https://icontherecord.tumblr.com/post/72883714923/full-transcript-nsa-deputy-director-john-inglis

Outgoing NSA Deputy Director John Inglis Interviewed on National Public Radio

January 10, 2013 [Should be 2014]

National Security Agency Deputy Director John C. “Chris” Inglis has spent most of his time recently defending the NSA from revelations by former contractor Edward Snowden. Snowden disclosed that the agency was gathering phone records of millions of Americans.

Inglis retires Friday. Before stepping down, he talked to Morning Edition co-host Steve Inskeep about running a spy agency in a democracy. Below is a transcript of the unedited audio of their conversation.

Listen to the interview via NPR’s Morning Edition.

Full Transcript:
DAVID GREENE, HOST: This is MORNING EDITION, from NPR News. I’m David Greene.

STEVE INSKEEP, HOST: And I’m Steve Inskeep. We walked, this week, into a vast building covered in reflective glass, the headquarters of the National Security Agency. We met there with John C. “Chris” Inglis. He’s the agency’s No. 2, its top civilian beneath the general who runs it, Keith Alexander. Inglis was in his final week at the NSA.

STEVE INSKEEP (HOST): OK, is it disappointing to have your final year at the NSA look like this past year has?

CHRIS INGLIS (NSA): Yes and no. Certainly yes, in terms of the shock and dismay that’s been induced in the American public, and some of the people who stand in the shoes of the American public, the Congress, about NSA. The accusations of misbehavior, which have not been borne out. That’s certainly disappointing. But given all that I have gotten from NSA, it’s been a year when I can pay back. It’s been a year when I can help reinforce the workforce.

It’s a year when I can step up and be held accountable for describing what the workforce does, describing what the mission is. And so, to that extent, I’ve been pleased that I stayed an extra year. Most deputy directors at NSA, on average, serve about three and a half years. And I’m sitting now at about seven and a half years. And so by rights, I would have left three years ago.

But we stayed, Gen. Alexander and I both stayed for a combination of reasons year by year. In the beginning of this year, we knew that we were going to head into some

financial difficulties. The nation is trying to figure its way through sequestration. There were some furloughs that were on the table for the Department of Defense. And so we decided that we would stay through this year, and I'm very glad I did.

INSKEEP: How damaging have the Snowden revelations been to this agency, in terms of its operations, its moral, anything else?

INGLIS: Well, I think you've hit it. They're damaging on several counts. First and foremost, we've revealed quite a bit through these unauthorized disclosures to our adversaries about how we express our interest in them, the means by which we might then divine some intelligence information about them. Such that those who are keenly paying attention to that might then avoid our interest. And so we can say with great confidence that terrorists and rogue nations have been paying attention and have begun to take the necessary steps to invalidate the means and methods by which we would get intelligence on them. But it also has harmed relationships between the executive branch and other components of the government.

As accusations have been made, again, in my view, most of which have been shown to be false, of activities within the executive branch that weren't fully understood or authorized by either the legislative branch or authorized by the judicial branch. And we've had to work hard to essentially understand what was true and what we have done and how we've exercised those authorities. The American public is certainly in a state of shock and dismay about what have been alleged abuses by NSA. The presidential review group recently concluded that there have been no illegalities or abuses by NSA. There are matters of policy before us, in terms of how you employ modern intelligence capabilities like we have at NSA. But I think that, you know, that's something that has to be repaired. We have to actually kind of be more transparent going forward, so the American public understands what we do, why we do it, how we do it.

And then, two, there have been some difficulties between ourselves and this nation and other nations with whom were aligned, with whom we have common interests. And we're going to have to work on repairing and restoring that. And then, finally, the private sector, which essentially is the engine of commerce driving the Internet forward. There have been many accusations hurled in their direction about what they have or haven't done. And I think, again, when it's all sorted out we'll find that they've acted very responsible. And we're going to have to work hard to repair that, their reputation not just with the American public, but their reputation with those consumers of their products and services around the world.

INSKEEP: You referred to terrorists or others taking actions to invalidate your ability to surveil them. I'd like to know what that means in practice. Because when I think about the way that people have been known to respond to revelations like this, they actually end up having to deny themselves the use of the entire global telecommunications network. I think of Osama bin Laden, who ends up hiding in a house and can only work with messengers. That's actually a significant disadvantage. Does it really damage them that much to know that someone is out there attempting to monitor them? Does it

really damage you that much to know that someone's out there?

INGLIS: Well, at the base of your question I think you're right. They must know that we would have an interest in their activities, and that they communicate about those activities. We must then, you know, use that as an opportunity to better understand them. But they don't know the precise means and methods that we might employ. It might be surprising to someone that a communication that makes its way from, say, some ungoverned space in the north of southwest Asia to a place like Yemen sometimes transits through the United States of America. It might be then be available for review by a foreign intelligence organization like the National Security Agency. We have reminded people of that time and time again across the summer. And within the Internet there are enormous number of choices that you might avail yourself of. If you don't want to use Service A, you can use Service B or Service C.

And then there are security services that you can overlay with that. Whether it's encryption or obfuscation and anonymity services, you can make use of all that to essentially hide your trail. And we've seen all of that play out, in the wake of the Snowden unauthorized disclosures.

INSKEEP: You have specific instances in which you…

INGLIS: We do.

INSKEEP: …believe that trails that you were following disappeared.

INGLIS: We do, we do. Now it's too soon to say that some of that isn't serendipity. It's the kind of natural roil that takes place in terms of the turnover of technology. Something that we were able to do might be lost because it was simply a technology transformation. And they naturally move to something else, or something that we had as a capability has slipped away from us based upon the natural roil that is technology and operational practice. But they're adding up in ways that are too numerous and too, I think, related to the disclosures to be accidental. And so, therefore, we've got a hard job ahead of us to sustain the kind of access that we have against those bona fide foreign intelligent targets that the nation must know something about.

INSKEEP: So you feel there was significant damage that you can measure from the various disclosures of programs like the metadata gathering program, of the monitoring of foreign leaders. There's been political damage to the United States, there's damage to this agency. Given the damage that has been done by the revelation of programs the NSA did in fact conduct, were those programs worth it?

INGLIS: Nations like the United States, I think all nations, essentially conduct their affairs in the larger world have to know something about the threats to their people in the territory. They would like to know something about the success or not of their foreign policies. And therefore, it continues to be worth it to invest in foreign intelligence. So it's necessary…

INSKEEP: But we're talking about specific programs. Was the metadata program, for example, has it been worth it, given that part of the cost of it is that it got disclosed eventually?

INGLIS: I think so. Well, that's a great question that we've been debating as a nation for the better part of six months. You're probably quite familiar with the testimony that I, General Alexander and others have made before Congress about the number of plots that have been thwarted by the totality of signet capabilities, intelligence capabilities that NSA brings to bear in various venues. We've described that as 54 total plots. That's, of course, not the totality of terrorist activity that we might have uncovered and exposed. But we were able to disclose in an unclassified domain, there are about 54 plots. Thirteen of those essentially had a U.S. nexus, the other 41 essentially had a nexus overseas. The vast majority of those were uncovered using what's called the 702 Authority, what has been sometimes referred to as Prism. We might for purposes in kind of a plain English way say that that's simply a lawful incept capability.

Most nations have that. That an organization like myself would be able to, upon presentation through some legitimate court authorization, presentation to a telecommunications vendor, say I'm interested in Person X, can you give me something responsive to that? So most of those are attributable to that. The 215 Authority, the metadata authority, that's a harder thing to pin down, quite frankly. I've been asked on a number of occasions, do you have a but-for case? Can you say that was the silver bullet, right, that but-for the existence of the metadata you would not have uncovered a plot? There's a candidate for that, which is the plot that was exposed in San Diego. I think we were able to essentially tell the FBI that an individual was materially involved in terrorism that they had, three years prior, investigated based on a tip and kind of laid that case to rest.

And but for the 215 Program, which we essentially tied that individual to some foreign terrorist activity overseas, the FBI would have let that case lain fallow for quite sometime. Now I cannot tell you that that wouldn't have turned up some other way. There wouldn't have been some other tool in the tool kit. And so here's the thing about the 215 or the telephone metadata program. It was precisely defined to cover a seam exposed in the 9/11 terrorist attacks that was described at length by the terrorist review committee. That said that, between NSA and the domestic law enforcement activities that there was a gap, there was a seam, that NSA knew things prior to 9/11 about the nature of terrorist conspiracies overseas that had not been tied to the U.S. component of that, Al Mitar is the case that comes to mind.

That we could see the other end of that communication at a safe house overseas but did not know and did not have the means by which to say that the further end of that was actually in the United States of America. So the 215 metadata program was designed to cover that seam. And very narrowly constrained to only that case. And so it's, in a mosaic, useful to essentially inform other tools. But it's not a silver bullet in and of itself

INSKEEP: But this is what I want to go through. You initially said, the agency said, and your boss General Alexander said, 54 plots were disrupted. What you've just affirmed for me is that the vast majority of those involved Prism, a different program.

INGLIS: That's correct.

INSKEEP: And there may only be one case that you can point to where you feel that the metadata program was significant. And in fact, the president's commission which looked into the NSA's operations, of course, didn't even endorse the one. They said it was hard to find any cases. And yet, there's been this tremendous political cost from its disclosure. That's why I ask again if it was worth it? If the reward from this program has been worth the financial cost, the cost in manpower, the cost in time and the political damage of it ultimately being disclosed, as many things ultimately are disclosed.

INGLIS: I do think so. Because I don't know that I'd want to go back in time and say that I would run the risk of not uncovering the one plot that I did or to not have that tool that's an insurance policy to try to find something that crosses the seam from a foreign terrorist plot to something that might then be inserted into the United States as an activity here. I think we as a nation have to ask ourselves the policy question of what risks do we want to cover? Do we want to cover 100 percent of the risk? Or do we want to perhaps take a risk that from time to time something will get through? 9/11 was the single execution, it was the execution of a single plot with multiple threats. And about 3,000 people lost their lives that day. That's one terrorist plot coming to fruition.

If that is an acceptable cost, if we can say, we can take the risk that we'll miss something, then we don't need to have all of the tools that cover these various seams. We don't need to have the belts and suspenders and Velcro that essentially will overlap in an interlocking way. The 215 is designed to essentially cover a seam that we don't know any other way to cover. There are other implementations of the 215 program. The government doesn't need to hold the data, it could be held by a third party. You could compel others to essentially do the kind of search that today NSA is authorized and charged to undertake. But the question remains as to whether you're going to have a capability to find something that is the connection of a foreign plot to a domestic extension of that plot. I have an insurance policy on my house. I'm happy to say that I've not collected on that insurance policy, at least for purposes of fire or significant damage in the 25 years I've lived in that house.

But I'm not going to give that insurance policy up, because it's a necessary component to cover a seam that I can't otherwise cover.

INSKEEP: You just mentioned other ways to do this program. Are you now as an agency considering those other ways? Just leaving the information with the phone company, for example, and picking it up through a, through a warrant from the Foreign Intelligence Surveillance Court when you need it?

INGLIS: Certainly. We are open to other limitations. I think…

INSKEEP: So you are considering that?

INGLIS: We are considering that. But I think that we're not the policy agent that would decide whether or not we would then embrace one of those other choices. We would be a component of executing that choice. What would we offer, having some subject matter expertise in this is that two things. One, you have to first determine for what purpose would you want to have this program? This program is narrowly focused on trying to determine whether there's a connection between a foreign terrorist organization and a domestic plot. So against the 54 plots that were disrupted, since 41 of those had no U.S. connection, it would have been impossible for this program to make a meaningful contribution to those. It could have only made a contribution to the remaining 13. We essentially used this for 12 of the remaining 13. It returned information in 8 of those that we turned over to the FBI.

But in the other four, where it didn't return information, it actually returned useful information to the FBI. It gave them confidence that there wasn't a domestic plot. They could focus their time and attention elsewhere. But you have to first determine, do you have a purpose like that for which you would collect this data? Then you have to determine what are the criteria of any implementation, regardless of where the data is stored, or who stores it, or who searches it. I think those criterion are four in number. First and foremost, if you're going to collect this data, you have to provide for the privacy of the civil liberty protections in that data. You have to ensure that there are controls imposed on that data. I think that was the great disservice that was initially done in the unauthorized disclosures, which is that what was released in the public domain was the order that said, NSA is authorized to collect the information, period.

But it was the secondary order. There's actually a primary order that says here are all the controls, the imposition of constraints that goes with that. Those are really important because if you don't have those then you do not have a properly balanced program. The second criterion that you'd have to have is does the data that you collected have sufficient depth. Meaning, does it go back far enough in time, that if you made a search of it, you came away saying there's nothing there, that you'd have confidence that there really wasn't anything there. Telecommunications companies today who collect this metadata for business purposes do so with varying lengths of time. And they do so in varying formats. Some of them might have it for 6 months, some of them might have it for years.

You'd want to have confidence that if you wanted to look back two years, three years, today, we look back five years, that the data was there. The third criterion would be does it have sufficient breadth. You want to know that you've essentially got the whole pile. If you're looking for a needle in the haystack you need the haystack. So you wouldn't want to check a database that only has one third of the data, and say there's a one third chance that I know about a terrorist plot, there's a two thirds chance I missed it because I don't have that data. And then the fourth and final criteria is that the program would have to have sufficient agility. And if you had a plot that was unfolding at the speed that a human or perhaps individuals coordinating across time and space

were effecting, you'd have to have some confidence you could move at that speed.

And so if the program provides that you can get an answer back in 5 days, but the plot that you're trying to determine is going to unfold in the next day-and-a-half, that's not going to work. If you can meet those four criterion, I think that you can implement this in any number of ways. And we are wide open to that. NSA does not determine the policy in this regard. NSA would have to faithfully execute the policy that was likely recommended by the executive branch. But with the coordination, cooperation and participation of the judicial and legislative branches as well.

INSKEEP: You mentioned your feeling that Edward Snowden's disclosures revealed the metadata program in an unfair way. It revealed the part that looked bad, it didn't reveal the protections that you tried to bring along with it. In retrospect, knowing that, do you wish that some years ago this agency had made some effort to disclose this program in a way that the public could debate it, in a way that it could be looked at fairly from your point of view?

INGLIS: In hindsight, yes. In hindsight, yes. But if you'd asked me on June 4th, say, just before all of this broke, if you'd said, are you concerned, Chris Inglis about the 215 metadata program? I would have said, not particularly because I would have said in my own mind, and I would have said to anybody who asked me, that is a properly constrained program. I would have emphasized the controls that are imposed on it. I would have described, right, not simply the noble purpose but the operational purpose that was behind it. And I would have described the participation of three branches of government in it. And I would have thought, I think naively at this point in time, that it was sufficient that those three branches of government had stood in the shoes of the American public and made that determination, and that it was executed under, right, that broad Rubrik of what we would call the whole of government.

I think that what we found in the summer of 2013 is that it was insufficient. And that what we're going to have to do as a nation, and particularly as an agency, is to rebalance, right, the balance that we have struck between security, secrecy and transparency. I think that we have struck a good balance between security and the defense of civil liberties. And when we take an oath to the Constitution here, like anywhere else in the government, it's to the whole of it. And so I think we would, we have always worried about, right, the defense of civil liberties and privacy, consistent with what the Constitution and the articulation of the laws that come under that. The committee itself or the presidential review group itself that recently kind of talked at length about NSA, said that, as opposed to pre-FISA, pre-1978, there's a stark contrast today.

There's no illegalities, no abuse of authority of power at NSA. However, there's been a strong policy discussion taking place. We think that's appropriate. And that policy discussion would have been better if it had been done in the thoughtful deliberative way that I think we're now approaching, as opposed to the salacious sensational way that these initial releases hit the street.

INSKEEP: If in hindsight it would have been better to disclose the metadata program and have a public debate about it, are there other parts of NSA's operations today, other programs that are not known to the public that you think it would be wise for the public to have a reasoned debate about?

INGLIS: Two answers to your question. I think, first and foremost, to some degree the American public must have confidence that what NSA does is appropriate, authorized and effective. And so the question remains as to whether 315 million Americans need to see it for themselves, or whether somebody can stand in their shoes? Because the second question that comes up is to what degree do you disclose this only to the 315 million, you know, Americans and beyond that you hold it at arm's length from those who would then do damage to us with that knowledge? Rogue nations, terrorists, right, proliferators, folks who are out there keenly trying to understand how NSA or other foreign intelligence organizations in the United States do their business. We cannot run the risk of giving away all of our capabilities, right, in the spirit of trying to make ourselves completely transparent.

And so we're trying to strike that right balance. The balance today I think has a policy component of whether it's broadly permissible, useful, effective to give the kinds of authorities to NSA that we do. And that I think should have a fuller public discussion. But when you get down to the very discreet, right, somewhere between strategic and tactical choices about how you then implement that, I think that we need to then have a closed in discussion between three branches of government, those who stand in the shoes of the American public, so that we can have a fully informed decision that then results from that fully informed dialogue. But I am not at this point saying that I would bring all of NSA's capabilities out into the open. Not because I'm in any way, shape or form thinking that the American public would be shocked or outraged by those but because I really don't think we can afford to give those capabilities away to our adversaries.

INSKEEP: You must have done a risk assessment though. Is there a program within the NSA, a discreet program in the way that the metadata gathering was a discreet program. Is there a program within the NSA that you think if it were disclosed that there would be a significant public debate about its correctness?

INGLIS: No, I don't think so. I think that in the early days of the summer of 2013, we thought our way through is there some broader framework, right, that we could describe that would help people understand the next release, the next unauthorized disclosure. And so we actually published a paper. And it said, that you could think about NSA this way. NSA is of course a foreign intelligence organization that therefore must be motivated in whatever authorities it's allocated to focus on that. We think of ourselves as not so much being enabled and therefore given the opportunity to do what we will, but having to be explicitly authorized. And so before NSA undertakes an action you must in fact understand, as an NSA official, me, you must understand what's my explicit authority. It can't be generic. It can't be inferred.

It has to be explicit. What is the articulation of that? Is it through a court order? Is it through an executive order out of the executive branch? And then beyond that, what's the priority given to the various issues that I would then go work on? I have essentially at the NSA have about 36,000 pages of requirements that I'm working on behalf of the executive branch. But those all can be traced back explicitly to an explicit authority, either from a court or from some executive branch authority that says, here's your authority to go get that.

INSKEEP: When you say requirement, you mean please gather intelligence on this particular subject.

INGLIS: That's right. A question that might be, can you tell me what the intention is of this rogue nation? Can you tell me what this terrorist group is doing? Right. And there's then when you expand those into all of the particular questions that then descend from that. Today are about 1,800 requirements at a coarse approximation. And when you then expand that, come to about 36,000 pages. And so the truth of the matter is beyond matters of law, which we are absolutely, you know, essentially going to obey, but beyond matters of law it would simply be inefficient for us to then go on a wild goose chase with those things we simply find interesting.

INSKEEP: Are you effectively abandoning the metadata program? If you're thinking about just leaving it with the phone companies, leaving the information with the phone companies, querying it when you have a specific need and you can get a judge, wouldn't that just be, basically be giving up the program?

INGLIS: I don't think so. I think a different implementation could meet the same four criterion that I told you about. That last one of which is that it's agile enough to essentially give domestic intelligence organizations, FBI, information at the speed that they need it to uncover and follow a plot. You can do that by implementing it at NSA. You can do that by implementing it at the vendors. You can do that by implementing it at a third party. But given the first three requirements, they're going to probably have to be some statutory and very likely some court involvement in order to setup the legal framework to achieve that. But that's not abandoning the program. That's implementing it a different way. I think most Americans would be surprised, this is out there but it's not been discussed at length, they'd be surprised at how infrequently we actually look at that data.

In all of 2012 there were less than 300 occasions where we said what we had was reasonable articulable suspicion, that's the legal standard that's applied here, to query that database. Less than 300 times. So while most people might think in the worst case that we're looking at that data pot everyday and trying to find interesting connections inside of it, we do not. We have to wait until we had some predicate, some stimulating event that gives us that reasonable articulable suspicion to look in the pot. Until that point in time it's a locked box.

INSKEEP: Although it is interesting though the president's commission wanted to

investigate this issue and wrote about it said, that yes, 288 times I think in 2012 you went to the metadata for a particular phone number. But then you're allowed to look at phone numbers that we're called from that number…

INGLIS: That's true.

INSKEEP: …and then numbers that were called from those numbers. And they outlined a scenario where one data request might cause you to look at a million phone numbers.

INGLIS: It could. But in all of 2012, we actually looked at 6,000.

INSKEEP: 6,000?

INGLIS: That's right. And that's not a change in the answer I just gave you. What happens is that, again, as a matter of record, is that we're authorized to essentially under reasonable articulable suspicion look at the first number. So we kind of, 288 times go in. That then returns some number of numbers that have been called. There's no names, there's no content. There's no locational data associated with it, it's just numbers that come back. We can then, we're authorized by the court, look further. We can take those numbers and do a second hop, or even a third hop. But we need to be judicious about that. Both for legal reasons is that we're trying to reduce constrain, right, the intrusion into this data set, right, that would otherwise occur. And it would be grossly inefficient to give the FBI a million numbers associated with one plot.

INGLIS: And so the constraints that we have applied, based upon our analytic judgments have essentially touched 6,000 numbers in that data set, in all of 2012. Not a million. A million is theoretically possible. But when you then consider what the actual implementation of that is, it's a much different answer.

INSKEEP: 6,000 numbers is the number in 2012?

INGLIS: 6,000 numbers is what we actually then touched, all based upon the seeds that started with less than 300.

INSKEEP: There was a similar program - was there not? - to gather metadata on electronic communications, emails and so forth.

INGLIS: Emails, there was.

INSKEEP: And it was abandoned because it was too hard to comply with the safeguards and because it was judged not to be practical, it wasn't worth the cost.

INGLIS: It was abandoned principally for the latter reason, which is it was just too hard to make operationally workable. In theory, and especially given that people move more and more to emails, right, that kind of communication, in theory it would be even more valuable to try to detect a plot that moves from a foreign domain to a domestic domain

using email metadata. The challenge is, is that the business model within the private sector doesn't support that. You and I grew up in an America where there were local calls, long distance calls, and the telephone company made their money by charging you for the number of local calls or the number of long distance calls for some duration. And for that reason they tracked that information. You could go to the telephone company and say, how many calls and what number called what number.

And they would actually track that with great precision. Email didn't get its start that way. The first email account I had from a company with three letters said, for $6.95 a month you can write a million emails or one email, we don't care. We're going to send you, sell you a bandwidth. And so there was no material business interest on their part to track the metadata. They just wanted to sell you access to the pipe. Given that that information it doesn't exist, it's hard to recreate it. It became operationally very difficult to do that. It is theoretically possible, but very expensive. And we've decided in late 2011 that while we thought we could meet the requirements of the court, we were quite confident that we could, the only way we could proceed was in so doing, that it was operationally too difficult to do that because the business model was so different.

INSKEEP: And yet you argued for some time that it was an important counter-terrorism tool.

INGLIS: I would say it still would be an important counter-terrorism tool. If we could figure out how to do it with reasonable cost, dollar cost and time cost. But at this point in time is something that in a world of limited resources you have to make choices.

INSKEEP: So I wondered if there was a contradiction between abandoning the email program, and keeping the phone record program. But you're basically saying the phone record program is just more practical, it can be done.

INGLIS: It's much more practical. It can be done. People still use telephones.

INSKEEP: Once in a while.

INGLIS: Once in a while.

INSKEEP: I want to ask about mistakes, errors, violations of privacy. You gave a fascinating talk late last year at the University of Pennsylvania in which you referred to a document that had been disclosed that referred to something like 2,700 errors by the NSA. You argued that about 2,000 of those were not really relevant, set them aside. And then acknowledged there were 711 actual errors where you violated someone's privacy in a way that was not authorized. What happened on those 711 times in one year?

INGLIS: Yeah, so if I could clarify that. The report, first and foremost, was written in the early part of 2012. We wrote it ourselves. And we generate these reports essentially to take a hard look at how all the various things that we do to collect a communication of

interest, store the communication of interest, query the communication of interest, we want to make sure we do that exactly right. And we determined in that report that on an annualized basis, we extrapolated the numbers, that we had essentially had about 2,776 situations that didn't go exactly according to plan. That was immediately interpreted by some press outlets when that was released - again, it was another unauthorized release - but when it was released, some number of press outlets immediately equated that to 2,776 privacy violations and went so far as to say that they were either willful or kind of attributable to the gross lack of conscientious actions on the side of NSA.

Which is why I went then to some pains to explain what that really was. It turned out in 2,065 of those cases, so about 75 percent of those cases, the situation was that the individual, the organization that we were authorized to understand something about, whose communications we were trying to collect, had moved, right. Either they had physically moved or their services had moved and they were in a different location. Our authorities essentially asked the question up front of where is the party of interest? You know, where is the communication of interest? And where is the collection taking place? And if any of those change, we're probably using the wrong authority. And so, 2,065 we notified ourselves that that had changed. They don't consult with us before they change their location.

And so the system actually worked exactly as it should, which is that it figured that out, stopped the collection, purged back to the point where we last knew with precision where they were and then went after the right authority to essentially begin that again. In my view, that would be a feature, right, a positive feature. That leaves then 711. They weren't privacy violations, per se. What they were was that an analyst somewhere across NSA entered the wrong telephone number, the wrong email address when they were attempting to target A, but instead they could have potentially targeted A-prime. In most of those cases the number that they entered because they fingered it, they got a 2 in there instead of a 3, or something of that sort. The number didn't exist and so it returned.

But in all those cases it was caught because we essentially had checks inside the system, almost always a second check to make sure that what we have done is exactly what we intended to do. And we caught all of those things. And essentially took the right action. Whether it was how we formed the selector or whether it was how we queried a database, whether it was how we disseminated a piece of information. And those 711 occurrences have to be considered against all the activities we took that year. And it turns out that the average analyst, if you attributed those errors to an analyst, none of which were willful, all of which were simply accidents, the average analyst at NSA would make a mistake about every 10 years. The accuracy rate at NSA is 99.99984 percent, which is a pretty good record. But that said, we worry enough about making any mistakes that the 711 are a peculiar interest to us.

We're going to fix those. And so we have driven those down quarter by quarter, year by year.

INSKEEP: I was fascinated by that math, that 711 errors in a year means that 99.99984 percent of the time you're right. And so I started doing the math and reversed it, tried to figure out, well, how many communications are they monitoring then? And when I did the math I concluded that that means that you're monitoring, I wrote down 44,437,500 communications in a year. You're nodding, that's about the scale of your activities?

INGLIS: That's what that math would lead you to but actually, it's not that simple. So let's say I'm interested in a particular terrorist, that individual might have dozens, might have across a given year hundreds of selectors. I'd kind of pick up and drop telephones on, you know, like it's fast food. They might form, discard email addresses at a rapid rate. Why? Because we told them that they're of interest to us. We've been telling them that for years through these unauthorized disclosures. So one individual might have attributable to them hundreds of these things. At the same time, we don't query one time a year. We might try to find out every few hours. We might try to find out every once in a while, you know, where this thing is. It might be that geo-location is of interest to us. And so all of that then constitutes a broad number of inquiries.

And then when that data comes back to NSA, we query that data various and sundry ways to ensure that we fully understand what the nature of these kind of insights are into these foreign activities. And so that then constitutes a multiplicative factor in terms of how you get to large numbers. So you can get quickly to your 44 million number but that equates to a much, much smaller number of actual persons or organizations that we're interested in with some degree of frequency because they themselves are essentially running fast across this territory. And we, ourselves, are trying to actually figure out how to understand this with a currency that's measured in minutes as opposed to months or years.

INSKEEP: One reason that number was of interest to me is because I'm sure after 9/11 the question was being asked are you casting the net widely enough? Is the question now whether you've been casting the net too widely?

INGLIS: Well, that is a question that we've been asked. And so I think it's a fair question. So what we have to be able to do is to at once discover. Right. So we have to understand that there are incipient threats. There might be terror plots out there that we know nothing about. And so we have to be able to try to figure out how would we sense that, how we'd see that coming our way. And so you need to cast the net a little bit wider than perhaps what you currently know. But at the same time, you need to make sure that for purposes of efficiency and proportionality, right, we need to use these tools with some degree of discretion, that you're not casting it too widely. And so the balance for us typically comes into the difference what we call metadata, right, and content oriented searches. So metadata, which might be attributable to something like what you see on the outside of an envelope, right? There's an address there, a return address.

INSKEEP: Sure, the phone number - who did they call? Where did they call?

INGLIS: That's right. And in cases of snail mail there might be even a time stamp up

there over the kind of stamp itself. You can tell a lot about who's communicating with who looking at that. And you can tell a lot about perhaps where the innocents are. You should leave that alone. Don't touch that. And perhaps where the parties of true interest are, right. What's the center of a terrorist network? Who perhaps is kind of conspiring to do what they might do, and who might be a level out from that, and two levels out from that. The metadata, if you cast that net widely enough, gives you a sense as to what the territory looks like, so that you then might traverse that territory and then go after the content with greater discretion and surgical precision. For purposes of efficiency you have to do your business that way. But for purposes of the law, and executing proportionality under the law, we also have to do our business that way.

INSKEEP: So are you casting the net too widely right now?

INGLIS: I don't think so. I think that there's a policy question to be asked about whether we should continue to collect the telephone metadata we know as the 215 Program. If we, as a nation, decide that we're willing to sustain the risk of not knowing, you know, those occasions when somebody crosses the seam, the purpose for which that program was defined, then we will have in fact said that the net was cast too widely and that we're going to essentially stop doing that to essentially reduce the possible incursion on the privacy of U.S. person communications. So that's a choice to be made. But we haven't yet made that choice.

INSKEEP: Well, let's go a little beyond the metadata program to the NSA's broader operations or even other disclosures that have been made, such as the monitoring foreign leaders. In that context, has the net been cast too widely?

INGLIS: I would say that NSA, as I indicated earlier in the conversation, has to not only understand that it has the authority, right, to target something of interest. But it must also know that there's a priority, right. We only operate against explicit priorities. And so we as a nation can make choices about how much we must know, need to know, about threats or activities in the world. I would tell you that there's an active consideration, the president has asked that question, about whether or not we should favor, right, some greater degree of outreach between intelligence organizations, between allies, in much the same way that we have for 70 years between the English speaking nations known as what I call the Five Eyes(ph). Great Britain, United Kingdom now, Australia and New Zealand, Canada, the United States. Should we extend, right, that same kind of degree of greater collaboration to others?

That's a fair question. Right. And I think that's a question we're actually walking our way through.

INSKEEP: Well, that's a policy question. I guess that might be a presidential question. But you can address that on a practicality level. When we think about some of these programs have proven to be controversial, have they been worth it? I get back to that question again. Did you get anything out of spying on Angela Merkel, or whatever? I mean was there anything that came out of that kind of monitoring that…

INGLIS: Yeah. Well, I won't talk about particular intelligence priorities. I will tell you that the vast majority, if not the entirety of the material that we have produced, which always cites the intelligence priority behind it, has been very useful and responsive to the requirements that essentially generated the activity in the first place.

INSKEEP: In other words, someone asked you and you gave them what they asked for.

INGLIS: Every report that NSA writes, and this would be true of any foreign intelligence organization within the United States the way we've essentially built the system, will cite, right, expressly what authority and what priority is being addressed by that.

INSKEEP: I want to ask about monitoring Americans. And before I do, I want to ask you a question that I'm sure you've been compelled to answer a 100,000 times, but it would be useful just to hear your definition of it and for people to hear that. Under what circumstances can this agency monitor the communications of Americans? U.S. persons, U.S. citizens, people living here.

INGLIS: That's a great question. It's an important question. So let me answer it this way in a slightly more comprehensive way than you might have intended because it's a complicated answer. I would say in order for this agency to target the content of an American's communications I need a court warrant. I need a court order. In order to target it, you know, as if I'm going after the American, the U.S. person communications. But it turns out that any communication in the world has at least two parties to it, right. There's kind of the sender, the receiver, there's the speaker, the listener, and vice versa. And so if I am legitimately going after, you mentioned earlier, Zawahiri, if he was kind of to create an email account and make use it, and if I was able to determine what that email address was, you could imagine that I might hypothetically at least, be interested in that.

And I might then try to find that communication in the world. And if on the other end of that communication there was a U.S. person, it turns out both parties own that communication. And so at the same time I'm doing something that everybody would say is quite legitimate. I got Zawahiri's email. I've at the same time collected the email of the U.S. person because they both own that communication. And we would call that in my business, an incidental collect of an U.S. person communication. That's what an incidental collection is. It's not that somehow we were fishing for tuna and we got dolphins, right. We actually got a communication owned by two parties, and one of them is a U.S. person. And I then have rules, right, that are imposed on me both by the court and by the executive branch, depending upon which authorities I'm bringing to bear that talk expressly, explicitly about how I am then to handle the U.S. party, the U.S. person in that communication.

And so the kind of long answer to your good and short question is that there are circumstances where I might incidentally get U.S. person communications. I've just explained one to you. But they are actually considered in advance as being not simply possible but probable in a world that increasingly is converged, right. All of these

pathways are shared by adversaries, hostile parties and friends alike. And we therefore have to consider the possibility we will encounter U.S. persons and know precisely what we will do and always faithfully do it.

INSKEEP: Are you - so in those incidental, in those cases of incidental collection, you what, disregard the U.S. person unless there is a court order involved?

INGLIS: In broad terms, you do disregard the U.S. person. So what you have to do is what we would describe as the activity of minimize, right. And so unless the identity of the U.S. person, right, is important to the foreign intelligence value of that communication, we must then kind of screen that out, filter that out. We would say, let's say, that Zawahiri kind of disclosed his intent to attack something of interest to us in an email, and he shared that kind of with some number of persons, one of whom was a U.S. person. We would have to identify in the report that we would write at the classified level, that there was a U.S. person involved in this. That he was a recipient of this, or she was a recipient of this. And we would go no further than that unless, and until such time as it became clear that that party was materially involved in this plot.

And if in that point and time we wanted to focus our time and attention on that U.S. person, I would then have to go get a warrant. No matter where they are on the planet earth, I'd have to get a warrant if I'm not going to focus on them as the target of interest, as opposed to them being incidentally involved in this communication.

INSKEEP: You're telling me that you always and have always in every case sought a FISA, a Foreign Intelligence Surveillance Court approval before focusing on a U.S. person?

INGLIS: Well, until I think it was 2008, if a U.S. person was overseas and they became of interest to me in the way that I just described, until 2008 the law provided that I could get an Attorney General authorization to target the U.S. person. Again, in my case it would only do that if it was a foreign intelligence purpose and if I had made the case to the Attorney General. The FISA Amendments Act that came in in 2008 essentially made it clear that no matter where you are on the planet earth, if you're a U.S. person, if you have U.S. person status, if NSA or any other foreign intelligence organization within the U.S. is going to target them, they must first get a probable cause statement from the court, the Foreign Intelligence Surveillance Court. So since 2008 the answer to your question is yes.

INSKEEP: Yes, you always do that.

INGLIS: Yes.

INSKEEP: I want to follow up on an aspect of that. Because we should note the NSA has said, you know, maybe we're gathering metadata on Americans, but we're not listening to your calls, we're not reading your emails except in these very limited cases where there was a court order. But, of course, you are gathering and vast amounts of

communications from around the world. And some of those will be between a foreigner and an American. And so American communications are being gathered in some fashion. Since 2011 haven't you had the authority to monitor the communications of Americans in that giant pile of communication without getting a specific warrant?

INGLIS: Oh, so what you're talking about is the authority that we have. So let me go through an example. And if this is the one, then I'll talk at whatever length you'd like about it.

INSKEEP: Please.

INGLIS: So let's say that I'm going after my hypothetical, you know, favorite party, right, the head of Al-Qaeda worldwide. I mean I collect some of his communications. And I have confidence that I in fact have his communications, and they're now in a pile that I expect an analyst to then understand. You know, what is he doing? What is he saying? You know, what conspiracy might be afoot? That analyst now has not simply the authority but the obligation to understand that pile because they're all responsive to the intelligence query that I made. Every one of those has been now selected out of that sea of information, those trillions of communications worldwide. They've been selected out as being materially responsive to my query of interest. What's he doing? And inside of that then, there are all sorts of questions you might ask, right.

Is this a plot against, right, so some financial institution within the United States. It turns out that's a U.S. person query. But if I wanted to know if this is a plot against one of those financial institutions I'd have to query that very limited constrained data set to see whether or not that institution is named. Analysts had the authority to do that, right. Those authorities are granted by the court, right, that gives us the authority to collect the information in the first place as part of the rule set that says, how might you then treat that pile? I think that's the question that's been asked of us some number of times. Are we in fact then using this as some back door to target the communications of Americans? We are not. We are using this essentially as a way to understand the pile of communications that were responsive to these foreign intelligence queries in the first place.

INSKEEP: At least in this limited circumstance, have there then been instances where you've monitored the communications of U.S. persons without a specific warrant to do so?

INGLIS: No. If monitor is that we're trying to find – we're trying to have continuity on a U.S. person essentially by essentially asking queries of this pile, no, because we would not have essentially focused the collection activities on those U.S. persons. The only way the U.S. persons could've gotten into that pile is that they are, in fact, on the other side of the communication of somebody we're legitimately interested in.

And the 702 provision goes so far as to say that we cannot use, right, our authorities under what's the so-called Prism program to reverse-target Americans, right? That's

expressly prohibited by the law.

INSKEEP: So if someone said – in fact, I'll just say – so if the question is have you targeted Americans using that authority in any case, the answer is no.

INGLIS: Not in the context…

INSKEEP: It's happened zero times.

INGLIS: …that you intend. Not in the context that you mean. So let's say some clever person says, you know, I'm not authorized to target Chris Inglis overtly, unless I go get a warrant and he's not done anything to show himself as being a threat to the nation. But I know that he's always in contact with somebody that I am legitimately authorized to go after or I could make some plausible case for that.

So why I don't go after Party B because I know that Chris is always in contact with him and I'll just collect enough communications that gives me insight into Chris Inglis? That is expressly prohibited by the law. It's written in that you cannot use that as a back door, as a 702 back door, the authority being 702, to target Chris Inglis. It's called reverse targeting.

INSKEEP: Let me ask you about another issue, if I might, having to do with U.S. persons. You go to the Foreign Intelligence Surveillance Court; you seek a warrant in the cases where your monitoring might call for you to look at a U.S. person. There have been calls, numerous calls, for some kind of public advocate to be in that court to essentially stand in for the person you're surveilling because, of course, they don't have a lawyer there.

If that were to be done, would it interfere with your work in any way?

INGLIS: We'd welcome it. So I would only put the caveat on there that it needs to be operationally efficient. So let's say that I'm authorized to target the head of Al Qaida worldwide and I'm actively doing that. I'm trying to figure out, you know, what communications services, selectors, that person's using. If at every moment in time somebody had to authorize me to put the next selector, right, on cover like, you know, he just changed his email address, can I put that on?

If that's where the advocate stands in that's operationally not terribly efficient. But if there's going to be some novel interpretation of the law, if there's some authority that's going to be applied as an extension of the law that others might say I've got a different view, we welcome that, right. I think that that would be quiet appropriate.

And I would go so far as to say that also with the court it might be helpful to have somebody who would assist them with matters of interpreting technology. How does the technology really work? And because that's not that straightforward, right, the technology is constantly roiling, right? It's changing over moment by moment and the

way people employ that technology is changing over moment by moment.

And so that might be another assist to the court, which I will tell you works very hard and faithfully to do all that themselves but any assistance that might be provided or any amicus that might be provided in terms of giving them an alternative view of the risks that are undertaken would be helpful.

INSKEEP: Just so I understand what you're telling me, you're saying that if this public advocate, hypothetically, got a say on all 44 million communications you're looking at in a year, that'd be a serious problem.

INGLIS: Yes. First, I'm not looking at 44 million communications in the context that you describe.

INSKEEP: OK. OK, go on.

INGLIS: But let's say it's a large number. If that kind of public advocate had to personally vouchsafe for every one of those collection activities then that would be operationally very inefficient and it would slow the system down. We would not in any way, shape, or form object to having some accountability exercise that says but I want to know how you've applied these authorities.

That, in fact, happens today. The National Security Division at the Department of Justice, the executive branch, has some number of activities both across the DOD, the Department of Defense, and the director of National Intelligence that actually, in arrears, look at all of our collection choices to make sure that we've made the right choices.

INSKEEP: What if you had this advocate each time you're seeking a warrant, which is a finite number of warrants that you do seek in a year. Is that operationally possible?

INGLIS: Yes. So I'd let the lawyers rule on that but I would say from an operational perspective I would welcome that advocacy in the room. The question is how operationally efficient can you make it.

INSKEEP: A few other questions. And I don't even know what time it is, by the way.

UNIDENTIFIED WOMAN: I think it's 1:35.

INSKEEP: Oh, it's 1:35. OK. So I want…

UNIDENTIFIED MAN: It's been 50 minutes.

INSKEEP: OK, great. Great. We may even finish a little bit early. We will see – we will see how things go here. I want to understand a couple of other things, however. One of them having to do with the state of technology. You've been described in the past year

as – in fact, in the past many years, as an immensely powerful agency with immense resources. And they certainly have been increased since 9/11.

Given the challenge that you face, do you feel like you're running an immensely powerful agency?

INGLIS: I do. I would say that we feel that we've been entrusted with a tremendously important responsibility and that cuts both ways. The pressure I feel on some days is have I, in fact, determined the threats to the nation such that I can inform the policymakers, decision-makers, people who stand in harm's way in uniform with sufficient insight and clarity that they'll help interdict those threats. That's a pressure.

Right, so that's a great burden. It's a great responsibility. But I think you mean it the other way, which is do I have the authority to do things that, if taken to excess, we should be concerned about, right, that those things can be abused. We do have authorities that could theoretically be abused but we have applied extraordinary constraint and controls to that.

INSKEEP: I actually mean it in a slightly different way. We were talking earlier about the email program that you abandoned because it would be nice to have but it just didn't make any sense.

INGLIS: Right.

INSKEEP: You're dealing with, you know, billions of communications around the world.

INGLIS: Right.

INSKEEP: Do you actually feel that you have the technical capability to monitor all the communications that you need to monitor? Or a sufficient number of them?

INGLIS: If the answer at the end of the day has to be a hundred percent confidence that we know all threats to all things at all times, of course not. We don't have that sort of god's eye view. We don't have that omniscient capability. And so there's a reasonable balance. The Europeans actually have a nice turn of phrase for this. Our European counterparts say that when you try to achieve the right balance between security and privacy, you need to think in terms of necessity and proportionality. Right?

Do you have some necessity to essentially incur upon, right, the otherwise private affairs of individuals of interest to you? And if you do, have you done that with certain – have you done that with the aspect of proportionality such that only in proportion to the nature of that threat? And that's really the nature of how we apply instruments of national power like intelligence.

You need to make sure that you have, at the end of the day, achieved some balance in that regard. We are neither omniscient nor unknowing. Right? We try to find that sweet

spot in between. And I would say that I think that given the investments that the nation has made, not simply in the capabilities that people most often think about in terms of technology, but in the brain trust that is NSA, we're quite capable of helping the nation understand threats to its people and its territory and to its relationships, so that we can with confidence say we can make a meaningful contribution.

INGLIS: And we are at the same time well constrained, controlled, you know, hobbled from making the sort of excessive application of those capabilities that you might worry about.

INSKEEP: Here's what I'm thinking about. You're in a competitive environment and a changing environment. You're not just competing with enemies of the United States whom you might want to track; there are also technology companies who are constantly changing their methods, would like to protect the privacy of their customers, would like to persuade overseas clients that their privacy is being protected.

INSKEEP: And so, I assume there is a push and pull of technology and innovation.

INGLIS: Yes. There is.

INSKEEP:

Are you winning or losing? Are you gaining or falling behind?

INGLIS: We're holding our own, I would say. So here's the great secret of NSA. I'll come lay this on the table. Most people when they kind of say I want a picture of NSA what they'll do is they'll take a picture of a device, a computer, technology, maybe the building that we're sitting in which has these black leaning panels on the outside.

That's actually not NSA. That's a component of NSA. But if you want to really know what the core of NSA is, it's its brain trust. It's its people. All right? We employ some, you know, number of people which includes 1,000 Ph.D.s, that includes a diverse array of disciplines that we bring to bear. I mean, it works more horizontally than it does vertically.

What we try to do is to determine what our challenges are, what we need to figure out, the use of a particular technology to communicate some conspiracy that would harm the United States. But how is that done? What are the security protocols being employed by our adversaries? How might we actually kind of understand the weaknesses in those and how might we then find that moment in time when we can understand what's actually being communicated by whom to whom about what.

That's actually an intellectual issue, not a technology issue. And so, for the 70 years that we've essentially been doing this business, all the way back to the days of World War II, the principal instrument of power that we bring to bear is the intellectual power that is constituted in the workforce. And I'm very confident that this workforce will be up

to the challenge of continuing to try to figure that out.

There's an anecdote that's quite dated but I think it's also possibly useful. In the middle of World War II, the Axis powers, who were in those days using something called the German Enigma Machine, a very capable device. The mathematics inside of it were very impressive, even in its day but today would be still impressive. They went from what were called three rotors to four rotors.

Each rotor had some number of positions. At the beginning of the day you'd set these rotors to A or Z or something in between. When they added the fourth rotor, right, most folks in the business said that's it, game over. You know, we had a kind of a thumbnail grip on three rotors but we couldn't possibly do four.

But they missed the point, which was it wasn't about the static advantage of how you exploit a three rotor machine; it was about the intellectual advantage of can we, even when they use a four rotor machine, try to determine the mistakes that they might make, try to determine the weaknesses in that system. Try to, in a system in motion, a communications system in motion, try to find that place where we might then outwit, outthink, outmaneuver an adversary in the space we now call cyberspace.

But in those days it was simply the short wave radio space. We still have an advantage. The United States and its allies still has an extraordinary advantage. We've got an enormous brain trust. And that's not simply people who work at NSA but the people who support NSA. And it's all done under the rule of law to ensure that those capabilities are brought to bear in a way that is completely consistent with the Constitution and the interpretations of the laws, the policies, and the orders.

That's why I was so distressed in June of 2013 when the only thing that was in the unauthorized leaks in the first week or two was the fact that NSA can collect large quantities of what we now know as telephone metadata. What was not released at the same time were the constraints and controls that are imposed on that and the ethos, the culture that is applied inside NSA to make sure that we're completely faithful to that.

We welcome further insight in that. I thought it was interesting that around right the December timeframe when one individual on the planet was saying that I won, I don't think anybody in NSA would ever think in those terms. What somebody at NSA might say is have I done enough to defend the nation. The director of compliance at NSA said that his Christmas wish was that he could give 315 million Americans a security clearance, so that they could come in and actually see what we do and how we do it.

We welcome that degree of transparency. I just don't want to bring in terrorists and rogue nations and those who are trying to do harm to this nation and give them the same insight.

INSKEEP: This is a side point, but I notice you're not saying the name Edward Snowden. Is there a reason you don't say his name?

INGLIS: No. I can say that name.

(LAUGHTER)

INSKEEP: But you're not going to just now.

INGLIS: I think Mr. Snowden deserves, you know, his day in court. He has his position. He has his opinion. I'd like to see him get his opportunity to make his case.

INSKEEP: As much as you disagree with what he did, has he helped you since he brought about a public debate that you now say that in hindsight you wish had happened before?

INGLIS: In the same way that somebody who burned my house down has given me the opportunity to perhaps build it in a way that I would prefer. And so I think his methods were reckless and irresponsible and given his originally stated case, which was he had been, you know, the self-determined judge and jury determined that NSA had exceeded its boundaries with respect to domestic collection and domestic activities and therefore, attempted to expose that.

In so doing, he also exposed enormous quantities of information about how we do the business of tracking terrorists and tracking rogue nations and the like. So, you know, given his expressed concern I think that he's greatly gone by that and I therefore find him reckless.

INSKEEP: What have the disclosures done to your relationships with technology companies?

INGLIS: Oh, it's strained them, to be sure. Those technology companies have only tried to do the right thing and to support this nation and other nations. There's no nation on the planet that doesn't do what we would call lawful intercept, that under legitimate authority try to understand a little bit about the threats to the nation that might be communicated in today's technologies.

And as those companies have been described as perhaps being inappropriately in collusion with various governments, not least of which this government, they've taken some I think unfair hits. I think when you look into it, those companies are responsible. They are a source of power of this nation. They are a source of benefit to anyone who would avail themselves of the services. And they therefore deserve to have the record set straight.

INSKEEP: Are they being less helpful than they were?

INGLIS: I think that when we need them they're still being helpful. Right? And, again, that's all done under the rule of law. That's all done responsibly. So the various companies who participated in the 702 program continue to be responsive. That

continues to be something that helps us understand threats to the nation, our people, and our territories and our partnerships.

INSKEEP: Some people have noticed what you almost might think of as a partisan divide, not about political parties but about people in different jobs. That if you're in the national security field, the Snowden revelations do not shock you or outrage you very much but that if you are working for a tech firm, a lot of tech executives are very mad, are very unhappy about this. How would you explain that divide?

INGLIS: I don't know that I can explain the divide. I see it. I would say that what I have to think about as an executive within the executive branch under our Constitution is do I have express explicit authority to do what I do? And therefore I can quickly reconcile that the application of the authorities that we've described in so many ways across the summer have not simply been explicitly authorized but they've been properly constrained which is the nature of our Constitution and the laws that derive from that.

And so I've long since reconciled myself to the way that balance is achieved. I'm not sure that if you're not in the government you would think about that. Right, you might just think about the dynamic of I'm trying to sell services to a world population, not simply the United States. And I'd like that world population to imagine that these are safe from kind of any intrusions whatsoever. Right?

And to the degree that that balance hasn't yet been struck to everyone's satisfaction, not just the United States, I think that you might then have a different lens through which you're looking at the same problem set.

INSKEEP: But that's an interesting point that they are selling to the world. And that means that Silicon Valley firms, in some cases in the past year, have lost business or have reported losing business because foreign partners don't want to deal with them and run the risk of being surveilled by the National Security Agency. Are they responding to that by taking additional measures to make sure that they're not surveilled by the NSA?

INGLIS: I think whatever measures they're taking to give their customers greater confidence that they can safely, securely communicate are very likely appropriate. Insomuch as NSA should not have access to communications that it should not have access to. All right? If kind of in the scheme of things, there are classes of persons, whether they're U.S. persons or innocent foreigners who should not essentially have their privacy incurred upon by NSA because there's no material reason, there's no authority that I could divine for that, they should have some confidence that they're protected.

Of note – you didn't ask me but I'll bring this up. You know, there is – a discussion has taken place where there have, in fact, been some willful abuses of the signet capabilities that NSA brings to bear. There have been 12 cases over the last 10 or so years where individuals made misuse of the signet system. They essentially tried to

collect a communication that they were not authorized to collect 12 times.

The vast majority of those were, in fact, overseas. Right? They were NSAers operating in foreign locations trying to collect the communication of an acquaintance so that they could better understand what that acquaintance was doing, but those acquaintances were foreigners. And our capabilities must be applied in a way that essentially meets the requirements imposed on me such that we would protect the privacy of foreign persons as much as we would protect the privacy of U.S. persons.

An inappropriate use of the signet system for any purpose is inappropriate. All right? And so if the companies are simply trying to give additional confidence, right, to the customers who have no reason to fear NSA, I should have no reason to fear that.

INSKEEP: Have any windows closed to you because corporations are behaving differently in the last six, eight months?

INGLIS: It's too soon to tell and those details I'm really not kind of in hand with. I would tell you that those companies are attempting to give some greater confidence to the people who make use of their services that they are not being inappropriately spied upon. And I don't have any qualms about that.

I would say that if, at the end of the day, we make it possible for terrorists to make use of these services in a way that they have absolute confidence that they'll never be undone, that they get anonymity services, they get encryption services, right, they get resilient, robust communications at any time of the day, then we will have achieved the wrong balance. But we're not there yet.

INSKEEP:

Do they have exit interviews for people who are leaving the National Security Agency?

INGLIS: They do.

INSKEEP: Did you do yours already?

INGLIS: I have not.

INSKEEP: You will be doing one?

INGLIS: I will. I'll have the opportunity to talk with my boss, right, as I leave. And there's also something here at NSA we call parting thoughts. Right, it's actually a wiki-like device where you can essentially make a statement to anybody that would care to read that on a volunteer basis. And so I'll do that too.

INSKEEP: I would think in an exit interview somebody would ask you – your boss might ask you – what would you change about this place? What would you change about this

place?

INGLIS: First and foremost, I think I would focus on what I wouldn't change about this. I'll answer your question in a second. But I would say that the kind of intellect, the kind of principled audacity that we attract and we encourage and develop has been a source of great strength for the nation, right, the things that we've been able to do. It is not an accident that there's not been a foreign-induced terrorist attack on this nation's soil in the last 12 years.

In the last three months alone there have been 5,000 deaths attributable to terrorist activities across the broad swath of southwest Asia, Africa, places that, you know, are in the news every day. There are activities that are trying to come onshore. It's not a mistake that that's actually been a failure for them all those years.

So there's a lot that I would say we have to sustain and keep going, which is a focus on the people, a focus on the principles and the ethos that essentially ensure that those people exercise their authorities the way that the American public would have them do that. I think going forward what I would change is that we need to continue to move in the direction of having greater transparency about the nature of NSA, what its authorities are, how those authorities are brought to bear.

There's going to be a limit, a natural limit to that. We're not going to be able to get into all of the explicit technical stuff that we do. You know, people should know that there's a presidential daily brief. That President Obama on a daily basis gets access to highly sensitive information. But, you know, we're not going to reveal what the contents of that are on a daily basis, however interesting and titillating that might be. So we've got to find that balance.

I would say further that as NSA goes forward it's going to have to make sure that it continues to provide an honest perspective on how these capabilities can be employed, what the risks of these capabilities being modified might be in both directions. If they're modified in one direction it might be that that incurs a greater possibility of intrusion on privacy. NSA needs to speak to that if that were to occur.

At the same time, we would speak to that this particular change that might be considered would possibly harm our ability to have insights into the threats to the nation. NSA needs to be an honest ombudsman in that regard. And in that regard, NSA should avoid becoming a policy organization and stay where it is, which is an execution organization.

That we are supposed to be the subject matter experts for the nation's cryptologic…

INSKEEP: Were you becoming a policy organization in any way?

INGLIS: No. But there was the temptation for that. As we become more and more public, and I've said for a very long time, we were 30 miles from D.C. in every way,

shape, and form and no one would come up to NSA. We got more people from overseas visiting us than we got from Washington, D.C. for long stretches of time.

And as we become more and more public, in the public's eye, we will be asked questions of what would you do about A or B. And we need to therefore make sure that we stay on the right side of the line with respect to the policy calls. We should faithfully execute those policies. We should faithfully provide subject matter expertise about the implications, the import of those policies.

But I think that we're best served, right, if NSA stays smartly within the executive branch, as an organization that faithfully executes those policies.

INSKEEP: One other thing and then I think I'm done. I talked with Steven Aftergood of the Federation of American Scientists, who you know and who has been an advocate of the NSA disclosing more, to say the least. He feels, as you feel in hindsight, that programs such as the metadata program could have been disclosed earlier, could have been publicly debated and that the NSA did not allow that shows a lack of confidence in the public and the political process. Is he right about that?

INGLIS: No, I don't think so. I think that – I mean, I think Steven Aftergood has quite a lot to his credit in terms of very thoughtful commentary and I would not therefore kind of dismiss that thought. But when I look back, I think that the choice made was more about the concern that if we disclose that program that our adversaries would pick up on it. And that they would then modify their behavior or take whatever actions they could, right, to make it less likely that if they reached across that seam that we're trying to find that they would be detected.

Right, so if we said, for example, in April of 2013, we have a telephone metadata data program, collection program, and we therefore will look for, right, the connection between a foreign terrorist organization and the domestic U.S. But we do not have a telephone – or, I'm sorry, an email equivalent to that. We don't collect email metadata.

Then any smart, savvy terrorist worth his salt would say, got it. You know, we're going to send perhaps, you know, emails or the equivalent of emails in the digital world but never, ever, ever make a telephone call. I think that's what actually was motivating us to make the choice that we did, which is to maintain the secrecy of that for the length of time that we did.

And now that we're kind of in this new world, right, post-June of 2013, it's a much easier choice about how then do you kind of reconcile this tension? How do you achieve that greater transparency? First and foremost, we need to be completely transparent, as we've always tried to be with those who stand in the shoes of the American public, right.

Whether it's the Congress or the judiciary, we need to be completely transparent with them and give them every opportunity to understand the ins and outs of the policy choices that they would make and then confer upon us. And then second, beyond that,

we have to figure out to what degree we're going to extend that conversation to the American public. And it's still early days. Even though we're six months into this it's still early days in terms of determining how and when that might take place.

The very fact that I'm sitting here with you is a component of that, our outreach to try to figure out what's the right balance in that regard.

INSKEEP: Of course, Congress is the public's representatives on this. And this is a question I would only ask you because you're leaving. Because if you were going to continue on and testify before Congress again you'd probably be compelled to say very little about them but how's Congress doing in overseeing this agency?

INGLIS: I would say well. I would say with respect to the House Permanent Select Committee on Intelligence – so that's the House side of the intelligence oversight – and the Senate Select Committee on Intelligence, there's a fairly vigorous and I would say rigorous, right, degree of inquiries, hearings, staff-level engagements where they understand what NSA does, what its capabilities are, how we employ those capabilities. Such that, right, in the early part of June when all this was exposed, they weren't very surprised.

We know all about that. With respect to the broader Congress, well, they've got a lot on their plate, right, whether it's trying to figure the sequestration out, whether it's trying to kind of reconcile the nation's finances to its income. And then the various committees that have a depth of expertise on the things that they're charged to actually uphold, it's impossible for 535 members of Congress to be expert about all the issues that come before them.

And so there's probably some further work to be done if these issues are of interest to the entirety of the House and Senate. There's some further work to be done to bring in more of them, to expose, right, these capabilities to them. If you'd asked them before June of 2013 how much more interest they had, they said I'm OK because the intelligence oversight committees look at that.

But now this is necessarily of greater interest to all of them and perhaps to particular subgroups of them, the judiciary committees on some of them. We welcome that insight. Our doors are always open to not simply the congressmen and the senators but to the staffers who would come up here. They are, by definition, cleared for everything we do. And so we have no qualms about sharing that with them, not least of which reason is it makes for better informed decisions on their part when they do grant us the authorities that we get.

INSKEEP: Have you felt in the last few months that you've in some cases been judged by people who don't understand what you do?

INGLIS: I do. I do. I think that's by all sides. And I think that it's not always their fault. I think that in many cases people who have judged have judged us on what they thought

was a whole telling of the story. So go back to the middle of June 2013 when all that was out there were the most salacious, sensational bits of what NSA's tool set might be but people didn't understand the nature of the controls that are imposed on the use of that tool set.

Again, in the early days – we used this analogy; I'll go back to it – which is looking at the blueprint of something gives you some insight into what the possibilities are, what the art of the possible is, but it doesn't tell you anything about how you operated, how you would actually, you know, use the machine. Right, so I can study an airplane's blueprint all day long. It doesn't make me a pilot.

That doesn't make me, you know, any more knowledgeable about whether the airline that's going to fly this airplane would do this in a safe, right, thoughtful manner. And it doesn't tell me anything about the possibility that 19 individuals might get up one morning and fly these airplanes as weapons of mass destruction into a tower somewhere or some number of buildings somewhere.

And so it's – you need to know more than what the blueprints tell you. You need to know something about the culture, the ethos, the controls, and I think we're now having that discussion. People who have come to some conclusions about NSA, before they understood the totality of that, I think have been disserved, right. That they didn't necessarily come to conclusions at a time when it was right and proper to come to them.

INSKEEP: Did you, in your discussions about programs like the metadata program, weigh the possibility that at some point it was going to be disclosed? Secrets get out sooner or later. Did you factor that in, in deciding whether to go ahead or not?

INGLIS: We did, actually. And I think I gave you earlier in the interview the sense that if somebody had asked me on June 4th, hey, we're going to talk all about in the public domain tomorrow this 215 metadata data program, what do you think? I would have told you, I think we're OK. Because, you know, three branches of government have participated in that.

The controls are imposed, right, when they take the cover off that box and look at how we've used that in all 2012 you know the rest of that story. We would've said that we've actually got the balance struck, right, between the security and the defense of civil liberties.

INSKEEP: And that's true with all of the disclosures of the past six months, the monitoring foreign leaders, Prism, other things, you would've said – I mean, you calculated the risk of the disclosure of all these things and concluded that they were all…

INGLIS: Oh, that's a different question, right. So with respect to the totality of what NSA does, I think that not all of those have withstood the test of the optics, you know, or

perhaps, you know, the above the fold right side of the newspaper test. All right. Some of these things, when people kind of say you are doing, you know, you're targeting who?

You know, isn't that a dear friend of yours and isn't that something that perhaps would do you more damage than good in understanding perhaps the nature of their aspirations, expectations in the world? And so I think, in part, going forward there will be a greater time and attention given to not just whether something is authorized and whether we need to have that information in order to make our way in the world but if this is going to be a greater risk of being exposed, are we willing to kind of see that exposure take place?

But if this is going to be a greater risk of being exposed, are we willing to kind of see that exposure take place?

INSKEEP: Mr. Inglis, thanks very much.

INGLIS: Thank you very much.

Transcript via NPR.org.

#speeches and interviews#NSA#John Inglis#Chris Inglis#Edward Snowden#Section 215#metadata#FIS#FISC
7 years ago5Permalink
Share