AmericanRhetoric.com

General Keith Alexander

Keynote Briefing at the Black Hat 2013 Conference

delivered 31 July 2013, Las Vegas, Nevada

AUTHENTICITY CERTIFIED: Text version below transcribed directly from audio

Well, Trey [Ford] and Jeff [Moss], thanks. Thanks for that introduction.

I think what they said to start out with is the reason I'm here. This is the technical foundation for our world's communications, you folks right here, and the issue that stands before us today is one of what do we do next? How do we start this discussion on defending our nation and protecting our civil liberties and privacy? The reason I'm here is because you may have some ideas of how we can do it better. We need to hear those ideas. But equally important, from my perspective, is that you get the facts. And so what I'm going to do today is try to lay out those facts.

Now as Trey or Jeff said, there are good reasons why some of this is classified and why some of it is stuff that we just don't put out there. And the big reason, from my perspective, is because terrorists use our communications. They live among us. How do we come up with a program to stop terrorism and to protect our civil liberties and privacy? This is perhaps one of the biggest issues facing our country today.

I also want you to get a sense for the people at the National Security Agency. It has been the greatest honor and privilege of my life to lead these noble folks. They're the ones -- and you'll get a little bit of sense of what they've done for our country over the past eight years while I've been there. And their reputation is tarnished because all the facts aren't on the table. But you can help us articulate the facts properly. I will answer every question to the fullest extent possible, and I promise you the truth -- what we know, what we're doing, and what I cannot tell you because we don't want to jeopardize our future defense.

What we're going to do in this briefing is give you the facts on these programs -- the business record, FISA, on FAA 702 -- on what we've done to stop terrorist attacks, address some of the problems that we see out there with inaccurate statements, and talk about where do we go from here.

That's where you come in. We need to hear from you, because the tools and the things we use are very much the same as the tools that many of you use in securing networks. The difference, in part, is the oversight and the compliance that we have in these programs. That part is missing in much of the discussion. I believe it's important for you to hear that, for you to understand what these people have to do in order to do their job to defend this nation and the oversight regime that we have with the courts, with Congress, and with the Administration. I think you need to understand that to get the full understanding of what we do and what we do not do.

I think it's important to also step back. Let's go back to the beginning. How did we get here? (And normally, being a General, I would say, next slide. But they gave me a device. And they said, figure it out. It says "cue." I thought that would be "clue." Okay. So there we go.)

Let's go back to 1993, the World Trade Center. It [the presentation slide] goes pretty quickly -- Khobar Towers, the East African Embassy bombings, the USS Cole, 9/11. Al-Qaida on the ones on the bottom there, throughout Khalid Sheikh Mohammed, helped fund the first World Trade Center [bombing] and was the mastermind behind 9/11. We became a nation transformed.

The intelligence community, according to the 9/11 Commission, failed to connect the dots. What do I mean by that? What do I mean by failed to connect the dots? We had intercepts of one of the 9/11 hijackers, Mihdhar, from Yemen. We didn't know, because we didn't have the tools and the capabilities to see, that he was actually in California. We couldn't provide the right tip or information that connected that foreign dot to a domestic plot. The intelligence community failed to connect those dots. And now what we're doing is putting into existence these programs.

But, I think, in order to understand -- So how do we actually use these programs? -- from my perspective, it's important to first understand the people at the National Security Agency -- what they do and how they do it. So from my perspective, the best first thing is to step back and say, "What did they do during this time period?" "What are they doing?" And so our job is defending this country, saving lives, supporting our troops in combat. And when you think about our Soldiers, Sailors, Airmen, and Marine[s] that were in Iraq and in Afghanistan, it is our responsibility, along with the rest of the intelligence community, to provide the information that they need to survive, to go after the enemy.

What you see on this slide is one of those tools that we brought to bear[1]. This is a technical tool. What's not shown on this slide is the thousands of NSA personnel who volunteered to go forward. Over 6,000 NSA employees have gone to Afghanistan and Iraq. Twenty of those cryptologists paid the ultimate price to ensure our troops had the intelligence they need. That's a noble purpose. That's what these people do. And you can see the impact. And for me, it was an honor and privilege to work with these folks. The time and the effort that they spent, our discussions with General Dave Petraeus, General Stan McChrystal, Ray Odierno, Lloyd Austin and Admiral Bill McRaven -- our job was to provide that intelligence that they need and the timeliness that they needed it to help them go after the adversary. And you can see the significant drop that occurred as we implemented those capabilities in Iraq and our troops went forward.

This is absolutely superb. The mindset of these people is foreign intelligence to save lives -- our lives, our military, our civilian. That is a true noble effort. And those are the types of people I have the great honor and privilege to lead. But the discussion today has to take that next step -- well, what about counterterrorism? And what do we do about the discussion that I put on the table, from the World Trade Center in 1993 to 9/11? What now?

We failed to connect the dots. And so, we had to come up with a way of helping to stop the attack. Our government -- Congress, the Administration and the courts -- all joined together to come up with programs that would meet our Constitution and help us connect those dots.

I think it's important to understand the strict oversight that goes into these programs because the assumption is that people are out there just wheeling and dealing; and nothing could be further from the truth. We have tremendous oversight and compliance in these programs, auditability. And for many of you with the technical background that work netflow and other things like that, you know that we can audit the actions of our people, a hundred percent in this case. And we do that.

But this information and the way our country has put it together is something that we should also put forward as an example for the rest of the world, because what comes out is we're collecting everything. That is not true. What we're doing is for foreign intelligence purposes to go after counterterrorism, counterproliferation, cyberattacks. And it's focused. And if you think about netflow and the amount of information, you couldn't afford -- we don't want to collect everything. It makes your analysis harder. If your intent is to go after terrorists, how do you do that? And so there are two programs that we have here: a metadata program, one that helps us connect the dots in the least intrusive way that we can; and FAA 702 or Section 702 authority, which allows us to go after content. I'm going to go into each of these in detail.

But I wanted to put out one thing that's important. Industry just doesn't dump stuff to us and say, "Hey, here's some interesting facts." They are compelled by a court order to comply. They are compelled by a court order to comply where all three branches of our government have come together; think about the lawful intercept program that we have here.

I think this is a standard for other countries because we have the court overseeing it; we have Congress overseeing it; and we have the Administration, and I'll go into all the different parts of the Administration that oversees that.

And I've heard some people say that the court is a rubber stamp. I'm on the other end of that table with federal judges. And anybody here who's been up against a federal judge knows that these are people with tremendous legal experience that don't take any -- I'm trying to think of a word here -- from even a four-star general. They want to make sure that what we're doing comports with the Constitution and the law. And they are dead serious on it. These are folks that have given their whole lives to our nation's judiciary system. These are folks who know they're probably not going to go to the Supreme Court, but they want to do something for our nation. These are tremendous judges. They aren't a rubber stamp. And I've been in front of that court a number of times. I can tell you from the wire-brushings[2] that I've received -- they are not a rubber stamp.

Let's go into the details of -- of these programs. (Press the button.)

I thought it would be important to give you a picture of what our analysts actually see. There it is, on the right hand side. This is for counterterrorism purposes, a program that is designed to go after communications of foreign terrorist organizations to help us connect those dots from a foreign actor to someone who may be in the United States trying to do us harm. This program was designed specifically to help us go after that Mihdhar case. I think it's important to have some of the facts on the table here and for me to give you more of those, more facts.

First, as you can see, what you have is the date-time of the call, the calling number, and the called number, the duration of the call, and we also put in the origin of the metadata data. And you can see it says "Business Record[s] FISA," just as another case, because our analysts who work this -- that's a flag for them that says "heads-up" -- this is important court data. This does not include the content of communications. This does not include your phone calls or mine, your emails nor mine, your SMS messages. There is no content. There are no names in the database, no address, no credit card numbers; and no locational information is used.

Let me give you an example of how this was important, how the foreign intelligence agencies, like CIA and NSA worked with FBI to help stop terrorist activities. And this actually was given out publicly -- Basaaly Moalin, a terrorist who was in California.

We had an intercept of a communications in Somalia -- a phone number of a person talking about terrorist activities, and that phone number, based on what they were talking about, allowed us to look into the database. What does that mean? The database is like a lockbox. The controls that go on this database are greater than any data repository in government, and the oversight is the same. To get a number approved, there are only 22 people at NSA that can approve that number. They have to prove that that meets the standards set by the court, that this has that counterterrorism nexus with al-Qaida-related groups.

Then and only then is that number added to a list that can be queried. Only those numbers on that list can be queried into that database. If you mistype a number, the database will reject it, because it has to be on that list. Only 35 analysts at NSA are authorized to run queries. They have to go through three separate different training regimen and pass tests to do -- to actually do queries into that database.

In 2012, there were less than 300 numbers approved -- bless you [to audience member who sneezed] -- approved for queries -- less than 300 numbers. Those queries resulted in 12 reports to the FBI. Those reports contained less than 500 numbers -- not millions, not hundreds of thousands, not tens of thousands -- less than 500. The intent of this program was to find a terrorist actor and identify that to the FBI.

If you think about it, the FBI is a great agency. Director Bob Mueller is one of the greatest people I've ever met. His agency does tremendous work for this country. Our job is not to complicate his life by giving him as many numbers as we can. Our job is to help him focus on the right numbers. And the number that we gave him in California -- they had actually had -- we gave that to them in 2007. In 2004, they had run an investigation on that individual, but did not have enough information to open up a full field investigation, so they closed that investigation down.

In 2007, with the number we gave them, they had enough information. They take that number -- and now their portion of this is they can take a national security letter, find out who that number belongs to, and they found out it was Basaaly Moalin. They can then, with probable cause, get a warrant. NSA only has the fact of a number. FBI can take that, see where it connects to, use a national security letter and the legal authorities given to them to take the next step. That resulted in the capture of Basaaly Moalin for a material support for terrorism and several co-conspirators.

The other program that I would like to talk to is the one we refer to sometimes as PRISM, but PRISM is part of it. It's the FAA 702 authority. This is for foreign intelligence purposes. This is content. This is not targeting U.S. persons. This is targeting threats overseas. This is our lawful intercept program, which is analogous to many other countries around the world. They compel service providers to provide information just as we do. But I mentioned earlier, we have, I believe, a great standard, when we look at the court, Congress, and the Administration all looking at what we do on each of these. I should mention on the previous slide, a hundred percent auditability.

So let me just go back to that. I didn't -- I didn't give you that part, and I promised I would, so I don't want you to think I left that out. ("A hundred percent auditability. Well, that was quick. So maybe they -- there is a no going back.") So on this program, a hundred percent auditability on every query that we make. And that is overseen by our inspector general, our general counsel. In 2009, in our discussions with the President, when he first came on board, we talked to him about these programs. And the issue was, how do we know the compliance is there and what more could we do?

We stood up, working with the committees in Congress, a directorate of compliance. This directorate of compliance was headed by legal professionals and information specialists that can look at everything that we do in these programs and ensure they comport with the court orders. But we also have oversight from the Director of National Intelligence, general counsel and IG from the Defense Department, from the Department of Justice, from the White House, from Congress (the Intel Committees), and from the courts. Our people have to take courses and pass exams to use this data.

So the same level of control is given to the FAA 702 data. In fact, this is the one that at times people say, "They're listening to all our communications." That is not authorized under this. But the issue would be, for me standing me up here, many are going to say, "Well, I hear what you're saying, but I don't trust that." Congress did a review of this program over a four-year period, the Senate Select Committee on Intelligence. And over that four-year period, they found no willful or knowledgeable violations of the law or the intent of the law in this program. More specifically, they found no one at NSA had ever gone outside the boundaries of what we've been given.

That's the fact. What you're hearing, what you're seeing, what people are saying is, "Well, they could." The fact is, they don't. And if they did, our auditing tools would detect them, and they would be held accountable. And they know that from the courses that they take and the pledge that they've made to this nation. And they take that very seriously. Remember, their intent is not to go after our communications. Their intent is to find the terrorist that walks among us.

How do we do that?

So we have two programs that help us do that. One is on metadata, the least intrusive measure that we could figure out -- and that's something that we should discuss -- that allows us to hone in and give the FBI greater insights into these actors. And we have this content program -- again, audited. Again, our people that go through this have to go through these courses and pass those tests. There are allegations out there that they listen to all our emails; they do all these things. That's wrong. We don't. And if we did, we would be held accountable -- a hundred percent auditability on what we do here.

At times I look at that and say, "Is this too much?" Our people say it's the right thing to do. The nation needs to know we're going to do the right thing. We comply with the court orders and do this exactly right, and if we make a mistake, we hold ourselves accountable and report it to everyone.

I want to give you an example of what this means to us, what this means to our nation. I'm going to talk about the Zazi case, or the New York City subway bombing, because I think it's important for you to understand how these programs come together.

NSA, CIA, our foreign intelligence agencies, our allies, have good ways to go after terrorists. One of those was an al-Qaida operative operating out of Pakistan, and we had insights to some of his communications and what he was doing.

We took his name, and through the 702 court, compelled one of the service providers to give us the content of his communications -- his email. In those emails, we saw him working with an individual unknown to us, discussing an imminent terrorist attack. All we knew [is] they were looking for the recipes for bombs. We had an email address, and in the email was a phone number. We didn't know if the phone number was U.S. or overseas.

We gave the email address to the FBI. Again, the FBI has legal authorities then to take that email address and find out whose address is this. And this was Najibullah Zazi, a terrorist in Colorado. And they told us that the phone number that was in that email was his. We used that phone number to go into the business records, FISA data, because it had nexus to an al-Qaida-related operation. We found the first connection from that phone number in Colorado to a[n] unknown phone number to the FBI in New York City. But the important thing was that phone number in New York City also was talking to another terrorist-related actor, in another layer out, to yet another terrorist. That helped us tell the FBI that number in New York City is really important. That number was Adis Medunjajin.

Time was of the essence in this case. You may recall that Zazi was driving across the country to conduct the attack. We intercepted this around the sixth of September and the attack was supposed to occur by 14 September. The FBI has to put these pieces together based on our input, what they get from customs and border patrol, what they get from other intelligence agencies and law enforcement, and figure out what's going down. They are superb; they stopped this attack. This would have been the biggest attack in the United States since 9/11. It came -- the initial tip came -- from the PRISM FAA 702 data. And Business Record FISA is a tool that also adds value, but it can only add value in the United States.

So what does that mean? What have these capabilities done? We have talked about 54 different terrorist-related activities. I've put them up here so that you can see what we've been able to do. These are facts. This is a partnership between our foreign intelligence agencies and the FBI, between our country and our allies. We stopped 13 related terrorist activities in the United States and 25 more in Europe.

There are a number of things that comes out of this slide. First, the Business Record FISA can only help in those that are in the United States. It had a role in 12 of those 13. In four, it came up with no results that was operation -- of operational value to the FBI. In the other eight, it provided leads for the FBI to go after. FAA 702 provides value across 53 of these, and in roughly half of them it was the initial tip. Our nation takes stopping terrorism as one of the most important things.

Audience Member: Freedom!

General Alexander: Exactly. And with that, when you think about it, how do we do that? Because, we stand for freedom.

Audience Member: Bull&%^#!

General Alexander: Not that. But I think what you're saying is that in these cases, what's the decision? Where's the discussion? And what tools should we have to stop those?

Audience Member: No, I'm saying I don't trust you!

Audience Member: You lied to Congress. Why -- Why would we believe you're not lying to us right now?

General Alexander: I haven't lied to Congress.

Audience Member: What about [unclear], congressional testimony?

Conference Staff Member: Wait for the question session.

General Alexander: Thank you for that. But I do think this is important for us to have this discussion, because in my opinion, what you quickly believe is that which is written in the press without looking at the facts. This is the greatest technical center of gravity in the world. I ask that you all look at those facts -- check that out. Read the congressional testimony. Look at what we're talking about here, because this is our nation's future. This is what we've done with these programs and in my opinion, that's not "bull." Those are facts.

And what we see coming at our country is more of the same. So the question that we have with all of us, so what do we do? Let's begin that discussion. We ought to put the facts on the table and have that discussion, so that people who are revealing information that can hurt the future of this country and our citizens -- I believe that is irresponsible and will have significant damage to our country. How do we defend this country? That's the question. What you're asking us to do is to defend the country. And you take an oath to that Constitution, and we take that very seriously. It's not either/or. It's both.

And so here, if you want to be constructive, if you want to help get this right, be part of that discussion. Put the facts on the table. That's what we need. You need to understand what we're trying to do to defend the country and protect civil liberties and privacy. On the Business Record[s] FISA, 15 judges have approved that 34 times. Congress, the courts, and the Administrations have looked at it. This morning, the director of national intelligence declassified some of those. Review that. See what we do in going after these.

So with that, I'd like to open it up for questions.

Audience Member: So obviously you have a lot of intelligence capabilities...but why do so many countries in the world want to attack us?

Mr. Trey Ford: Forgive me, guys. Generally speaking, you -- you provide the keynote the opportunity to determine if he wants to accept questions from the audience or to receive them in an organized manner. We reached out to the community to try to gather those, to organize those. We weighted them. We ranked them. This is not canned. The General doesn't know what we're throwing at him, but I want to make sure that we're asking your questions for you. We've got a very limited amount of time.

General Alexander: If -- If I could, though.

Mr. Ford: Please...it's yours.

General Alexander: You know, I have no problem with the questions because I think that's a great question. Why --

Audience Member: Repeat.

Mr. Ford: Could you repeat the question?

General Alexander: So the question that was asked was, "So why do countries want to attack us?" Why does al-Qaida want to attack us? Why do we stand in the way of them reaching their objective? And I think you should look at what they're trying to create: a caliphate. They believe that the Middle East should be run under the Islamic law, sharia form of law, and that everybody should comply with that form of law; and that we, the United States, working in the Middle East, have stood in their way. They want to attack us.

Audience Member: They want to attack us because we're bombing them!

General Alexander: Go ahead [to Mr. Ford]. So -- So it is...interesting that when you look at it, go back to the facts of '93: the World Trade Center, the Cole,. Look at the East African embassy bombings. Look at 9/11. And so that's what we face. Go ahead [to Mr. Ford].

Mr. Ford: General, the top rated question was question number seven on the survey: Do you think our national security intelligence and monitoring initiatives negatively impacts our innovative domestic capabilities ability -- companies' ability to adequately grow in foreign markets over fears of back doors or covert access? More directly, is the NSA making U.S. companies less competitive?

General Alexander: That's a great question. So the -- from my perspective, I think it's important that we put the facts on the table of what a lawful intercept is and what these companies are compelled to comply with. And every country has lawful intercept -- or almost every country has lawful intercept programs that compel companies to provide information. The difference, from my perspective, is the oversight by the courts, Congress, and the Administration in ensuring that we do this right. Go ahead [to Mr. Ford].

Mr. Ford: There was a great question posed yesterday. I would like to echo that. There is a clear difference between the NSA cannot and the NSA will not. It's a discretionary or it's a preventative control?

General Alexander: So there are both. I think there are technical things that we can do to limit our collection. And we do that. In the United States, if you think about netflow and what do you, perhaps, in securing a network, how you look at different parts, you can shield off certain parts from collecting netflow data. We do the same thing to ensure we comply with the law. So the domestic communications we can technically take on. But there has to be another set of standards because the reality is communications often times are international. What happens if we run into a U.S. person's communications? So part of what it has been recently released talks about the minimization procedures, the training that everyone at NSA has to go through if we run across those communications. And we hold our people accountable to doing that exactly right.

Mr. Ford: One question that came up a lot out of band was, once a classified document is publicly leaked, as in the case of the PRISM documents, why does the classification remain the same? Why can't government employees look at the Internet?

General Alexander: Well -- Well, there's two reasons on that one. I think the issue is on this, how do we protect our nation? How do we defend it? You know, some of this is classified. It's not classified to keep it from you, a good person. It's classified because sitting among you are people who wish us harm. If we tell everybody exactly what we're doing then the adversaries will know how to get through our defenses. That's why I believe that what has happened, the damage to our country is significant and irreversible. What we're talking about is future terrorist attacks. And when you look on this slide [#9] here, will we have the success over the next 10 years that we've had over the last? And I think it is worth considering what would have happened in the world if those attacks -- 42 of those 54 were terrorist plots -- if they were successfully executed, what would that mean to our civil liberties and privacy? So those are issues. Now, why do we classify -- thank you [to audience]. Go ahead [to Mr. Ford]

Mr. Ford: General, I know the NSA doesn't shop where we do. Our attendees here at Black Hat have a certain cadre of tools in our arsenal for defense. Our adversaries are well-read, well-steeped, have access to our tools and means. We appreciate the glimpse into what the NSA is doing -- and I know you can't share more -- but I would like you to speak to your -- your position on whether or not these media leaks have affected the NSA.

General Alexander: Well, it has, you know, and I think you can hear it from some of the comments that we've gotten here, the sporadic comments. You see, think about people who are willing to go forward to Iraq and Afghanistan to help insure our Soldiers, Sailors, Airmen, Marine[s], and the civilians get the intelligence that they need. I believe these are the most noble people that we have in this country. They are willing to put their lives on the line for their fellow -- for their fellow soldiers and fellow Americans, and other countries. And 20 of them lost their lives. And when you think about that, the issue is, these same people who take that same oath to uphold and defend the Constitution are the ones that run these programs. And we get all these allegations of what they could be doing. But when people check, like the Intelligence Committee, they found zero times that's happened. And that's no bullshit. Those are facts. (Please don't put that out in open press -- just that one word. I have 15 grandchildren.)

Mr. Ford: Alright, one more question before we break, General. In a moment, I'm going to talk to my mom and dad. And I just want to know, your people can't listen to me call my mom, right?

General Alexander: That's correct.

Mr. Ford: Okay.

General Alexander: And now there's two parts to that. You --

Mr. Ford: That's a yes or no question!

General Alexander: And...I think...it's one....Here's the issue if you put that out there. We have technical controls to limit that. And then we have policy. So the technical is they can't. You know, I asked the same thing about my daughters. I have four daughters. Can I go and intercept their emails? No. And...the reason --

Mr. Ford: Can you [to audience]?

General Alexander: You may be able to [to audience]. But -- But the technical limitations are in there. Now, people who try to circumvent that, there is also a hundred percent auditing. So when you put in my daughter at "x.com," and an auditor then looks and says, "What's the foreign intelligence purpose of this query?" And the analyst putting that in has to state that and show that what they're doing meets that standard.

Audience Member: Isn't Trey a terrorist? You're at Black Hat.

Mr. Ford: Thanks [facetiously].

General Alexander: Trey's a good person. No terror -- well, I guess; I hope -- No terrorist associate.

General Alexander: So -- So the issue really becomes, the issue that I would ask you to look at and all of those that find what we're doing that should be limited more, my comment is help us defend the country and come up with a better solution. You're the greatest gathering of technical talent anywhere in the world. If we can make this better, the whole reason I came here was to ask you to help us make it better. And if you disagree with what we're doing, then you should help twice as much.

Audience Member: Read the Constitution!

General Alexander: I have. You should, too.

Mr. Ford: General, I -- I know it would have been a lot easier to not come. Black Hat is a warm, loving crowd that loves, you know, guests in a different way -- but thank you so much for coming out.

General Alexander: Thank you.

[1] Real Time Regional Gateway

[2] *Wire-brushing* refers to a verbal harangue; a "chewing out"