UNITED STATES DEPARTMENT OF DEFENSE

INTERVIEW WITH RICHARD LEDGETT, JR.
TED MODERATOR CHRIS ANDERSON

Washington, D.C.
Wednesday, March 20, 2014
MR. ANDERSON: We had Edward Snowden here a couple days ago and this is response time. And several of you have written to me with questions to ask our guest here today from the NSA. So Richard Ledgett is the 15th Deputy Director of the National Security Agency and he’s the senior civilian officer there, acts as its Chief Operating Officer guiding strategies, setting internal policies and serving as principal advisor to the Director. And all being well, welcome Rick Ledgett to TED.

Applause

MR. LEDGETT: I’m really thankful for the opportunity to talk to folks here. I look forward to the conversation. Thanks for arranging for that.

MR. ANDERSON: Thank you Rick, we appreciate you joining us, it’s certainly quite a strong statement that the NSA is willing to reach out and show a more open face here. You saw, I think, the talk and interview Edward Snowden gave a few days ago. What did you make of it?

MR. LEDGETT: So I think it was interesting, it was … we didn’t realize that he was going to show up there so kudos to you guys for arranging a nice surprise like that. I think that like a lot of the things that have come out since Mr. Snowden starting disclosing classified information, there were some kernels of truth in there but a lot extrapolations and half-truths in there and I’m interested in helping to address those. I think this is a really important conversation that we’re having in the United States and internationally and I think it is important and of import and so given that we need to have that be a fact based conversation and we want to help make that happen.

MR. ANDERSON: So, the question that a lot of people have is what do you make of Snowden’s motivations for doing what he did and did he have an alternative way he could have gone?

MR. LEDGETT: He absolutely did have alternatives, ways he could have gone and I actually think that characterizing him as a whistleblower actually hurts legitimate whistleblowing activities. So what if somebody who works in NSA and there are over 35,000 who do, they are all great citizens, they are like your husbands, fathers, sisters, brothers, neighbors, friends and relatives, all who are interested in doing the right thing for their country and for our allies internationally. And so there are a variety of venues to address if folks have a concern. First off there’s their supervisor and up through the supervisory chain
within their organization. If folks aren’t comfortable with that there are a number of Inspectors General. In the case of Mr. Snowden, he had the option of the NSA Inspector General, the Navy Inspector General, the Pacific Command Inspector General, the Department of Defense Inspector General, and the Intelligence Community Inspector General, any of whom would have both kept his concerns in classified channels and been happy to address them.

MR. ANDERSON: He has said sir, that working as a contractor

MR. LEDGETT: He had options to go to the Congressional committees and there are mechanisms to do that that are in place so he didn’t do any of those things.

MR. ANDERSON: Now, you had said that Ed Snowden had other avenues for raising his concerns. The come back on that is a couple things, one, that he certainly believes that as a contractor, the avenues that would have been available to him as an employee weren’t available, two, you know, that there’s a track record of other whistle blowers like Drake and Drake being treated pretty harshly by some views. And thirdly, what he was taking on was not one specific kind of flaw that he had discovered, but programs that had been approved by all three branches of government.

I mean, in that circumstance, couldn’t you argue that what he did was reasonable?

MR. LEDGETT: No, I don’t agree with that. I think that the -- his -- sorry, I’m getting feedback through the microphone there. The actions that he took were inappropriate because of the fact that he put peoples’ lives at risk, basically, in the long run, and I know there’s been a lot of talk in the public by Mr. Snowden and some of the journalists that say that the things that have been disclosed have not put national security and people at risk, and that is categorically not true, they actually do.

I think there’s also an amazing arrogance to the idea that he knows better than the framers of the Constitution in how the government should be designed and work for separation of powers and the fact that the executive and the judicial or the executive and the legislative branch have to work together and they have checks and balances on each other, and then the judicial branch, which oversees the entire process, I think that’s extremely arrogant on his part.

MR. ANDERSON: Can you give a specific example of how he put peoples lives at risk?
MR. LEDGETT: Yeah, sure. So, the things that he’s disclosed, the capabilities, and NSA is a capabilities-based organization, so when we have foreign intelligence targets, legitimate things of interest, like terrorists is the iconic example, but it includes things like human traffickers, drug traffickers, people who are trying to build, you know, advanced weaponry, nuclear weapons and build delivery systems for those, and nation states who might be executing aggression against their immediate neighbors, which you may have some visibility in some of that that’s going on right now, the capabilities are applied in a very discreet and measured and controlled ways. So, the unconstrained disclosure of those capabilities means that as adversaries see them and recognize, hey, I might be vulnerable to this, they move away from that.

And we have seen targets in terrorism, in the nation state area, in smugglers of various types and other folks who have, because of the disclosures, moved away from our ability to have insight into what they’re doing. The net effect of that is that our people, who are overseas in dangerous places, whether they’re diplomats or military, and our allies who are in similar situations, are at greater risk because we don’t see the threats that are coming their way.

MR. ANDERSON: So, that’s a general response saying that because of his revelations, access that you had to certain types of information has been shut down, has been closed down, but that presumes -- I mean, the concern is that the nature of that access was not necessarily legitimate in the first place. I mean, describe to us this bull run program where it’s alleged that the NSA specifically weakened security in order to get the type of access that you’ve spoken of.

MR. LEDGETT: So, there are -- when our legitimate foreign intelligence targets of the type I described before use the global telecommunication system as their (inaudible) methodology, and they do, because it’s a great system, it’s the most complex system ever devised by man, and it is a wonder and lots of folks in the room there are responsible for the creation and enhancement of that and it’s just a wonderful, wonderful thing, but it’s also used by people who are working against us and our allies and so if I’m going to pursue them, I need to have the capability to go after them.

And, again, the controls are in how I apply that capability, not that I have the capability itself. Otherwise, if we could make it so that all the bad guys used one corner of the Internet, we could have a domain, badguy.com, that would be awesome and we could just concentrate all our efforts there. That’s not how it works. They’re trying to hide from the government’s ability to isolate and interdict their actions, and so we have to swim in that same space.

But I will tell you this, so NSA has two missions, one is the Signals Intelligence mission that we’ve, unfortunately, read so much about in the press, the other one is the Information Assurance mission, which is to protect the
national security systems of the United States. And by that, that’s things like the communications that the President uses, the communications that control our nuclear weapons, the communications that our military uses around the world, and the communications that we use with our allies, and that some of our allies themselves use.

And so we make recommendations on standards to use and we use those same standards, and so we are invested in making sure that those communications are secure for their intended purposes.

MR. ANDERSON: It sounds like what you’re saying is that when it comes to the Internet-at-large, any kind of strategy is fair game if it improves America’s safety, and I think this is partly where there’s such a divide of opinion, that there’s a lot of people in this room and around the world who think very differently about the Internet. They think of it as a momentous invention of humanity, kind of on a par with the Guttenberg Press, for example. It’s the bringer of knowledge to all, it’s the connector of all, and it’s viewed in those sort of idealistic terms.

And from that lens, what the NSA has done is equivalent to the authorities back in Germany, inserting some device into every printing press that would reveal which books people bought and what they read. Can you understand that from that viewpoint it feels outrageous?

MR. LEDGETT: I do understand that. I actually share the view of the utility of the Internet and I would argue it’s bigger than the Internet, it is the global telecommunications system. The Internet is a big chunk of that, but there is a lot more, and I think that people have legitimate concerns about the balance between transparency and secrecy, that’s sort of been couched as a balance between security and -- I mean, between privacy and national security. I don’t think that’s the right framing. I think it really is transparency and secrecy.

And so that’s the national and international conversation that we’re having and we want to participate in that and want people to participate in an informed way.

So, there are things -- let me talk to that just a little bit more -- there are things that we need to be transparent about -- our authorities, our processes, our oversight, who we are. We, NSA, have not done a good job of that and I think that’s part of the reason that this is so -- has been so revelational and so sensational in the media. Nobody knew who we were, we were the “No Such Agency” the “Never Say Anything”.

You know, there’s take-offs of our logo of an eagle with headphones on -- around it, and so that’s sort of the public characterization. And so we need to be more transparent about those things. What we don’t need to be transparent about, because it’s bad for the U.S., it’s bad for all those other countries that we work
with and that we help provide information that helps them secure themselves and their people, it’s bad to expose operations and capabilities in a way that allows the people that we’re all working against, the generally recognized bad guys, to counter those.

MR. ANDERSON: Isn’t it also bad to deal a kind of body blow to the American companies that have essentially given the world most of the Internet services that matter?

MR. LEDGETT: It is. It’s really the -- the companies are in a tough position, as are we, because the companies -- you know, we compel them to provide information, just like every other nation in the world does. Every industrialized nation in the world has a lawful intercept program where they are requiring companies to provide them with information that they need for their security, and the companies that are involved have complied with those programs in the same way that they have to do when they’re operating in Russia or the UK or China or India or, you know, France, any country you choose to name.

And so the fact that these revelations have been sort of broadly characterized as “you can’t trust company A because your privacy is suspect with them” is actually only accurate in the sense that it’s accurate with every other company in the world that deals with any of those countries in the world. And so, it’s being picked up by people as a marketing advantage and it’s being marketed that way by several countries, including in some of our allied countries where they are saying, hey, you can’t trust the U.S., but you can trust our telecom company because we’re safe.

And they’re actually using that to counter the very large technological edge that U.S. companies have in areas like the cloud and Internet-based technologies.

MR. ANDERSON: You’re sitting there with the American flag and, you know, the American Constitution guarantees freedom from unreasonable search and seizure. How do you characterize the American citizen’s right to privacy? Is there such a right?

MR. LEDGETT: Yeah, of course there is. I think that -- and we devote an inordinate amount of time and pressure -- inordinate and appropriate, actually, I should say -- amount of time and effort in order to ensure that we protect that privacy and, beyond that, the privacy of citizens around the world. It’s not just Americans.

You know, several things come into play here. First, we’re all on the same network. My communications, I’m a user of a particular Internet email service that is the number one email service of choice by terrorists around the
world, number one, and so I’m there right beside them in email space in the Internet. And so, we mean to be able to pick that apart and find the information that’s relevant.

In doing so, we’re going to necessarily encounter Americans and innocent foreign citizens who are just going about their business and so we have procedures in place that shreds that out, that says, okay, when you find that -- not if you find it -- when you find it, because you’re certain to find it, here’s how you protect that. These are called minimization procedures, they’re approved by the Attorney General and Constitutionally based, and so we protect those. And then for people -- you know, citizens of the world who are going about their lawful business on a day-to-day basis, the President, in his 17 January speech, laid out some additional protections that we are providing to them.

So, I think, absolutely, folks do have a right to privacy and we work very hard to make sure that that right to privacy is protected.

MR. ANDERSON: What about foreigners using American companies Internet services? Do they have any privacy rights?

MR. LEDGETT: They do. They do, in the sense of the only way that we are able to compel one of those companies to provide us information is when it falls into one of three categories -- we can identify that this particular person, identified by a selector of some kind, is associated with a counterterrorist or proliferation or other foreign intelligence target.

MR. ANDERSON: Much has been made of the fact that a lot of the information that you’ve obtained through these programs is essentially metadata. It’s not necessarily the actual words that someone has written in an email or given on a phone call, it’s who they wrote to and when and so forth. But it’s been argued, and someone here in the audience has talked to a former NSA analyst who said, metadata is actually much more invasive than the core data, because in the core data you present yourself as you want to be presented. With metadata, who knows what the conclusions are that are drawn. Is there anything to that?

MR. LEDGETT: I don’t really understand that argument. I think that metadata is important for a couple of reasons. Metadata is the information that lets you find connections that people are trying to hide. So, when a terrorist is corresponding with somebody else who’s not known to us but is engaged in doing or supporting terrorist activity, or someone who’s violating international sanctions by providing a nuclear weapons-related material to a country like Iran or North Korea, is trying to hide that activity because it’s illicit activity.
What metadata lets you do is connect that. The alternative to that is one that’s much less efficient and much more invasive of privacy, which is gigantic amounts of content collection. So, metadata, in that sense, actually is privacy enhancing.

We don’t, contrary to some of the stuff that’s been printed, we don’t sit there and grind out metadata profiles of average people. If you’re not connected to one of those valid intelligence targets, you are not of interest to us.

MR. ANDERSON: So, in terms of the threats that face America overall, where would you place terrorism?

MR. LEDGETT: I think terrorism is still number one. I think that, you know, we have never been in a time where there are more places where things are going badly and forming the Petri dish in which terrorists take advantage of the lack of governance. An old boss of mine, Tom Fargo, Admiral Fargo, used to describe it as arcs of instability, and so you have a lot of those arcs of instability in the world right now, places like Syria where there’s a civil war going on and you have massive numbers, thousands and thousands of foreign fighters who are coming into Syria to learn how to be terrorists and practice at activity and lots of those people are Westerners who are -- who hold passports to, you know, European countries or in some cases the United States, and so they are basically learning how to do jihad and have expressed intent to go out and do that later on in their home countries.

You’ve got places like Iraq, which is suffering from a high level of sectarian violence, again a breeding ground for terrorism, and you have the activity in the Horn of Africa and in the Sahel area of Africa, again, lots of weak governance which forms a breeding ground for terrorist activity.

So, I think these very serious things number one, I think number two is cyber threat. Cyber is a threat in three ways. One way, and probably the most common with your people have heard about it is the theft of intellectual property. So, basically, foreign countries going in, stealing companies’ secrets, and then providing that information to state-owned enterprises or companies connected to the government to help them leapfrog technology or to gain business intelligence that’s then used to win contracts overseas.

That is a hugely costly set of activities that’s going on right now. Several nation states are doing it.

Second is the denial of service attacks. You’re probably aware that there had been a spate of those directed against the U.S. financial sector since 2012. Again, that’s a nation state who’s executing those attacks and they’re doing that as a semi-anonymous way of reprisal.

And the last one is destructive attacks, and those are the ones that concern me the most. Those are on the rise. You had the attack against Saudi Aramco in
2012, August of 2012. It took down about 35,000 of their computers with a wiper-style virus. You had a follow on a week later to a Qatari company. You had March of 2013, you had a South Korean attack that we’ve attributed in the press to North Korea that took out thousands of computers. Those are on the rise and we see people expressing interest in those capabilities and a desire to employ them.

MR. ANDERSON: Okay, so a couple things here, because this is really the core of this almost. I mean, first of all, a lot of people who look at risk, who look at the numbers, don’t understand this belief that terrorism is still the number one threat. You know, apart from September 11, I think the numbers are in the last 30 or 40 years about 500 Americans have died from terrorism, mostly from homegrown terrorists.

The chance in the last few years of being killed by terrorism is less than -- far less than the chance of being killed by lightning. I guess you would say that a single nuclear incident or bioterrorism act or something like that would change those numbers. Would that be the point of view?

MR. LEDGETT: Well, I’d say two things, one is, the reason that there hasn’t been a major attack in the United States, that is not an accident. That’s a lot of hard work that we have done, that other folks in the intelligence community have done, that the military has done, and that our allies around the globe have done.

You’ve heard the numbers about the tip of the iceberg in terms of numbers of terrorist attacks that NSA programs contributed to stopping was 54, 25 of those in Europe, and of those 25, 18 of them occurred in three countries, some of which are our allies, and some of which are beeping the heck out of us over the NSA programs, by the way.

So, that’s not an accident that those things happen. That’s hard work. That’s us finding intelligence on terrorist activities and interdicting them in one way or another, through law enforcement, through cooperative activities with other countries and sometimes through military action.

The other thing I would say is that your idea of nuclear or chem bio threat is not at all farfetched and, in fact, there are a number of groups who have, for several years, expressed interest and desire in obtaining those capabilities and work towards that.

MR. ANDERSON: It’s also been said that of those 54 alleged incidents that as few as zero of them are actually anything to do with these controversial programs that Mr. Snowden revealed. It was basically through other forms of intelligence that your -- you know, you’re looking for a needle in a haystack and the effect of these programs, these controversial programs, is just to add hay to the
stack, not to really find the needle. The needle was found by other methods. Isn’t that -- isn’t there something to that?

MR. LEDGETT: No, that’s actually -- there are two programs that are typically implicated in that discussion, one is the Section 215 Program, the U.S. Telephony Metadata Program, and the other one is popularly called the PRISM Program. It’s actually Section 702 of the FISA Amendment Act. But the 215 Program is only relevant to threats that are directed against the United States and there have been a dozen threats where that was implicated.

Now, what you’ll see people say publicly is there’s no “but for” case, and so there’s no case where but for that, the threat would have happened. But that actually indicates a lack of understanding of how investigations -- terrorist investigations actually work.

If you think about on television, you watch a murder mystery. What do you start with? You start with a body and then they work their way from there to solve the crime. We’re actually starting well before that, hopefully before there are any bodies, and we’re trying to build the case for who the people are, what they’re trying to do, and that involves massive amounts of information. Think of it as a mosaic. And it’s hard to say that any one piece of a mosaic was necessary to building the mosaic, but to build the complete picture, you need to have all the pieces of information.

On the other, the non-U.S. related threats out of those 54, the other 41 of them or 42 of them, the PRISM program was hugely relevant to that and in fact was material in contributing to stopping those attacks.

MR. ANDERSON: Snowden said two days ago that terrorism has always been what is called in the intelligence world, “a cover for action”, that it’s something that, you know, because it evokes such a powerful emotional response in people, it allows the initiation of these programs to achieve powers that an organization like yours couldn’t otherwise have. Is there any internal debate about that?

MR. LEDGETT: Yeah, I mean, we debate these things all the time and there is discussion that goes on at the -- in the executive branch and within NSA itself and the intelligence community about what’s right, what’s proportionate, what’s the correct thing to do. It’s important to note that the programs that we’re talking about were all authorized by two different presidents, two different political parties, by Congress twice, and by federal judges 16 different times.

And so, it’s not a -- this is not NSA running off and doing its own things, this is a legitimate activity of the United States foreign government that was agreed to by all the branches of the United States government, and President Madison would have been proud.
MR. ANDERSON: And yet when Congressmen discovered what was actually being done with that authorization, many of them were completely shocked. Or do you think that is not a legitimate reaction that certainly because it’s now come out publicly that they really knew exactly what you were doing with the powers they had granted you?

MR. LEDGETT: So, Congress is a big body. There’s 535 of them and they change out frequently in the case of the House every two years, and I think that the NSA provided all the relevant information to our oversight committees and then the dissemination of that information by the oversight committees throughout Congress is something that they manage.

I think I would say that Congress members had the opportunity to make themselves aware and, in fact, a significant number of them, the ones who are assigned oversight responsibility, did have visibility of that and you’ve actually had the chairs of those committees say that in public.

MR. ANDERSON: Now, you’ve mentioned the threat of cyber attacks and I don’t think anyone in this room would disagree that it is a huge concern, but do you accept that there’s a trade off between offensive and defensive strategies and that it’s possible that they very measures taken to “weaken encryption” and allow yourself to find the bad guys might also open the door to forms of cyber attack?

MR. LEDGETT: So, I think that -- two things, one is you said “weaken encryption”, I didn’t, and the other one is that the NSA has both those missions and we are heavily biased towards defense, and actually the vulnerabilities that we find in the overwhelming majority of cases, we disclose to the people who are responsible for those -- for manufacturing or developing those products.

We have a great track record of that and we’re actually working on a proposal right now to be transparent and to publish transparency reports in the same way that the Internet companies are being allowed to publish transparency reports for them. We want to be more transparent about that.

So, again, we eat our own dog food. We use the standards, we use the products that we recommend, and so it’s in our interest to keep our communications protected in the same way that other peoples’ need to be.

MR. ANDERSON: Edward Snowden, when after his talk, was wondering the halls here in the bot and I heard him say to a couple people -- you know, they asked him about what he thought of the NSA overall, and he was very complementary about the people who work with you, said that it’s a really impassioned group of employees who believe -- who are seeking to do the right
thing and that they’re being -- the problems have come from just some badly conceived policies.

He came over certainly very reasonably and calmly. He didn’t come over like a crazy man. Would you accept that at least, even if you disagree with how he did it, that he has opened a debate that matters?

MR. LEDGETT: So, I think that the discussion is an important one to have. I do not like the way that he did it. I think there were a number of other ways that he could have done that that would have not endangered our people and our -- the people of other nations through losing visibility into what our adversaries are doing, but I do think it’s an important conversation.

MR. ANDERSON: I mean, it’s been reported that there’s almost a difference of opinion with you and your colleagues over any scenario in which he might be offered an amnesty deal. I think your boss, General Keith Alexander, has said that that would be a terrible example for others. You can’t negotiate with someone who’s broken the law in that way. But you’ve been quoted as saying that if Snowden could prove that he was surrendering all undisclosed documents, that a deal maybe should be considered. Do you still think that?

MR. LEDGETT: Yeah, so, actually, this is my favorite thing about that 60 Minutes interview was all the misquotes that came from that. What I actually said, in response to a question about, you know, would you entertain any discussions of, you know, mitigating action against -- and I said, yeah, it’s worth a conversation. This is something that the Attorney General of the United States and the President also actually both talked about this and I defer to the Attorney General because this is his lane, but there is a strong tradition in American jurisprudence of having discussions with people who’ve been charged with crimes in order to -- if it benefits the government, to get something out of that, that there’s always room for that kind of discussion.

So, not presupposing any outcome, but there is always room for discussion.

MR. ANDERSON: I mean, to a lay person it seems like he has certain things to offer the U.S., the government, you, others, in terms of putting things right and helping figure out a smarter policy, a smarter way forward for the future. Do you see -- has that kind of possibility been entertained at all?

MR. LEDGETT: So, that’s out of my lane. That’s not an NSA thing. That would be a Department of Justice sort of discussion. So, I’ll defer to them.
MR. ANDERSON: Rick, as Snowden ended his talk, I offered him the chance to share an idea worth spreading. What would be your idea worth spreading for this group?

MR. LEDGETT: So, I think, learn the facts. This is a really important conversation and it impacts not just NSA, not just the government, it’s you, it’s the Internet companies, I mean, the issue of privacy and personal data is much bigger than just the government, and so learn the facts, don’t rely on headlines, don’t rely on sound bites, don’t rely on one-sided conversations. So, that’s the idea, I think, worth spreading.

We have a sign in our -- a badge tab -- we wear badges at work with lanyards and if I could make a plug, my badge lanyard at work says “Dallas Cowboys”, go Dallas, and the -- I’ve just alienated half the audience, I know -- so, the lanyard that our people who work in the organization that does our cryptanalytic work have a tab that says, “Look at the data.” So, that’s the idea worth spreading. Look at the data.

MR. ANDERSON: Rick, it took a certain amount of courage, I think, actually, to come and speak openly to this group. It’s not something the NSA has done a lot of in the past, and plus the technology has been challenging. We truly appreciate you doing that and sharing in this very important conversation. Thank you so much.

(Applause)

* * * * *