning of September 11<sup>th</sup>. I know I do: making a decision to evacuate non-essential workers at NSA while the situation was still unclear; seeing the NSA counter terrorist shop in tears while black out curtains were being stapled to walls around their windows; like many of you, asking my wife to find our kids and then hanging up the phone on her.

Another memory comes from two days later when I addressed the NSA workforce to lay out our mission in a new environment. It was a short video talk beamed throughout our headquarters at Fort Meade and globally. Most of what I said was what anyone would expect. I tried to inspire. Our work was important and the Nation was relying on us. I tried to comfort. Look on the bright side I said to them: right now a quarter billion Americans wished they had your job...being able to go after the enemy. I ended the talk by trying to give perspective. I noted that all free peoples have had to balance the demands of liberty with the demands of security. Historically we Americans had planted our



flag well down the spectrum toward liberty. Here was our challenge. “We were going to keep America free,” I said, “by making Americans feel safe again.”

But to start the story with that Thursday, September 13<sup>th</sup> is misleading, because it is really near the end of the first reel of this movie. To understand that moment and that statement, you would have to know a little bit about what had happened to the National Security Agency in the preceding years.

NSA intercepts communications and it does so for only one purpose: to protect the lives, the liberties and the well being of the citizens of the United States from those who would do us harm. By the late 1990s, that job was becoming increasingly more difficult. The explosion of modern communications in terms of volume, variety and velocity threatened to overwhelm us.

The Agency took a lot of criticism in those days—that it was going deaf; that it was ossified in its thinking; that it had not and could not keep up with the changes in modern communications. All that was only reinforced when all the computer systems at Fort Meade went dark for three days in January of 2000 and we couldn’t quickly or easily explain why.

Those were interesting times. As we were being criticized for being incompetent and going deaf, others seemed to be claiming that we were omniscient and reading your e-mails.

The Washington Post and New Yorker Magazine during that time incorrectly wrote that, “NSA has turned from eavesdropping on the Communists to eavesdropping on businesses and private citizens,” and that, “NSA has the ability to extend its eavesdropping network without limits.” We were also referred to as “a global spying network that can eavesdrop on every single phone call, fax, or e-mail, anywhere on the planet.”

I used those quotes in a speech I gave at American University in February 2000. The great “urban legend” then was something called Echelon and the false accusation that NSA was using its capabilities to advance American corporate interests: signals intelligence for General Motors or something like that. With these kinds of charges, the turf back then feels familiar now: how could we prove a negative (that we weren’t doing certain things) without revealing the appropriate things we were doing that kept America safe.

You see, NSA had (and has) an existential problem. In order to protect American lives and liberties it has to be two things: powerful in its capabilities and secretive in its methods. And we exist in a political culture that distrusts two things most of all: power and secrecy.

Modern communications didn’t make this any easier. Gone were the days when “signals of interest” went along a dedicated microwave link between strategic rocket forces headquarters in Moscow to an ICBM base in western



Siberia. By the late nineties, what NSA calls “targeted communications”—things like al Qaeda communications—co-existed out there in a great global web with your phone calls and my e-mails. NSA needed the power to pick out the one and the discipline to leave the others alone.

So this question of security and liberty wasn’t a new one for us in September 2001. We always have had this question: how do we balance the legitimate need for foreign intelligence with our responsibility to protect individual privacy rights? It is a question drilled into every employee of NSA from day one, and it shapes every decision about how NSA operates.

September 11<sup>th</sup> didn’t change that. But it did change some things.

This ability to intercept communications, commonly referred to as Signals Intelligence (SIGINT), is a complex business with operational, technological and legal imperatives often intersecting and overlapping. There is routinely some freedom of action—within the law—to adjust operations. After the attacks I exercised some options I always had that collectively better prepared us to defend the Homeland.

Let me talk about this for a minute. Because a big gap in understanding is what’s standard—what does NSA do routinely?

Where we set the threshold for what constituted “inherent foreign intelligence value” in reports involving a US person, for example, shapes the level of some of our collection and reporting. The American SIGINT system in the normal course of its foreign intelligence activities inevitably captures this kind of information—information to, from or about what we call a US person (by the way, that routinely includes anyone in the United States, citizen or not.) So, for example, because they were in the United States Mohammad Atta and his fellow 18 hijackers were presumed to be protected persons.

“Inherent foreign intelligence value” is one of the metrics we must use to ensure that we conform to the 4<sup>th</sup> Amendment’s “reasonableness” standard when it comes to protecting the privacy of that person. If the US person information isn’t relevant, the data is suppressed or what we call minimized. The individual is not mentioned, or if he is, he is referred to as US person number one. If the US person is actually the named terrorist, well, that could be a different matter.

The standard by which we decided that—the standard of what was relevant and valuable, and therefore what was reasonable—would understandably change as smoke billowed from two American cities and a Pennsylvania farm field, and we acted accordingly. To somewhat oversimplify the question of inherent intelligence value—to just use an example—we had a different view of Zacarias Moussaoui’s computer hard drive after the attacks than we had before.



This is not unlike what happened in other areas. Prior to September 11th airline passengers were screened in one way. After September 11th, we changed how we screened passengers. Similarly, although prior to September 11th certain communications weren't considered valuable intelligence, it became immediately clear after September 11 that intercepting and reporting these same communications were, in fact, critical to defending the homeland.

These decisions were easily within my authorities as Director of NSA under an executive order, known as Executive Order 12333, that was signed in 1981—an Executive Order that has governed NSA for nearly a quarter century.

Let me summarize: in the days after 9-11, NSA was using its authorities and its judgment to appropriately respond to the most catastrophic attack on the Homeland in the history of the Nation.

That shouldn't be a headline, but as near as I can tell, these actions on my part have created some of the noise in recent press coverage. Let me be clear on this point--except that they involved NSA, these programs were not related to the authorization that the President has recently talked about. I asked to update the Congress on what NSA had been doing and I briefed the entire House Intelligence Committee on the 1st of October 2001 on what we had done under NSA's previously existing authorities.

As part of our adjustments, we also turned on the spigot of NSA reporting to FBI in an unprecedented way. We found that we were giving them too much data in too raw a form. We recognized it almost immediately—a question of weeks—and made adjustments.

This flow of data to the FBI has also become part of the current background noise. Despite reports in the press of “thousands of tips a month,” our reporting has not even approached that kind of pace.

I actually find all of this a little odd. After all the findings of the 9-11 Commission and other bodies about the failure to *share* intelligence, I'm up here feeling like I have to explain pushing data to those who might be able to use it.

And it is the nature of intelligence that many tips lead nowhere but you have to go down some blind alleys to find the tips that pay off.

Beyond the authorities that I exercised under the standing executive order, as the war on terror has moved forward we have aggressively used FISA warrants. The Act and the Court have provided us with important tools and we make full use of them. Published numbers show us using the Court at record rates and the results have been outstanding.

But the revolution in telecommunications technology has extended the actual impact of the FISA regime far beyond what Congress could ever have



anticipated in 1978. And I don't think that anyone could make the claim that the FISA statute is optimized to deal with a 9/11 or to deal with a lethal enemy who likely already had combatants inside the United States.

I testified in open session to the House Intelligence Committee in April of the year 2000. At the time I created some looks of disbelief when I said that if Usama bin Ladin crossed the bridge from Niagara Falls, Ontario to Niagara Falls, New York, there were provisions of US law that would kick in, offer him protections and affect how NSA could now cover him. At the time I was just using this as a stark hypothetical. Seventeen months later this was about life and death.

So we now come to one additional piece of NSA's authorities: these are the activities whose existence the President confirmed several weeks ago. The authorization was based on an intelligence community assessment of a serious and continuing threat to the homeland. The lawfulness of the actual authorization was reviewed by lawyers at the Department of Justice and the White House and was approved by the Attorney General.

There is a certain sense of sufficiency here: authorized by the President, duly ordered, its lawfulness attested to by the Attorney General, and its content briefed to the Congressional leadership.

But we all have a personal responsibility. And in the end, NSA would have to implement this--and every operational decision the Agency makes is made with the full involvement of its legal office.

NSA professional career lawyers—and the Agency has a lot of them—have a well-deserved reputation. They're good. They know the law. And they don't let the Agency take many close pitches.

And so, even though I knew that program had been reviewed by the White House and the Department of Justice, I asked the three most senior and experienced lawyers in NSA. Our enemy in the global war on terrorism doesn't divide the United States from the rest of the world. The global telecommunications system doesn't make that distinction either. Our laws do—and should. How did these activities square with these facts? They reported back that they supported the lawfulness of the program—supported, not acquiesced. This was very important to me.

A veteran NSA lawyer, now retired, told me that a correspondent had suggested to him recently that all of the lawyers connected with this program had been very careful from the outset because they knew there would be a "day of reckoning." The NSA lawyer replied that that had not been the case. NSA had been so careful, he said—and I'm using his words here--because in this very focused, limited program NSA had to ensure that it dealt with privacy interests in an appropriate manner.



In other words, our lawyers weren't careful out of fear. They were careful out of a heartfelt and principled view that NSA operations had to be consistent with bedrock legal protections.

In early October 2001 I gathered key members of the NSA work force in our conference room and introduced our new operational authorities to them. With the historic culture at NSA being what it was (and is), I had to do this personally. I told them what we were going to do and why. I also told them that we were going to carry out the program and not go one step further. NSA's legal and operational leadership then went into the details of our new task.

The 9-11 Commission criticized our ability to link things happening in the United States with things that were happening elsewhere. In that light, there are no communications more important to the safety of the Homeland than those affiliated with al Qa'ida with one end in the United States. The President's authorization allows us to track this kind of call more comprehensively and more efficiently.

The trigger is quicker and a bit softer than it is for a FISA warrant but the intrusion into privacy is also limited—only international calls and only those we have a reasonable basis to believe involve al Qa'ida or one of its affiliates. The purpose of all of this is not to collect reams of intelligence but to detect and prevent attacks.

The Intelligence Community has neither the time, the resources, nor the legal authority to read communications that aren't likely to protect us, and NSA has no interest in doing so.

These are communications that we have reason to believe are al Qa'ida communications, a judgment made by the American intelligence professionals (not political appointees) most trained to understand al Qa'ida tactics, communications and aims.

Their work is actively overseen by the most intense oversight regime in the history of the National Security Agency. The Agency's conduct of the program is thoroughly reviewed by the NSA's General Counsel and Inspector General. The program has also been reviewed by the Department of Justice for compliance with the President's authorization.

Oversight also includes an aggressive training program to ensure that all activities are consistent with the letter and intent of the authorization and with the preservation of civil liberties.

Let me also talk for a minute about what this program is not. It is not a driftnet over Dearborn or Lackawanna or Fremont grabbing conversations that



we then sort out by these alleged keyword searches or data mining tools or other devices that so-called experts keep talking about. This is targeted and focused.

This is not about intercepting conversations between people in the United States. This is hot pursuit of communications entering or leaving the United States involving someone we believe is associated with al Qa'ida.

We bring to bear all the technology we can to ensure that this is so. And if there were an anomaly and we discovered there had been an inadvertent intercept of a domestic-to-domestic call, that intercept would be destroyed and not reported but the incident—the inadvertent collection—would be recorded and reported. But that's a normal NSA procedure—for at least a quarter century.

And, as we always do when dealing with US person information, US identities are expunged when they are not essential to understanding the intelligence value of reports. Again, that's a normal NSA procedure.

So let me make this clear. When you are talking to your daughter away at State college, this program *cannot* intercept your conversations. And when she takes a semester abroad to complete her Arabic studies, this program *will* not intercept your conversations.

Let me emphasize one more thing that this program is not. Look, I know how hard it is to write a headline that is accurate, short and grabbing. But we should really shoot for all three attributes.

“Domestic Spying” doesn't really make it. One end of any call targeted under this program is always outside the United States. I have flown a lot in this country and I've taken hundreds of *domestic* flights. I have never boarded a domestic flight in this country and landed in Waziristan.

In the same way—and I am speaking illustratively here—if NSA had intercepted al Qa'ida ops chief Khalid Sheik Mohammed in Karachi talking to Mohammed Atta in Laurel, Maryland in say July of 2001...if NSA had done that and the results had been made public, I'm convinced that the crawler on all the 7/24 news networks would not have been: NSA domestic spying!

Had this program been in effect prior to 9-11, it is my professional judgment that we would have detected some of the 9-11 al Qa'ida operatives in the United States, and we would have identified them as such.

I've said earlier that this program has been successful. Clearly not every lead pans out, from this or any other source, but this program has given us information that we would not otherwise have been able to get. It's impossible for me to talk about this more in any public way without alerting our enemies to our tactics or what we have learned. I can't give details without increasing the danger to Americans. On one level I wish that I could, but I can't.



Our enemy has made his intentions clear. He has declared war on us. Since September 11<sup>th</sup> al Qa'ida and its affiliates have continued to announce their intention and continue to act on their clearly stated goal of attacking America. They have succeeded against our friends in London, Madrid, Bali, Amman, Istanbul and elsewhere. They desperately want to succeed against us.

The 9-11 Commission told us that "Bin Laden and Islamist terrorists mean exactly what they say: to them America is the font of all evil, the 'head of the snake', and it must be converted or destroyed." Bin Laden reminded us of this intention as recently as last Thursday.

The people at NSA, and the rest of the Intelligence Community, are committed to defend us against this evil and to do it in a way consistent with our values.

[We know that we can only do our jobs if we have the trust of the American people. And we can only have your trust if we are careful about how we use our tools and resources. That sense of care is part of the fabric of the intelligence community—it helps defines who we are.]

I recently went out to Fort Meade to talk to the work force involved in this program. They know what they have contributed and they know the care with which it has been done. Even in today's heated environment, the only concern expressed to me was continuing their work in the defense of the nation, and doing so in a manner that honors the law and the Constitution.

As I was talking with them I looked out over their heads to see a large sign fixed to one of the pillars that breaks up their office space. The sign is visible from almost all of the work area. It's yellow with bold black letters. The title is readable from 50 feet: "What Constitutes a US Person." And that is followed by an explanation of the criteria.

That has always been the fundamental tenet of privacy for NSA. And here it was, in the center of a room, guiding the actions of a workforce determined to prevent another attack on the United States.

Security and liberty. The people at NSA know what their job is.

I know what my job is, too. I learned a lot from NSA and its culture during my time there. But I come from a culture, too. I have been a military officer for nearly 37 years and from the start I have taken an oath to protect and defend the Constitution of the United States. I would never violate that Constitution nor would I abuse the rights of the American people. As Director I was the one responsible to ensure that this program was limited in its scope and disciplined in its application.



American intelligence and especially American SIGINT is the front line of defense in dramatically changed circumstances, circumstances in which—if we fail to do our job well and completely—more Americans will almost certainly die. The speed of operations, the ruthlessness of our enemy, the pace of modern communications has called on us to do things and do them in ways never before required. We have worked hard to find innovative ways to protect the American people and the liberties we hold dear. And in doing so we have not forgotten who we are.