PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

PUBLIC HEARING

Consideration of Recommendations for Change:
The Surveillance Programs Operated Pursuant to
Section 215 of the USA PATRIOT Act and
Section 702 of the Foreign Intelligence
Surveillance Act

November 4, 2013

The public hearing was held at the Renaissance Mayflower Hotel, 1127 Connecticut Avenue NW, Washington, D.C. 20036 commencing at 9:30 a.m.

Reported by: Lynne Livingston

BOARD MEMBERS

David Medine, Chairman
Rachel Brand
Patricia Wald
James Dempsey
Elisebeth Collins Cook

PANEL I

Section 215 USA PATRIOT Act and
Section 702 Foreign Intelligence Surveillance Act

Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, Department of Justice
Rajesh De, General Counsel, National Security Agency
Patrick Kelley, Acting General Counsel, Federal Bureau of Investigation
Robert Litt, General Counsel, Office of the Director of National Intelligence

PANEL II

Foreign Intelligence Surveillance Court

James A. Baker, formerly DOJ Office of Intelligence and Policy Review
Judge James Carr, Senior Federal Judge, U.S. District Court, Northern District of Ohio and former FISA Court Judge, 2002-2008
Marc Zwillinger, Founder, ZwillGen PLLC and former Department of Justice Attorney, Computer Crime & Intellectual Property Section

PANEL III

Academics and Outside Experts

Orin Kerr, Fred C. Stevenson Research Professor, George Washington University Law School
Jane Harman, Director, President and CEO, The Woodrow Wilson Center and former Member of Congress
Stephanie K. Pell, Principal, SKP Strategies, LLC; former House Judiciary Committee Counsel and

Federal Prosecutor
Eugene Spafford, Professor of Computer Science and Executive Director, Center for Education and Research in Information Assurance and Security, Perdue University
Stephen Vladeck, Professor of Law and the Associate Dean for Scholarship at American University Washington College of Law

PROCEEDINGS

MR. MEDINE: Good morning, I'm David Medine and I'm the Chairman of the Privacy and Civil Liberties Oversight Board.

Welcome to the first public hearing of the PCLOB. It is 9:20 a.m. on November 4th, 2013, and we're in the ballroom of the Mayflower Hotel, located at 1127 Connecticut Avenue NW, Washington, D.C.

This hearing was announced in the Federal Register on September 16 and October 25, 2013. As chairman, I will be the presiding officer.

All five board members are present and there is a quorum. The board members are Rachel Brand, Elisebeth Collins Cook, James Dempsey, and Patricia Wald.

I will now call the hearing to order. All in favor of opening the hearing say aye.

(Aye)

MR. MEDINE: Upon receiving unanimous consent we will now proceed.

PCLOB is an independent bipartisan agency within the Executive Branch, established by the implementing regulations of the 9/11 Commission Act. It is comprised of four part-time board members and a full-time chairman.

The board's primary missions are to review and analyze actions the Executive Branch takes to protect the nation from terrorism and ensuring the need for such actions is balanced with the need to protect privacy and civil liberties and to ensure that liberty concerns are appropriately considered in the development and implementation of law, regulations and policies related to efforts to protect the nation against terrorism.

Essentially the PCLOB has two functions, an advisory and oversight role with respect to our country's counterterrorism efforts.

I want to thank the many panelists who will be participating in today's hearing for agreeing to share their views with the board.

I also want to thank Sharon Bradford

Franklin, the Board's Executive Director, Sue Reingold, the Chief Administrative Officer and Diane Janosek, the Chief Legal Officer for their tireless efforts in making this event possible.

PCLOB has agreed to provide the President and Congress with a public report on two federal counterterrorism programs, the Section 215 program under the USA PATRIOT Act, and the 702 program under the FISA Amendments Act.

The 215 program is sometimes referred to as the business records collection program. One of the things the government collects under this program is telephone metadata for intelligence and counterterrorism purposes pursuant to order by the Foreign Intelligence Surveillance Court.

The 702 program involves collection of foreign intelligence information from electronic communications service providers under Foreign Intelligence Surveillance Court supervision.

The purpose of today's hearing is to consider possible recommendations the board might

make regarding these programs, as well as the operations of the Foreign Intelligence Surveillance Court.

Just to be clear, the questions the Board Members pose today do not necessarily represent either their views or the views of the board.

The purpose of this hearing is to explore a wide range of recommendations to assess their benefits, costs and possible unintended consequences. The Board believes it will be in the best position to make its recommendations by having public discussion of these options.

There will be three panels today. The first will consist of government officials whose agencies have varying degrees of responsibility for the surveillance programs that will be the subject of our report.

After the first panel we will be taking a lunch break.

This afternoon, the second panel will include a former Foreign Intelligence Surveillance

Act judge and two lawyers who have appeared before the court, the FISC, one on the government side and one representing a private sector client.

Finally, the third panel will include a former member of Congress and four academics who will respond to the discussion during the first two panels.

Board members will each pose questions during each panel with ten minute questioning rounds for the first panel and five minute rounds for the other two panels. Panelists are urged to keep their responses brief to permit the greatest exchange of views.

This program is being recorded and a transcript will be posted on www.pclob.gov. Written comments from members of the public are welcome and may be submitted online at regulations.gov or by mail until November 14.

Since we are still waiting for one panelist we might just take a few minutes break, or we can get started. It might be helpful to maybe just take a few minutes break.

MR. DEMPSEY: Why don't we get started.

MR. MEDINE: You want to get started? Okay, we'll jump in and then we'll pick up with the rest of the panel.

I want to introduce our panelists, Rajesh De, who's the General Counsel at the National Security Agency, Patrick Kelly, who's the Acting General Counsel at the Federal Bureau of Investigation, and Brad Wiegmann, who's the Deputy Assistant Attorney General at the National Security Division of the Department of Justice.

There were allegations in the press last week that the NSA had secretly broken into main communication links that connect Yahoo and Google data centers around the world under something called Project Muscular, which allows the NSA and the British Intelligence Agency Government Communication Headquarters or GCHQ to copy data flows across fiber optic cables that carry information among the data centers of these Silicon Valley companies.

Could the panel please explain what

that program is about and what impact it has upon the programs that are the subject of today's hearing, which is the 215 and 702 program?

MR. DE: Why don't I start on that. I'm sorry, I can't address the veracity or lack thereof of the details of the article, but I think it's worthwhile making a few general points for everybody.

Even by the terms of the article itself there is no connection to the 702 or 215 programs that we are here to discuss. I would suggest though that any implication which seemed to be made in some of the press coverage of this issue that NSA uses Executive Order 12333 to undermine, or circumvent or get around the Foreign Intelligence Surveillance Act is simply inaccurate.

As the panel will know, and as the public should know, FISA is statute that has particular jurisdictional coverage. You're either covered by FISA or you're not covered by FISA. And historically FISA was intended to cover that

type of collection that most would impact U.S. person privacy and the key factors which many learned scholars, folks like David Chris, have written about, are things like the nationality of targets, location of coverage, location of targets, where the collection and how the collection is undertaken.

I would note just as a general matter though that any collection NSA does would involve minimization procedures that are approved by the Attorney General, or if coverage were under FISA, by the FISC, that has rules in place to minimize the collection, retention and use of any incidentally collected U.S. person information.

The last point I'd make is, and I'd implore you and the public that as you read articles that may or may not be true, just to read them with the rigor that you would expect us to speak about activities.

And so in some of these articles, I think I noticed you would have a line in paragraph two of the article that says, NSA is well

positioned to collect vast amounts of U.S. person information, and somewhere around paragraph 30 you might have a line that says, it's unclear how much U.S. person information NSA collects or retains. And so I think it would be useful for everybody to read coverage with a certain amount of rigor.

And I'd leave it at that.

MR. MEDINE: Then I want to turn to the 215 program that is the subject of today's hearing. As you know there are a number of legislative proposals that have been introduced to, a range from abolish the program to modify the program, and a lot of concerns have been raised about the scope of collection, the information held by the government.

What is your response to the proposal that the 215 bulk program should simply be shut down?

MR. DE: Well, why don't I speak to the operational part of the program for a minute and then I can maybe turn it over to Brad for Justice's point of view and obviously to the FBI

for whom this program is extremely beneficial.

So from NSA's point of view, I think we've made a few points publicly which is that this is a valuable program, that along with many other surveillance tools contributes to our mission. It was intended to help cover a seam to make the connections between foreign threat streams, any domestic nexus that those might threat streams might have.

I think I'd make the point though that 215 in particular, which is the telephone metadata program, and maybe I should just start with some basics since obviously the panel is well-versed in this program, only involves telephone metadata. It does not involve any content of telephone calls, it does not involve any identifying subscriber information, and NSA does not collect any cell site location information.

This tool is used primarily as a discovery tool in order to discover, unearth potential leads to domestic ties to international threat streams. And if such tips are evidenced we

hand them over to the FBI for further investigation.

I think though that in the public debate there's been a lot of discussion of, name a plot, that without this tool inevitably would have happened, and I think that's probably not the right question to ask.

From the intelligence community's perspective intelligence is a function that is brought together by lots of different tools that work in complement to one another.

And I would also suggest that any particular plot, it's rare that you're going to find a situation where some particular event was only unearthed or only stopped as a result of one particular intelligence tool. And I think that probably misleads the debate in terms of the value of the program, but I'd ask my FBI colleagues and DOJ colleagues to weigh in.

MR. KELLEY: We find the 215 program to be very helpful to us. We, since 9/11 have been charged not with retroactively solving, which we

continue to do, but on the national security side to prevent terrorist attacks. Now that's a fundamentally different and much harder thing to do. So we need information.

This is one tool. It's not the only tool. It's not a tool that we can say is absolutely must have. It is extremely critical though and helpful to us. When we try to connect the dots, the more dots that we have to connect, the better off we are in accomplishing our mission of preventing terrorist attacks. So the program that we have here -- good morning.

MR. LITT: Sorry I'm late. Transportation into Virginia is a little difficult, although I will note that the panel started early.

MR. KELLEY: As I said, the 215 program as Raj indicated provides us with metadata. It does not provide us with content of communications, just data such as the number from which a call was made to the number that is dialed, the length of the call and the date of the

call.

So it's primarily of interest to us because we may have telephone numbers from our own other tools, investigative tools, but we may not realize the significance of the number, without the 215 abilities that NSA has to analyze that data and then provide context to us in turn, we may not realize the significance.

It provides a way for us to be agile. It provides a way for us to respond more quickly. Time in counterterrorism investigation is a very important element. It has resulted in several cases over the years, more than several, being opened that we may not have otherwise opened.

It has also permitted us to focus resources. We may have had a preliminary investigation, for example, open and then when the information came to us that this number we had was contacting a known or suspected terrorist safe house, for example, overseas, it then would provide us the requisite articulation of facts to escalate that preliminary investigation to a full

investigation.

That in turn allows us to focus our resources better and focus our energies and our investigative efforts.

I think that over the years we've had a number of open declarations filed that give us an indication of the value of the program. In 2009 Director Mueller filed an affidavit with the FISC Court that indicated that at a particular time there were 27, I think, full investigations open.

It's very difficult in any particular investigation to say that this fact or that fact is very important, but over time we can say that these things are extremely helpful to us. So we do think there's value in the program.

MR. MEDINE: I guess my question is if the program was discontinued would it be a practical option as some have suggested to just gather information from the telephone company providers rather than having NSA maintain data on all Americans' phone calls?

MR. DE: Let me defer to Pat on the use

of NSLs perhaps, which would presumably be the alternative.

MR. KELLEY: If we did not have this program and used other lawful investigative ways to obtain particular phone numbers from particular subjects, we wouldn't be able to see the patterns that the NSA program provides us.

We would be able to, for example, through the use of a grand jury subpoena or a national security letter on the national security side, obtain information about a particular phone number and we'd get the first tier of the phone numbers that that number had connected with, but we would not be able to go into a second tier or a third tier, hops it's commonly called, which the NSA program provides.

Additionally, we would be able to perhaps go to service provider, to service provider, to service provider and then individually try to connect those dots, but without the ability to look at all the data in a composite way, it would be much harder, it would

be much slower, much more difficult for us to do that.

So with those two indicators there, we'd be less agile, we'd be less informed, and we'd be less focused and we think that as a result we'd be a lot less effective in preventing the attacks that the American people want us to prevent.

MR. MEDINE: I see that my time has expired. Ms. Brand?

MS. BRAND: Thank you, Mr. Chairman.

Let me just follow-up on that since your time ran out. I had some questions related to the same subject.

Even if you were able to use a grand jury subpoena or an NSL to go provider to provider to ask for the information, would the information be there without a record retention requirement?

MR. KELLEY: That's a very good question. Without the 215 program it would be up to the service provider to determine how long they would keep the records. I think FCC regulations

require them to keep these things for 18 months. The NSA program keeps them for five years.

So the likelihood without the 215 program would be that much of that information would simply not be there, so there would be no dots to connect.

MR. LITT: Can I add something on that?

MS. BRAND: Sure.

MR. LITT: It's my understanding that FCC regulations, and I'm not an FCC lawyer by any means, but that the FCC regulation relates to toll billing records.

It's not at all clear to me that if all providers moved to a system where there are no longer -- first of all, that doesn't include local calls. And second, if providers move to an environment where none of them are billing for toll calls at all whether those records would be retained even pursuant to the FCC regulation.

MS. BRAND: Thank you. You just answered my next question.

MR. LITT: Sorry, Rachel.

MS. BRAND: Perfect. No, that's good.

Relatedly, we've heard some talk about sort of a competition downwards in terms of retention requirements where it's not required by FCC regulation that providers for sort of commercial competitive reasons would decrease their own record retention periods. Have you seen any evidence of that actually happening or is that more of a theoretical concern?

MR. DE: I can't speak to that particular issue but I probably should add one other point in addition to what Bob and Pat made. In order to run a program like the 215 program the data has to be provided or kept in a way that allows it to be integrated.

And so I think in addition to the availability of the records, they have to be available in a way that would allow for the sort of analysis that the 215 program allows.

MS. BRAND: Can you, any of you, speak to whether there might be some privacy concerns that would be created if, just posit for a moment

that there is a record retention requirement of, say, two years for something more than toll billing records, or perhaps even just toll billing records, does that in your mind create additional privacy concerns?

And relatedly, would there be any reason why those retained records could not be sought in civil litigation, divorce proceedings, criminal proceedings, immigration proceedings or any other kind of legal process?

I don't know who wants to take that, maybe DOJ. Brad, do you want to?

MR. WIEGMANN: Sure. So, you know, these are records that the companies keep for at least some period of time now and they can be obtained, as Pat mentioned, through an NSL or through grand jury subpoena, etcetera. So these are records that don't enjoy Fourth Amendment protection under the Supreme Court's holdings.

But I think the longer you require the companies to keep them, then that's data that is being kept by a company for a longer period of

time.

So if you create a five-year period then that's information that's available there and can be subpoenaed. You know, private lawyers can subpoena the data. I mean the data is not, it's not private in that sense, but to the extent people have concerns about the data being compelled, it would be held for a longer period of time by the private sector rather than by the government. So that's at least conceivably a privacy concern for them.

MR. KELLEY: In addition to that, once the data's destroyed by the companies, of course then it's not available, which is on the privacy side a good thing because hackers can't get into it, and as you indicated in your questioning it couldn't be used for other purposes.

I've been told, for example, that if the data exists, other levels of law enforcement from local, state, federal would want it for whatever law enforcement purposes they were authorized to obtain it, and civil litigation

could also seek to obtain it for such things relatively mundane as divorce actions. Who's calling who and your spouse if it's a contested action, for example.

So if the data is kept longer by the companies then I think the privacy considerations certainly warrants some scrutiny.

MS. BRAND: The hacking point that you raised is to my mind both a national security concern and a privacy concern, but I have to ask in light of some of recent revelations, do you think that, is the data in the government's possession more protected from hacking than it would be if it were in the possession of the private sector? And what are you doing and what can you do to make sure that it is?

MR. DE: I think that's a great question and I think that any evaluation of where else to keep such data should take that comparison into account.

So we don't have any reason to believe, based on current assessment, that Edward Snowden

had access to raw material in the business records database. Now why is that the case?

I think I'd make the case that the current program is one of the most highly regulated programs in the federal government today and I think that regardless of the benefit of folks who have privacy concerns or interests in the protection of such data.

So what do I mean when I say it's a highly regulated program? For one, pursuant to the court's orders, the data has to be kept segregated from all other types of raw intelligence.

Two, the purpose of the program is purely for counterterrorism purposes so this data can't be used for other purposes, as we've just been discussing might be the case in other circumstances.

Three, the program is re-authorized every 90 days by the Foreign Intelligence Surveillance Court. We at NSA, together with Justice report to the FISC every 30 days on the

use of the data. The program is audited every 90 days by the Department of Justice.

Pursuant to the court's orders only 22 senior officials may approve queries into the data and those queries have to be based on a reasonable articulable suspicion that the number used is associated with a specific foreign terrorist organization.

Only seven officials by court order are authorized to disseminate information to the FBI, for example, if any U.S. person information is involved.

There are significant technical controls limiting access to the data. So for example, a typo in this case can't go through in a query because there are technical controls that only allow RAS approved numbers to be used as query terms.

And finally, pursuant to the court's orders there are rules for the Inspector General at NSA and of course we have oversight from the Department of Defense which has its own inspector

general, as well as the ODNI which has its own inspector general.

MS. BRAND: I just want to follow-up on the RAS, the reasonable articulable suspicion standard, and I have a series of questions which I'll continue in the next round if I need to.

But can you explain what that means? What is RAS? Give me an example of how much information would be enough to meet it. Is this the Terry stop standard? Is it something more?

MR. DE: So this is a legal standard that does sort of have origins in Terry stop jurisprudence. And I'll turn to Brad in a minute to articulate that.

But what that would mean is it's effectively the same standard that's used for stop and frisk for a law enforcement officer to pat down somebody on the street. Every single RAS determination has to be documented before a query is made.

MS. BRAND: But give me an example of what would be enough. Give me an example of sort

like the basis for a RAS determination.

MR. DE: So it could be, for example, through other intelligence a known connection of a telephone number to an Al Qaeda operative, for example.

The intent of the standard is to be significant enough that a query can't be made on a hunch or for no particular reason at all, but sufficiently able to be met so that the tool can in fact be used as a discovery tool to discover unknown operative, which is the whole point of the program.

MS. BRAND: And what is the paper trail, what kind of records create the basis for a RAS determination?

MR. DE: So every RAS determination is documented and kept in a computer database. They are only, every RAS determination is only valid for a set period of time pursuant to the court orders. It's 180 days if it's a U.S. number or 365 days if it's a non-U.S. number.

NSA as a matter of proactive

compliance, reexamines RAS determinations in half that time. Every 90 days the Justice Department comes to NSA and audits RAS determinations, written RAS determinations, as does our Inspector General, pursuant to the court's orders.

MS. BRAND: And after 180 days does the RAS selector disappear? Can you get it re-authorized? What happens with that?

MR. DE: It may not be used to conduct queries unless a new RAS determination is made or a continuing viability of the existing RAS determination.

MS. BRAND: And what's that re-authorization process? Is it simply reliance on the evidence that was provided the first time or does that evidence have to be reverified?

MR. DE: It certainly has to be reverified as of the time of the determination. So any time a RAS determination is made the information used to support that determination has to be to the best of our knowledge current at the time of the determination.

MS. BRAND: So one suggestion that we've heard to improve the process would be for DOJ to have more involvement in the RAS process, the process of approving a particular RAS selector. I think the theory there is that DOJ has more experience with determining whether standards of proof have been met.

Does the administration have a position on that suggestion? Brad, I'm looking at you because you're from DOJ, but anyone can answer it.

MR. WIEGMANN: I really think I understand that argument but I think the better analogy is to the operator on the street who's making that determination. I mean lawyers don't make that determination if there's reasonable articulable suspicion to stop someone and frisk them on the street because they're suspected of criminal activity.

I think for the same reason here we're not going to be in as good a position as an intelligence operative is to know whether there's suspicion that a number is associated with a

particular foreign terrorist organization overseas. So I think we've got it about right where we have it now to leave that with the operators.

So the example I always think of, you ask what would be a RAS determination would be, you know, a laptop is obtained when a foreign government arrests a terrorist overseas and that's a laptop that we believe is used to communicate, that terrorist has used to communicate with other terrorist operatives, and on that laptop there's a bunch of phone numbers.

That's the type of situation where a phone number obtained on that, and you look up and you see there's a U.S. phone number, the government wants to know who is he calling in the United States.

And so that's the kind of classic example I always think of, and that's something I think that's really more operational and not so much a DOJ lawyer sitting back in Washington making that judgement.

MR. MEDINE: Thank you.

Ms. Cook?

MS. COLLINS COOK: Thank you. And I wanted to thank you guys for coming today. I think it's helpful to have the opportunity to ask some more and more specific questions as we are moving through our process of analyzing these programs.

I did want to ask one follow up question, Brad, on what you were just talking about. It's certainly true that the police officers are the ones on the street making the determination in a specific case, but that's typically after a long period of training, a lot of thought given on how the training is developed and implemented.

To what extent is DOJ involved in the development of the RAS standard, the training of that and the oversight to ensure that the operator on the street is in fact appropriately using the RAS standard?

MR. WIEGMANN: Well, we do, as Raj

said, we do review each and every RAS determination after it's made at the Department of Justice. We're not doing it in real time because we think, as I said before, and on the front lines that's the operators who are in the best position to do that.

But also to say, the point I didn't make was that this is designed as kind of an alarm system. It's a kind of rapid reaction program so that the government, when they have this number they want to know right away whether that number's calling any numbers in the United States to see whether we can find out if there are any contacts and whether there's terrorist plotting that's occurred.

But given a little more time, absolutely, lawyers are involved, heavily involved in reviewing every single RAS determination to look back at all the facts and say, was there enough there.

So there is that kind of balance. You have both the operators, but then the lawyers come

in after the fact to make sure that those were all correct.

And if we were to find a compliance problem with a RAS determination that would be reported, and is reported, to the court, again, in conjunction with those 90 day reviews that Raj mentioned.

MR. DE: If I could add one point onto this. I think the now-public court orders authorizing the program expressly articulate that which actually happens in practice, which is we and Justice work together on all significant legal interpretations of the 215 program and that includes training materials and other things like that.

MS. COLLINS COOK: So I wanted to go back to something you had mentioned earlier, Raj. You started off by saying that there's a lot of talk about how many plots have been disrupted or thwarted, and you said that's not the right question.

So I have a two-part question for you,

what is the right question and how frequently is the Department of Justice asking the question, how often is NSA asking the question in a serious and systematic way, is this an effective program? It turns out it's going to be a three-part question, and when you do so what metrics are you using?

MR. DE: So I think that is a very valuable question to ask across the board for NSA intelligence programs, and I'm sure Bob will speak to intelligence programs regardless of the agency. So let me give you a few data points for the 215 program.

As I mentioned, this program is re-authorized every 90 days by the FISC --

MS. COLLINS COOK: Actually can I stop you there. I'm asking about the effectiveness of the program and not necessarily compliance or whether it continues to meet legal requirements, but as a counterterrorism tool, whether as rapid response, as Brad, you've characterized it, or prevented it, as Pat, you've characterized it, the effectiveness of the program.

MR. DE: So every 90 days we submit a declaration both from NSA and from the intelligence community that articulates the need for the program and how, as part of the relevant standard.

And so in other words, the standard to make the relevance showing needs to articulate why such telephone records are helpful in the counterterrorism mission, to put it in lay person terms.

And so I would say at a minimum every 90 days there's some internal mechanism built-in to at least revalidate the program.

I'd also add that as Congress has been doing recently adding legislative sunsets to provisions, regardless of whether one thinks that's a good idea or a bad idea, that is a built-in idea that Congress should reevaluate the effectiveness of intelligence programs.

The 215 program was re-authorized twice within the last five years and apart from current efforts is up for expiry in 2015. And so those

are natural points to evaluate the effectiveness of the program.

The third thing I'd mention is like all federal agencies, NSA has significant resource constraints and so apart from the mission value of the program, we are constantly reevaluating all sorts of programs, particularly expensive ones like the 215 program, to see if they're worth the expenditure.

And then the fourth data point I'd add is there's been some public discussion of another metadata program that was conducted on email metadata that's no longer in existence. And that program was ended in 2011 precisely for the reason you raise which was, at least in part, an evaluation was made that it wasn't meeting operational effectiveness needs.

MR. KELLEY: And if I could add to that, it's very difficult to say, just say we've stopped this number of attacks, or opened this number of cases, or produced this number of intelligence reports. But as I indicated before,

we have provided publicly some numbers and some illustrations, including a plot that was to bomb the New York subway system. So that's one case and one plot disrupted.

There was a similar attack in Madrid several years ago, as you know, and hundreds of people were killed and wounded in that single attack.

So when you evaluate effectiveness, it's not just numbers that you have to look at, but you have to look at victims who are no longer victims or never were victims. And I think to put everything into context here is very important. So I think that question deserves a lot of public attention and looking at the full spectrum of the value includes everything from people who are not victims up to intelligence reports that are produced.

MS. COLLINS COOK: You had mentioned earlier in response to some of the questions that Rachel had asked that you could end up with a situation without the 215 program where you would

have data perhaps up to 18 months, the age of the data would be 18 months, as opposed to five years now.

To what extent do you in a systematic and regularized way assess the helpfulness of the data that is two years old, three years old, four years old, five years old? Is there an empirical basis for believing that these older records are still in fact useful?

MR. KELLEY: I'm not aware of any study where we've gone back to look at those specifics. But again, in this counterterrorism environment we have to look in terms of a very broad programmatic review, not just attacks thwarted but how terrorism organizations exist, what their finances are, what their objectives are, how they operate.

So if we, for example, had a different type of tool to obtain numbers, most of those numbers that we would obtain would be going forward. We wouldn't have the ability to look back. So if the data is retained for a shorter period of time then ours to analyze is also

reduced.

So again, I don't think that we can put precise numbers or definitions on it, but I do think that in the long run the more dots we have to look at these analytical or through these analytical tools, then the better we will be at connecting them.

MS. COLLINS COOK: And I just wanted, I think I have -- yes, good, I still have a little bit more time. You had indicated there could be limits on the use of either grand jury subpoenas or NSLs because you would only get what you referred to as the first hop. But couldn't you do sequential NSLs or sequential grand jury subpoenas to obtain exactly that second or third hop type of information?

MR. KELLEY: I think we perhaps could. I don't know if we could get the second and third layer, as you said, without going repeatedly. We would end up probably going to court very frequently and very routinely.

As Raj indicated, the systems that we

have, we have to go back to court every 90 days as it is and get the determination of the court that what we're doing is warranted, and part of that includes the relevancy and the value judgement that allows the system to go forward.

MS. COLLINS COOK: Although just to be clear, you would not have to go to court to use national security letters.

MR. KELLEY: No, I'm sorry, that's correct.

MS. COLLINS COOK: Which may be a different reason not to use national security letters, but just to be clear on that.

MR. WIEGMANN: So I think part of the concern on that is that, one, it's a slower process to issue NSLs and grand jury subpoenas, and as Pat said, you have to do it repeatedly.

And then critically you'd have to do it across providers. So if you have multiple providers participating then you have to go to provider A, and then if that number calls someone, the number is for provider B then you have to

issue an NSL to provider B and C, and then you see the networking. In other words, you're having to do multiple.

And if those numbers are calling numbers back again across the different data streams from different providers it makes it infinitely more complicated to start to try to do NSLs or grand jury subpoenas to multiple different providers for multiple hops. So I think that's part of the reason why it's complicated.

In addition to the fact you said about how long is the data to ensure as a legal matter that it has to be retained. And again, I think it's important to say that some of these providers may retain the data voluntarily for a length of time but without something like this order you don't have a guarantee that they're going to keep the data.

MR. MEDINE: Thank you.

Mr. Dempsey?

MR. DEMPSEY: Thanks, and good morning again. Listening to the discussion about the RAS

and you know, thinking about Terry vs. Ohio, which is the reasonable specific articulable facts giving reason to believe, it seems to me there are two issues there.

One of course is when you think about it, that's the very standard the New York City police has used in its stop and frisk program, which is at the very least highly controversial and a lot of people feel has ended up being implemented in a discriminatory way. The police in New York City would say, well, every single one of those stops was based upon a RAS.

Secondly, in the police stop case it seems to me that the good aspect of it and the bad aspect of it is, is that the issue is resolved immediately. Either the police find something and they arrest you or they let you. Again, in New York there was the humiliation of being stopped, which is not nothing clearly, but it's resolved immediately.

And it seems to me that you've picked up the first half of Terry, specific and

articulable facts giving reason to believe, but the second half of Terry was that some criminal activity is afoot, that there's some suspicion of criminal conduct which you resolve immediately through the stop, which is the purpose of the stop.

But here I'm wondering about the second half, so specific and articulable facts giving reason to believe, and then it seems to get vaguer that the selector being used is associated with a terrorist group and associated -- is there a way to make that more concrete?

You cite the example of, well, we've got a terrorist's computer and there were phone numbers in it. Well, yeah, let's find out who those phone numbers are calling and are any of them in the United States.

But what else could associated with mean? And then how can you give it more concreteness so you avoid this problem?

Because it seems to me that you make the determination and then the information is

tipped, so to speak, or given to the FBI to pursue. And it's not the kind of thing that can be so immediately resolved.

So I'm wondering even is the Terry example the right reference point here, or is there another way to define what you're looking for? You know, reason to believe that a search of the number will be likely to uncover somebody in the United States who may be engaged in terrorist activities for example, something more definitive than this just associated with.

MR. LITT: So let me offer some comments on that. The first is that I think actually the comparisons to the police Terry stop all run in favor of this program as a considerably lesser intrusion. For one thing I think the actual degree of intrusion based on the determination is considerably less.

A Terry stop involves a policeman stopping you and frisking you on the street, which is by itself a considerably greater intrusion on a person's privacy than simply running a telephone

number that's not associated with any individual name against a bunch of other telephone numbers that aren't associated with any individual name.

The second thing is that the consequences that can flow from that are considerably different. Obviously one of the consequences that can flow from a police Terry stop is an immediate arrest without any subsequent review, without any intervening review or judicial determination.

In this case the only consequence that can flow is that a telephone number is tipped to the FBI for further investigation, and that further investigation requires independent legal justification. And in particular if there's any desire to intercept anybody's communications, any American's communications, that requires a judicial warrant based on probable cause.

The third difference I think is the degree of oversight. As was mentioned before, to my knowledge generally speaking there's no systematic oversight by prosecutors and/or

inspectors general and/or others of day-to-day determinations that lead to Terry stops by police. That's one of the reasons why there's the litigation in New York. As Raj has said at some length, there is systematic oversight here.

So I think that all of those determinations make this a considerably lesser intrusion than the police Terry stop.

In terms of the possibility of an alternate standard, obviously there are a number of alternate standards that could be applied. But the important thing to remember is that this program is a discovery program.

The whole idea of this program is to identify avenues that warrant investigation and to rule out avenues that don't warrant investigation. And the more you require, the more you add on to the standard that's required before you can even investigate, the less useful the tool becomes.

So for example, if you talk about reason to believe that the number may lead to a contact in the United States, well that's exactly

what we're trying to find out here. We've got a number. If we've got a terrorist's phone number, exactly what we're trying to find out is do we have information to think that this may lead to productive investigation in the United States.

MR. DEMPSEY: And just one quick thing Raj, if I could. On the question of follow-up, Pat or others, there's very close review of the RAS determinations itself. What sort of review is there of how does the FBI use the information that is generated?

MR. KELLEY: Well, we use the information, as Bob indicated, to further our investigative efforts, so we can open a preliminary investigation perhaps or we can open a full investigation.

MR. DEMPSEY: But my question is, does the, sort of review process go and look at what was the outcome, how was it used, how did we confront or not confront an individual? Sort of tracing all the way down to the street or to the FBI's follow-up investigation, what sort of

assessment or tracking is there of that?

MR. KELLEY: Well, I think what you're referring to is our oversight and compliance efforts. We have both internal and external up to and through Congress, as well as the Department of Justice, the Department of Justice Inspector General, the Department of Justice Office of Intelligence routinely do reviews and audits internally.

From the street level, for example, the investigative cases that we have are reviewed by supervisors every 90 days to see what the status is.

In addition to that, the FBI has an Office of Integrity Compliance where we are continuously looking at the risk that we will, in executing our mission, not to follow the letter of the law.

So through all of those internal and external systems of oversight we are continuously reviewing the way we conduct our business.

MR. DEMPSEY: Raj, you had a point?

MR. DE: I want to add one point. Just to put a fine point on the comparison to the New York controversy because I think at NSA we're really worried about conflation of the public record, so I just want to give folks a sense of what using the Terry stop standard means here, the comparison to a stop and frisk.

That would mean a police officer writes down the reason for a stop and frisk, as we do for telephone metadata, before they did that activity.

It would mean that only one of 22 supervisors would approve that stop and frisk before it happened.

It would mean that, in our case, the data is all anonymous, as opposed to a stop and frisk where have a physical human being, Bob was alluding to that point, in front of you.

The stop and frisk standard, we have post-query audits every 90 days, so that would mean a police department audits every 90 days what happened.

And we also report to a court every 30

days and get it re-authorized every 90 days.

So while, yes, in some legal sense the standard, the legal standard derives from the Terry stop standard, I think just those factors alone distinguish the use of that standard in this context and clearly evidence that it's a far, far more regulated and rigorous process than is feasible in the physical search context.

MR. DEMPSEY: Thank you.

Judge Wald?

MS. WALD: Thank you. I'm going to open with a kind of a general question. Since the revelation of the 215 program, which was a secret program before, there have been, as you well know, a plethora of suggested reforms, quote, reforms, or suggested changes, etcetera.

I'm interested in whether or not you think any of these suggested reforms that you're aware of deserve, not just serious consideration, but perhaps adoption.

Let me just give you sort of an example. It was a secret program, it's now no

longer the fact of the program and many of its operational details that the government has revealed, are no longer secret.

Now I assume from the fact that you're here today and from many of your answers that you think that the program deserves to be continued. So there are two parts to my question.

You know, one is whether or not any of the reforms suggested by various people that you think are worthy of consideration, or two, do you think the fact that you want the program to continue could cast some doubt on the need for secrecy of the fact of the program to begin with, which of course is one of the big questions being debated, whether or not when you have a bulk collection program of any kind that affects a lot of citizens, a lot of residents, the fact of that program, if not all the details of its operation, deserve to be debated publicly in Congress and known to the public?

It's kind of a double-barreled question. I'll let anybody that wants to.

MR. LITT: I'd like to take a crack at that, but first I have a personal favor to ask and that is if Jim Dempsey could turn his tent a little because the floodlight is shining. Thank you very much. I'm getting blinded by it.

So to answer your second question first about secrecy, I don't think you can draw from the fact that we want the program to continue the conclusion that the program should never have been secret.

There are many intelligence programs that operate more effectively when they're not known because disclosure of what we obtain and how we obtain it can enable our adversaries to avoid or take steps to avoid what we're doing.

That said, that doesn't mean that once they've been disclosed they're entirely ineffective. There's no question in my mind that this program is at least potentially less useful now than it would have been before disclosure. Whether it's actually less useful or not is going to take time to determine.

But going forward obviously we have declassified and released the last two orders of the FISA Court and we are obviously under the President's direction in a more forward leaning mode with respect to transparency.

But we still, as sort of custodians of the intelligence apparatus that protects the nation, we still have to be sensitive all the time to the fact that disclosures do risk compromising our capabilities.

With respect to your first question, I think that we have repeatedly said that we're open to consideration of a variety of possible reforms to the program, so long as they don't eliminate its utility.

We've talked about shorter retention periods. We've talked about possible limitations of the number of hops that we can make queries out. We've talked about some sort of process for after the fact review of RAS determinations by the FISC. We've talked about providing greater transparency as to the manner and the extent to

which the program is used.

All of these are subject, again, to the qualification that we don't want to impose such restrictions, that they would eliminate the utility of the program. And we don't want to impose on ourselves burdens that we can't meet. Some of the transparency proposals are things that we simply can't do with any reasonable effectiveness, so.

MS. WALD: But to follow-up a little bit on that, there have been some articles recently in the paper, and I think they contain some polls, I know there are lots of polls, but suggesting that there's widespread public distrust of NSA as a result of many of the revelations over the last several weeks.

Do you think that there's some need for some, whatever you want to call it, remedial effects, making changes, some more types of public disclosure?

For instance one, you've suggested that there may be, but one area that's covered in some

of the bill in Congress is that need for a more, I think the word used is secure foundation for the 215 program and specific, legislative. I know it's been re-authorized, but in a specific legislative acknowledgment of that program.

There's certainly been a fair amount of confusion and some criticism of the fact that if you read 215, the public records bill, on its face, you don't get much notion that this might be involved, etcetera. And so as you know, some of the efforts are said to put it on a sound specific legislative basis that everybody knows what you're going to do or that there is such a program, etcetera. What are your feelings about that?

MR. DE: Can I speak to the first point, Judge, which I think --

MS. WALD: Yeah, sure.

MR. DE: Is a very valid point. So you know, as the General Counsel for NSA my first duty to is to make sure that our activities are lawful.

But I view my role and all of the senior officials at NSA to ensure the extent

possible given the nature of our work, the public legitimacy of what our agency does. There is no doubt that is an important factor.

That being said, I think this particular program had historically all the indicia of institutional legitimacy that one could expect given the current setup of the FISC and institutional oversight that we have.

So in other words, and some of this is obviously known to you all but just to make sure members of the public are aware, not only was this program approved by the Foreign Intelligence Surveillance Court every 90 days, it was twice, the particular provision was twice re-authorized by Congress with full information from the Executive Branch about the use of the provision.

Now as to whether that should be codified separately or not as a confidence building measure, for all intents and purposes I think the public debate we're having now effectuates the public legitimacy aspect of the program, and we'll see how it plays out and how

the reform measures are taken.

But I don't think a separate codification is necessary for the legal legitimacy of the program but I think your point is well taken that public confidence needs to be ensured. I would only suggest that to the extent public confidence is shaken, in part that is as a result of historical secrecy and in part it's a result of a large amount of misinformation and confused public debate. And it's hard to separate the two. Those are two, they're intermingled of course. And so I think it's the former that is certainly necessary for a democratic institution to continue.

MS. WALD: So if there were another -- I'm sorry, go ahead.

MR. LITT: I just want to add one very brief comment to Raj's in terms of the extent to which Congress was kept informed. By statute we're required to provide copies of significant opinion and decisions of the FISC to the Intelligence and Judiciary Committees of both

Houses of Congress and they got the materials relating to this program, as we were required to by law.

MS. WALD: So last question on my last minute. If there were, if there were another bulk data, metadata program type to come along, based on your experience with this, all that's happened with 215, do you think it would be desirable, undesirable for it to become a matter of public knowledge and open discussion in Congress? Not the details of the program but that there was to be a bulk program which would affect a large amount of the citizenry?

MR. LITT: So I think that really very much depends upon the nature of the program and what it is.

I think if the nature of it can be disclosed without compromising intelligence sources and methods, then that's something that would be considered.

But if the public discussion is going to lead to a considerably disclosure of sources

and methods, I don't see how we can do that. This is why the Intelligence Committees of Congress are set up. This is why we're required to notify the Intelligence and Judiciary Committees of things that we do pursuant to FISA because they essentially stand as the proxies for the people in overseeing sensitive intelligence collection programs.

MR. MEDINE: I guess we'll turn to the subject of oversight of the program. As I understand it there is judicial approval of the program itself but there is not judicial approval of the selection of particular phone numbers, the RAS determination, reasonable articulable suspicion, either before, nor is the court afterwards apprized of what selectors have been chosen so that they can evaluate whether the program is operating consistent with the authorization for the program itself.

Would it be practical, assuming that there was an exception for exigent circumstances, where there was an urgent need to pursue a

particular phone number with perhaps after the fact reporting, would it be practical with that exception for the court to approve the RAS determination in advance or to review RAS determinations after the fact, perhaps as part of the 90 day review process and approval process, to make sure the program is operating as the court expected it to be operating.

MR. DE: So we are, we're certainly open to an increased role for the FISC, I think. And the same, in particular I know ODNI and other agencies feel the same.

I'd make a couple of points. One, I think among the criteria that are necessary to maintain the usefulness of the program, we've heard a variety of things this morning. We tend to summarize them in sort of four kind of major buckets.

One is maintaining privacy protections. We hit on that earlier. One is maintaining the comprehensiveness of the data. The third is maintaining the depth of the data, the number of

years you keep it. And the fourth is operational agility, getting to the question you've just raised.

I think we have concern that it will be difficult and not practical to preserve the operational agility of the program, to have ex-ante approval by a court for every RAS determination.

But I think you've raised a very valuable point that we currently have reporting requirements to the FISC, and in fact we report to the FISC every 30 days in fact, even though the program is authorized every 90 days. And so that 30 day vehicle could well be a useful vehicle to provide RAS determinations to the FISC, for it to review the documented determinations that are made today.

I'd just note that those determinations, and Brad mentioned this earlier, are currently reviewed by the Justice Department. But to the extent it builds public confidence I think it would be of no concern for NSA in

particular to have the FISC review those after the fact.

MR. LITT: One concern that we have actually talked about in our own internal discussions with the idea you articulated of ex-ante review with an emergency exception is that given that the nature of this program is such that we're frequently operating in exigent circumstance we'd be a little uncomfortable with a scheme that's set up where the statutory exception essentially swallows the statutory rule.

MR. MEDINE: And what about after the fact? The court has, I think indicated publicly that it's difficult for the court to assess compliance with its own orders. What if there's a mechanism for every 30 days to report back on the RAS determinations that were made so it wouldn't interfere with operational concerns but it would give the court the chance to, say, correct direction if you're exceeding the court's expectations or give validation if you are squarely within what the court expected you to be

doing?

MR. LITT: I think that that's something we're very open to, to considering. Obviously all of these things, it depends upon what exactly the proposal is, but I think that in concept that's something that we would be comfortable with.

MR. WIEGMANN: We also have to keep in mind the burdens on the court as well and what their resources are to do that. But for the reasons that Raj and Bob explained, I agree that post, ex-post review of RAS is an idea worth considering.

MR. MEDINE: I want to shift to the 702 program briefly, which is the electronic communication service provider program. As we know, over the last couple of weeks there's been a lot of concern by non-U.S. persons, foreign citizens about being subject to surveillance.

What are your thoughts about whether, that this program essentially is designed to focus on the rights of U.S. persons being surveilled and

court approval for U.S. citizen? What do you think about extending some degree of protection to non-U.S. persons who are being, whose communications are being reviewed pursuant to the 702 program?

MR. DE: So I think maybe I can start and then you can speak. Just as a general matter, one, there is in fact for all of our collection a policy process in place, an interagency process to determine that for which we conduct foreign intelligence generally.

And so I would like to make sure folks don't have the misimpression that intelligence gathering is not directed in the first instance.

Secondly, all collection has to be related to an authorized FI purpose. That includes our 12333 collection.

And our 702 collection in particular has to be conducted pursuant to certain certifications that are submitted to the court for particular foreign intelligence purposes.

The third point I'd make is that even

though we have a number of protections in place for U.S. person, information beneficiaries of that also are foreign nationals who may be subjects of investigation. So in other words, our retention limits and other protections that are currently in place in fact serve as protections for any subject of intelligence collection.

And then fourth, I know the DNI is currently considering whether we want to document any further protections for non-U.S. persons beyond those that are articulated today.

MR. LITT: So if I can just follow on, there is I think a good reason why not only the United States but most nations provide a greater degree of protection for their own citizens and nationals and others with respect to intelligence activities.

Historically the great fear of intelligence agencies has been that like the example everybody always gives of the Stasi, that their powers will be directed inappropriately towards repression of their own citizenry. And I

think that's why historically in this country we have a greater degree of protection for U.S. persons, but as Raj says that doesn't mean that there are no protections for other persons.

In that regard I think it's worth noting the letter that the NSA Inspector General sent to, I believe it was Senator Grassley a month or six weeks ago, which has now been released publicly, which identified a dozen or so instances in which they had determined that NSA personnel had inappropriately used collection authorities.

And I believe that the majority of these involved -- first of all, they were all under Executive Order 12333. None of them were under FISA. There's never been a finding of a willful violation of FISA.

But even in this case the majority of these were improper queries of information about non-U.S. persons. And so it's not only the fact that we have rules that protect non-U.S. persons but those rules are actually enforced. These people were disciplined or resigned from NSA as a

result of this.

And I would just reiterate what Raj said, which is that we are open to considering whether there's some value in formalizing and making more public the rules that we do have for protecting the personal information about non-U.S. persons.

MR. MEDINE: And so turning to the protections for U.S. persons, as I understand it under the 702 program when you may target a non-U.S. person overseas you may capture communications where a U.S. person in the United States is on the other end of the communication.

Would you be open to a warrant requirement for searching that data when your focus is on the U.S. person on the theory that they would be entitled to Fourth Amendment rights for the search of information about that U.S. person?

MR. DE: Do you want me to take this?

MR. LITT: Thanks, Raj. Raj is always easy, he raises his hands for all the easy ones.

MR. DE: I can speak for NSA but this obviously has implications beyond just NSA as well.

MR. LITT: I think that's really an unusual and extraordinary step to take with respect to information that has been lawfully required.

I mean I started out as a prosecutor. There were all sorts of circumstances in which information is lawfully acquired that relates to persons who are not the subject of investigations. You can be overheard on a Title III wiretap, you can overheard on a Title I FISA wiretap. Somebody's computer can be seized and there may be information about you on it.

The general rule and premise has been that information that's lawfully acquired can be used by the government in the proper exercise of authorities.

Now we do have rules that limit our ability to collect, retain and disseminate information about U.S. persons. Those rules, as

you know, are fairly detailed. But generally speaking, we can't do that except for foreign intelligence purposes, or when there's evidence of a crime, or so on and so forth.

But what we can't do under Section 702 is go out and affirmatively use the collection authority for the purpose of getting information about U.S. persons.

Once we have that information I don't think it makes sense to say, you know, a year later if something comes up we need to go back and get a warrant to search that information.

MR. MEDINE: One last question on this round, which is that under 702, as I understand it, you can collect information about a target rather than to or from the target, and some concerns have been raised about the breadth of that, the scope of that authority.

What impact would there be if that was narrowed to limiting targeting of communications to or from the person that's about this person of interest?

MR. DE: Let me make a couple of general points. One, I think a balanced collection, just speaking at the most general level, is helpful from a discovery standpoint. And it's hard to articulate more in an open setting exactly how that collection is useful. But it has uses beyond that of to or from collection.

I'd say a couple of points in terms of the privacy protections around a balanced collection. The data that comes in, in that way, and it's hard to get more specific, is treated differently than other data, and in fact has a shorter retention period. So there are procedures in place that are intended to account for the greater privacy impact of a balanced collection. And those procedures have been approved by the FISC.

MR. MEDINE: Thank you.

Ms. Brand?

MS. BRAND: Thank you. I want to follow-up on a couple of things that have been

raised before, I'm going back to 215 now.

Bob, you said there were certain, in response to Pat's question about what proposals the administration could accept, you said there are certain transparency proposals that we just couldn't do. What ones are those?

MR. LITT: Well, in the absence of interagency clearance and OMB approval I'm reluctant to state official administration positions on any particular proposals.

MS. BRAND: What ones do you think we can do?

MR. LITT: I do think that proposals, for example, that require us to count things that we aren't now counting and that might be difficult to count present problems for us.

For example, I don't know if there is such a proposal, but if there were a proposal, for example, that says tell us the number of U.S. person telephone numbers that have been acquired every 90 days pursuant to this, that might be a very difficult thing for us to accomplish because

we don't go out and count that.

So things that impose substantial burdens on us like that might be the sort of thing that would present problems for us. And again, I'm not speaking with respect to any specific proposal but that's the kind of consideration that we would take into account.

MS. BRAND: Okay. I'm going to come back and --

MR. KELLEY: I have a point on that. Again, not talking or addressing any specific proposal, but if we were required to for a particular service provider, carrier, telecommunication provider to disclose the number of orders that were served on them, that would give our adversaries a very good indicator, perhaps depending on the relative numbers, whether to use that service provider or not use that service provider.

The adversaries are listening just as we all are to this discussion so that kind of specificity is very, very difficult for us to

accept.

MR. DE: If I may add to that. One thing which presumably the panel is aware of, the DNI has announced a proactive transparency measure which is an annual report of the number of orders issued under various provisions of FISA and the numbers of targets affected.

And so I think what you're seeing is the Executive Branch trying to the extent possible to take the proactive steps towards transparency that can be taken consistent with operational effectiveness. And so that report would delineate the number of orders and targets affected for FISA orders that are based, premised on probable cause, FISA orders under Section 215, orders under Section 702 of FISA and so forth.

MS. BRAND: Okay. And I want to come back to FISA or transparency, especially in the FISC context if I have time, but I did want to follow-up on the discussion about a return requirement on RAS selectors to the FISC.

That sounds like a good idea in the

abstract but I'm a little unclear about what exactly it would add in practical reality.

What exactly would the court do with it? I mean I presume the way it would work, I guess, is on a regular basis, 30 days for example, you would provide a list of RAS selectors to the court, along with some documentation. I'd be interested to hear what that documentation would be. What would the court do with that information?

MR. DE: I'll defer to Brad on the second part of that, but in terms of the documentation itself, today we keep the documentation of the factual basis that established the predicate for the query in the first place.

And so at least from NSA's perspective we keep that sort of documentation and it wouldn't be a great burden to provide it to another oversight mechanism.

But as to how the FISC would handle that, I'll defer to Brad who, the Justice

Department represents us all obviously before the FISC.

MR. WIEGMANN: One option would be all those RAS determinations and if it found compliance problems on its own, then it could call in the government and say I'm not comfortable with how the program is being implemented. And so --

MS. BRAND: Can I just, I think there's something wrong with Brad's microphone. I'm not sure what we can do about that.

MR. WIEGMANN: I got a new one. Is this better?

MS. BRAND: Yes, thank you.

MR. WIEGMANN: So in other words, it could function much like current. Right now if the Justice Department identifies problems with RAS determinations we report those to the court and information could be purged. The court could respond if we have a compliance incident and order relief. They could suspend the operation of the order, suspend the program. They could take whatever remedial steps that they thought were

appropriate in order to enforce the requirements of the order.

So this could be the same mechanism, except that it would, the Justice Department wouldn't necessarily be the intermediary in between --

MS. BRAND: I guess I'm wondering --

MR. WIEGMANN: Rather than us reporting the compliance then the court could on its own independently review the RAS determinations.

MS. BRAND: Well, that's what I'm getting at. I'm not asking exactly about what the court would do if it found a compliance problem, but how the court would figure out if there is a compliance problem, if you would expect them to be literally looking at every RAS selector and assessing whether the evidence justified the determination or what?

MR. LITT: So I think it's important to remember that in the last year there were 288 RAS selectors, so we're not talking about thousands and thousands.

But somebody, I think it was the chairman, may have mentioned the idea of having some sort of outside assessment of are we in fact applying the RAS standard appropriately.

And it seems to me that a judge could look at, in the same way that judges review the validity of Terry stops by police, was this information sufficient to form a reasonable and articulable suspicion to support a stop and frisk, a judge could look at the documentation that NSA has and say, are you setting the line in the right place? Are your people, do your people in fact understand what the RAS standard is and are they applying it appropriately?

And if a judge felt that they were either being, setting too high a standard or too low a standard the judge could provide that feedback, along with whatever remedial measures Congress deemed were appropriate.

MS. BRAND: And is that, just stop me and tell me if we need to talk about this in a different setting. But in the analogous return

requirement in Section 105 of FISA for multi-point wiretaps, is that what the court does with information returned to it under that provision?

MR. WIEGMANN: I'd have to get back to you on that.

MS. BRAND: Okay. If you would get back to me on that, that would be great. That's something I've been wondering about.

I wanted to ask you about a provision in the Leahy bill which would change the standard under 215. As I understand it, that first it would add the words material, so relevant and material to a FISA investigation. And then it would limit 215 to being used to seek information that pertains to a foreign power or agent of a foreign power, activities of a suspected agent of a foreign power who's under investigation, or someone in contact with or known to a suspected agent of a foreign power.

So you may not have an official administration position on this provision yet but I'd like to ask you about it anyway, and answer it

to the extent that you can. First of all, what do the words and material add? What would the court do with that?

MR. LITT: I had the same question as I read this bill over the weekend. I'm not sure what the intent is. I think you'd have to ask the chairman.

I think the obvious intent is to try to, I think it's no secret that the sponsors of this bill want to eliminate the bulk collection program and I think that the intent of the language that they're proposing is to prevent bulk collection. How it accomplishes that, I'm not entirely sure.

MS. BRAND: Do you have a sense of what evidence you present to the court to establish materiality that's additional to or different from what establishes relevance, any of you?

MR. WIEGMANN: I don't. I mean I'm not sure how it would be different.

MS. BRAND: And then can you address the other limitation, sort of three categories of

information that would be allowed and how that would practically impact investigations since this would be no longer like the current 215, which is sort of a general subpoena authority under FISA?

MR. LITT: So I think that the purpose of this pertain to language is -- I believe that the intent is to try to ensure that queries, that business records can only be obtained with respect to identifying individuals. I think that's what their intention is here. And for the reasons we've previously discussed, that would essentially shut down the program.

MS. BRAND: How would it affect though individual, sort of run of the mill, 215 orders, or would it? I mean is your opinion that it affects only bulk collection or would it affect your everyday 215 application?

MR. KELLEY: Well, I think that from our perspective the proposal is flawed in the sense that it has the assumption or presumption that we know the person that we're after, and that's the essence of the terrorism prevention is

we don't know who we're after. So if we are limited to seeking numbers from a known, then we're not going to be very effective.

Again, it bears repeating that we're connecting the dots here, so the fewer dots that we have the fewer connections we will make. So again, I don't think that model works.

I think given the type of data that we're talking about that is susceptible to analytical connectivity, unlike other types of business records, then we need large volumes of that data in order to make those connections.

So whether we are changing the standard from relevant to relevant and material, or saying that there must be a connection to someone who's known, you are reducing the amount of data available and therefore making it much more difficult to make the connections that we need to make.

MR. WIEGMANN: Just to add to that, I think it is important to recognize that those changes would apply not only to the bulk

collection but to regular 215 orders.

I mean people are forgetting, because this is the authority used in the bulk context, that the predominant use of the authority is to obtain individual records in a more targeted way and this would essentially change the standard to closer to the pre-PATRIOT Act standard.

So rather than a broader relevance standard, which gives you more of the flexibility that Pat was talking about, in your ordinary case where, let's say you want to get hotel records, or car rental records, or whatever that might be relevant to your investigation, you'd have to meet that higher showing in order to get those regular records that are more targeted in an investigation.

So it would have a kind of collateral impact on ordinary 215 orders that have nothing to do with the activities that are the current subject of controversy.

MS. COLLINS COOK: Thank you. Raj, going back to what you were talking about that the

administration is going to be disclosing in terms of the types of requests by, I think you said target, which I understand in the electronic surveillance context where the statute explicitly talks about targets of surveillance. What does that mean for Section 215?

MR. DE: So right now the DNI is leading a process to figure out how we can best articulate that language in a way that's meaningful to the public, because obviously in the context of 215, we would have one order but it involves quite a significant amount of records. We would want to make sure we provide some information that's useful, and in fact transparent in some way.

And the same sort of analysis is happening now with respect to Section 702 as well. What's the best means to provide insight into orders and targets affected but at the same time preserve the sort of national security needs we need too. So that process is underway and the DNI is leading that.

MS. COLLINS COOK: I also wanted to follow-up, there's been a lot of discussion about the ability of private sector, I will call them partners and their ability to disclose on a company by company basis their cooperation with the government.

Do you think that there are proposals out there that would allow company by company disclosures that would be advisable or feasible?

MR. LITT: So first of all, this is a matter that's currently in litigation. As you know, there are papers that have been filed articulating positions of the companies and of the government on this.

MS. COLLINS COOK: Sure. Putting aside whether or not it's permissible under the current regime, whether there could be a statutory regime that would be advisable or feasible.

MR. LITT: So again, I think the point is that we, the proposals that we've articulated would allow on the one hand a government -- for the public to know on the one hand on a

government-wide basis how often various authorities are used.

And number two, on a company by company basis how often they are turning over information about their subscribers to the government.

Where we start to have a problem is, as Pat said, when you allow the companies to breakdown on an authority by authority basis what they're providing, because that starts to give a lot more granularity about what our capabilities are against particular platforms, given the kinds of authorities that we are exercising.

If all of a sudden a company that has not had a large number of Title I FISAs all of a sudden has a spike in Title I FISAs, that's something that's going to be noticed by our adversaries and may lead them to shift away from that provider.

I think the flip side of that is from the viewpoint of public transparency what's important to the subscribers is to know how often is the government going to get my information.

And in particular I think frankly from our perspective how rarely it happens compared to the overall number of subscribers, that the number of subscribers of these services, the percentage whose information is provided to the government is a minuscule fraction, even when you take into account all of the government authorities together.

So the overriding concern we have is not having this information broken down at a level of detail that would enable people to avoid surveillance.

MS. COLLINS COOK: So following up on a couple of questions that came up in the first round. There are now a fair number of proposals and discussions about alternative means for accomplishing the Section 215 program or something approaching that program.

My question to you is, how often do you assess alternate means during the course of a program?

So absent the public disclosures,

absent the need to opine on legislative proposals, how often are you internally considering ways to do programs through means which might raise fewer privacy concerns?

MR. DE: So let me speak first to that. I think there's a very valid and reasonable question of the intelligence community generally and to NSA in particular as to how often programs are reevaluated and on what sort of rigorous schedule does that happen.

As I mentioned earlier there's some natural points at which that happens, whether it is in the context of renewals of authorities, whether it's in the context of congressional re-authorizations, whether it's in the context of budget decisions that need to be made.

And frankly, in a place like NSA, it happens every day in the context of normal work assessments. As to whether there should be a more focused process for periodic reevaluations of assessment of reporting requirements, I think that's something we should be thinking about.

MS. COLLINS COOK: So following up on something that Pat had asked earlier and one of the themes and one of the themes that she was hitting, do you think that this discussion today and the amount of information that is currently publicly available about the Section 215 program is predictive of our ability to have a similar conversation about other programs, whether they are current or future?

And that's probably to Brad or to Bob.

MR. LITT: I guess I'm not sure I understand the question.

MS. COLLINS COOK: I think we've heard a few times that the fact that we're having this hearing or the fact that the government's legal rationale has now been made public, that certain FISC orders and accompanying materials have been made public demonstrates that we could have this type of discussion about any range of programs, whether current or future. Do you think that that position is logical or correct?

MR. LITT: So I can start by recounting

the story that may or may not be apocryphal about Zhou Enlai, who reportedly was asked what he thought about the French Revolution and his answer was, it's too soon to tell.

And I think that's very true here. It's too soon to tell really what the effect of these disclosures is going to be. In the intelligence community we are always looking at risks. What's the risk that if this comes out into the public there is going to be damage?

And it's unquestionably and irrefutably true that if information about how we collect intelligence becomes public, it provides an opportunity for our adversaries to avoid that. Will they take advantage of that? We'll only know over an extended period of time whether that's the case or not. I mean we may never know for certain. We may only see certain kinds of information dry up without having somebody post a sign that says, we are no longer doing this because we know the United States can collect this.

MR. KELLEY: I'll just follow up. In the FBI, if you've been to FBI headquarters, as I know you have, if you looked in the courtyard there's a saying on the wall there that says the most effective weapon against crime, including terrorism is cooperation, cooperation of the public.

We rely on the public. We want the public. We need the public. It's our FBI but it's their FBI as well. It's important for us therefore to be sure that we understand where the lines are and we want to go right up to the line but we don't want to cross the line.

So the debate is helpful but at the same time, as Bob has indicated, we have a process in place for that debate. All three branches of government have looked at the 215 program and have said it was okay.

It took an unauthorized disclosure to bring about this discussion, and we don't fear the discussion. We think that the American public is somebody we'd like to have a discussion about.

But it's the adversaries that we're concerned about, because for every disclosure that the public has, the American public has, our adversaries have it as well.

So if we can stick within the established channels to have that discussion to protect the things that need to be secret, then I think institutionally and individually we're better off.

MR. DE: If I can add I think to your question though as to the logical syllogism that we're having this debate and discussion today does that mean that the program never should have been classified, clearly that's not true for the reasons Bob articulated. We don't know the harms yet and there may be harm happening today.

But given the disclosure happened and the harms that will be effectuated are being effectuated, I think what you're seeing is an effort by the Executive Branch to try to be as transparent as possible under the circumstances.

And to that point I think it's

certainly possible to think that greater public discourse about intelligence matters is a good thing without thinking that it took an illegal act to expose lawful programs in and of itself was a good thing.

MS. COLLINS COOK: One final question, Raj, for you in this round. You had referred to minimization procedures and they're traditionally collection, retention and dissemination use.

Can you give an example of a collection minimization requirement? I think that's something that, you know, you look to the typical Title III context and traditionally folks stopped listening when you heard someone who wasn't the target, you took the headphones off, and how that translates into the national security context.

MR. DE: Let me try to address it in a little bit more of a general sense and perhaps in a classified setting we can get into the more technical details.

I think here we're talking about where collection is directed, how collection is

directed, the technical means by which it's effectuated. There are a range of mechanisms in order to minimize to the extent possible, minimize the incidental collection of U.S. person information on the front end as much as feasible given the national security imperative of doing the collection in the first place.

And then there are, we take, as you alluded to, we take those steps that are the steps possible at every stage in the process, not just collection, but during use of information, analysis, dissemination and retention of information.

MR. LITT: If I can just add another sort of conceptual type of minimization procedure at the collection end in this regard is that in a number of areas there are heightened requirements of approval and legal review before collection can be undertaken against U.S. persons.

MR. MEDINE: Mr. Dempsey?

MR. DEMPSEY: Thanks. I had a question about the relationship between the government and

the communication service providers, particularly in the sort of world of globalized information services and American companies providing services to people around the world.

Do you agree that it's important that there be an arms length relationship between the government and the service providers and that there be a perception, that there be a reality of an arms length relationship and that there be a perception of an arms length relationship?

MR. DE: Yes.

MR. DEMPSEY: I've seen reference to the NSA referring to corporations as its partners, service providers as its partners, presumably partners in surveillance.

Doesn't that undermine the perception of an arms length relationship, referring to corporations as the government's partners? Can you see how that would be miss or interpreted suggesting a close relationship?

MR. DE: I think this question probably evinces the problem with selective and misleading

disclosures generally because certainly I review a lot as the general counsel at NSA. I don't want to review every PowerPoint. I don't review every single employee's articulation of things.

I think the term partnership is probably one that's used across government in a variety of contexts. And so I take your point that one wouldn't want to leave the public with the misimpression that there isn't an arms length relationship between any private entity and any government entity.

On the other hand, I think I would caution folks reading too much into particular use of words in any given PowerPoint or whatever was at the basis of your question.

MR. DEMPSEY: Under the 215 program there's this thing referred to in the opinions as the corporate store. So searches are run with the RAS selectors, and as I understand it, the tree of data that results from that goes into the so-called corporate store where it's not subject to the limitations that you've discussed today.

In terms of searching it, can it be now searched without limitations.

Is there any quantification or could there be a quantification of how much data is in that corporate store?

MR. DE: I might have to take that for the record and get back to you. I'm just probably not prepared to speak to it today.

MR. DEMPSEY: And going to this question of sort of 215, one question is, what's next, or what could be next?

What if the government were to decide that it wanted to go back and start using 215 for Internet metadata.

All of the rationale -- well, I guess the question, would the rational for telephony metadata apply to Internet metadata? And then would all of the controls carry over to that, or how would such a program be developed and structured?

MR. LITT: So let me offer a couple of thoughts. First is to bear in mind that Section

215 requires that you obtain business records. There have to be records in existence that you are obtaining.

As we discussed earlier, the telephone companies keep and maintain the metadata for their own business purposes and that allows us to use 215 to get that. It's not clear to me that the same legal authority could be used with respect to Internet service providers.

More generally I think that the FISA Court's approval of the use of 215 for --

MR. DEMPSEY: But just on that I mean, it's my understanding that Internet service providers do maintain data, sometimes for a short period of time, sometimes for a longer period of time, but under the rationale of 215 even holding it for a minute or an hour is enough to --

MR. LITT: I don't know enough about the technicalities of that. But I'm just saying there's a general limitation on 215. It has to be some sort of documents or tangible things.

More generally the FISA Court's

approval of the business record collection was based, number one, in part on a specific showing that was made that the collection of the metadata in bulk was relevant to an investigation and that it had to be collected in bulk in order to be relevant. And we'd have to make that same showing to the FISA Court for another category of data.

Number two, I think that while it may or may not be strictly a part of the statutory standard, I think that the FISA Court's approval of this collection was based very much on the limitations and restrictions that were imposed on our ability to use the data.

It's not at all clear to me, we've never made the request, but it's not at all clear to me that the FISA Court would ever have approved a request that said we want to collect all the telephony metadata and use it for whatever purpose we want to without any controls or restrictions.

So I would anticipate that if there ever, if there were another bulk collection program that we wanted to institute, the FISA

Court would look at the controls that were proposed and the manner in which relevance of the bulk collection was established and template them up against each other and ensure that in fact both the statutory standard and the Fourth Amendment were met.

MR. DEMPSEY: You know right now you've got 215 relevance and that covers everything from one guy's hotel reservation at one hotel to potentially every hotel reservation at every hotel of everybody ongoing indefinitely, and all of that hinges on relevance.

Is it possible to bifurcate 215, have your more particularized requests under the standard that's explicit in the statute and then take this set of concepts and limitations that has built up around the telephony metadata program and come up specifically with a statute tailored for something which I see as quite different, which is the sort of bulk collection, the ongoing collection?

MR. LITT: I think in the abstract,

yes, but statutes aren't written in the abstract. And the question is what it would do, what that statute would provide, whether it would work to allow us to do what we think we need to be able to do.

MR. DEMPSEY: Well, for example, in the 215 program, the telephony metadata program you have something more than mere relevance. You have a concept of necessity, which is not in the statute explicitly but I think which is a premise of the program, which is it's necessary to collect all the data in order to be able to get the value. Isn't that a standard that could be codified?

MR. LITT: Well, I mean I guess Brad can perhaps speak to this better than I can. My understanding of the basis on which the FISA Court determined that the bulk collection was relevant was in fact in part the necessity, that it wasn't a separate concept that was --

MR. DEMPSEY: Necessity is not something that comes from the law of relevance because if you look at the law of relevance,

necessity is not, I think.

MR. WIEGMANN: Actually I mean if you look at -- I think my mic still may not be working so I've got some issues here.

If you have other contexts where let's say computerized data is obtained, let's say under a grand jury subpoena or in civil discovery, and the question is always, like, okay, I want to get a certain amount of data and how broadly can I scoop in order to get the core data that I want?

And with the courts in looking at that say, well, how broadly is necessary for you to be able to get that core amount of data? Is it necessary to seize the whole computer because there are files on it that you know you can get? And the courts have generally said, yeah, you can get the whole computer maybe in order to get certain information on it.

Or there's other cases about financial records and some of the things the government had cited in its white paper that we've published, talk about this context in terms of analogies and

from other sayings.

So I think there are analogies that show that basically you're kind of using a least restrictive means test, or the means that if it's necessary to get a larger amount of data in order to get the core amount of data that's relevant to your investigation, that that's okay.

But all that having been said, if you wanted to codify that and set up -- I mean your question is could you set up, could you segregate the ordinary 215 applications from bulk and set up special rules for bulk because it raises different concerns? Sure, you could do that. I mean we would just have to look at that and make sure that it met the needs of the program and so forth, but absolutely you could do that.

MR. DEMPSEY: That's it for this round. Thanks.

MR. MEDINE: Judge Wald?

MS. WALD: I just want to nail down one thing factually to make sure I understand it. And that's with the 215 collected metadata which

includes all the telephone metadata for all calls made in the United States those, that body of data is subject, as I understand it or am I understanding it correctly, to the regular dissemination exceptions in Executive Order 12333 for any evidence of crime, or certain kinds of personnel decisions, or to, quote, understand foreign intelligence, is that right or not?

MR. LITT: You're talking about the actual bulk collection itself?

MS. WALD: Yes, yes.

MR. LITT: Yes, it's subject to those rules but more importantly it's subject to far more stringent rules imposed by the FISC.

MS. WALD: Okay, but the actual program as it's put forth by the government would -- the reason I'm asking the question obviously is that because there's been certainly perceived unrest or unhappiness among some segments of the public with knowing that all of their telephone metadata though it may be, is out there, the notion of, well, if it's out there but you're not subject to

any queries because the number that's actually queried is very small, as you've reported, still the question arises, well, would the data of people who never get queried never get brought into the query system still be subject to these kinds of disclosures?

So you say, you point out that the FISC Court may have interpreted it to require more stringent data but still am I correct that some of this evidence, metadata evidence can be disseminated even under those restrictions for --

MR. LITT: Only the results of queries. So the data --

MS. WALD: So if it's my phone --

MR. LITT: Can I just, just to make this clear.

MS. WALD: Yeah, I want to get that clear.

MR. LITT: The bulk data that is collected can only be disseminated pursuant to the procedures approved by the FISC, which supercede the more general rules --

MS. WALD: 12333.

MR. LITT: 12333 in this regard. To the extent that 12333 -- I mean 12333 governs everything we do, but with respect to this particular collection the FISC limitations are much more stringent and we can only disseminate query results and even -- and the 12333 then comes on top of that, which is to say that the query results can't even be disseminated unless they meet the test of 12333.

MS. WALD: All right. Well, I just wanted to get that.

MR. WIEGMANN: And so for any U.S. person information, it's only for counterterrorism purposes is the standard.

MS. WALD: I understood that part. Okay, thank you.

Following up a little bit on the necessity question that Jim asked, I think it was pointed out in the white paper that came out on the 215 program that it was necessary, it was said this widespread collection was necessary. And the

necessity fell within the usual formula of being necessary to a, quote, authorized investigation included the relevance of necessity to the technological tools, or getting the haystack, as it were, rather than exclusively to the more traditional interpretation of what related to an authorized investigation means in criminal law, or has meant in criminal law, as despite we could fight about the grand jury cases, how far they go on that. But usually the traditional interpretation was it's related to an investigation if it's going to lead to the actual evidence relating to the subject matter of the investigation.

To get down to the question would be, if 215's relevance is keyed in part to the technological capacity of your search instruments then can that be further expanded if new tools, new technological tools would allow you greater search capacity in this or in other bulk programs, could the, quote, haystack be made as big as the technological tools that you have to use it are?

As opposed to the more traditional grand jury which may have some exceptions, but they weren't huge, which related to, is this going to actually lead to evidentiary-wise to some evidence that's relevant to the subject matter of the investigation.

Sorry for the wordiness of the question, but I think you know what I'm asking.

MR. WIEGMANN: So if your question is do the changes that technology could allow for different --

MS. WALD: Yeah. Yeah, you've said it better.

MR. WIEGMANN: Standards, right. I think it is. That was one of the factors that the court looked at is what the technological means that NSA had available to it to search this data and how effective could those tools be in that particular context.

So yes, I think as NSA develops new tools or as other parts of the intelligence community do that, that would be a factor that's

considered.

But it's not a dispositive factor. The fact that you have the tools means that automatically ipso facto you have the ability to get whatever data that those tools permit you to get if it leads to the information, because you have to look at all the other factors that the court considered. How important is the information? How necessary is it to get the information in a larger quantity? What's the nature of the information?

And obviously that's a critical factor here that the information is not protected by the Fourth Amendment. It's just phone numbers, it's not content and so that's obviously a key consideration that would not make this program available for other contexts, particularly with respect to content information.

So I don't know if that answers your question but I do think --

MS. WALD: Yeah, yeah.

MR. WIEGMANN: I do think technological

changes do make a difference.

MS. WALD: It does. I'm trying to get at what to some has seemed an open-ended notion of having a technology driving the extent of the collection authority, as opposed to the old fashioned method of is this going to lead to some evidence.

Okay. That leads into my -- I think I've got time for one more question, yeah. And that is, as I read it the government's legal justification as laid out in its papers and in some of the material that's been disclosed for the current 215 program has to and does rely heavily on the Smith, Maryland notion that the telephone metadata in that case did not constitute a Fourth Amendment or legally cognizable privacy interest.

Now certainly Smith v. Maryland we all recognize is still on the books, but there have been some intimations of possible future changes in the U.S. v. Jones case, both in the D.C. Circuit and in some of the concurrences in the Supreme Court, as well as since Smith v. Maryland

we've had a lot of research pointing out the potential informative value of a lot of metadata on a person. If you can find out really not content but a lot of the metadata on the kinds of communications the person has had, the places they've gone, etcetera, etcetera, you're going to know as much in many cases, maybe more in some, than you'd get from the actual content of those communications, suggesting to some that that dichotomy is not such a definite one.

I guess my basic question is if in the future Smith v. Maryland should be changed to take account of some of these trends or as suggested metadata, some situations may well have privacy value, cognizant legal privacy value?

Would programs like 215 lose their, in your view, lose their legal foundation, their legal legitimacy?

MR. WIEGMANN: So I think that remains to be seen. I understand you're referring to the Jones case in the Supreme Court that talked about Smith v. Maryland. Obviously it's fundamental, as

we've explained in our briefs, to the analysis of the court here that the information is not protected by the Fourth Amendment under Smith because it's been shared with the phone company.

Again, the basic idea of Smith is information that is a billing record that belongs to the phone company that you have voluntarily exposed to the phone company in making a phone call is not protected by the Fourth Amendment.

To the extent that that changes in the future because of changes in technology, changes in how the courts perceive privacy in the context of large amounts of metadata, I think it remains to be seen.

I mean the holding in Smith and Jones, again to be clear, was not based on that change, it was based on the idea that there was a trespass in putting a GPS device on your individual car. So it was about a GPS device put on the bumper or on the underside of a vehicle and tracking that vehicle in that manner. And it was based on the physical intrusion, which we wouldn't have in this

context certainly. So we don't think Jones is controlling or causing to question our current authorities.

But obviously if there are future developments in the law those would have to be reevaluated by the FISA Court and other courts as they evaluate such a program, so.

MR. LITT: And if I can make one point here, which I think is very important. There certainly are a lot of academic studies that say you could take metadata and extract a lot of information from it. We aren't allowed to do that. We don't do that.

We have a very specific, limited purpose for which we use this metadata and that's all we're allowed to use it for.

And I think, as I said earlier, I think there would have been a very different situation presented if we had asked the FISA Court to say we want to get this metadata and we want to do anything we want with it.

MR. DE: I just want to echo that point

that Bob made because it's really important for folks who are engaged in this public discussion to not conflate the very legitimate point you've made, Judge, which is that perhaps a great deal could be discerned from metadata in a variety of contexts.

But in terms of this particular program, it's only for counterterrorism purposes per order of a court. There's no subscriber information involved. And so I've heard people spinning out threads that one could determine what doctors one visits, who are one's best friends, and a variety of things that in the abstract and without any legal or policy controls in place might be possible, but that's not the world we're in with this particular program.

MR. KELLEY: And Judge, if I may, just one final comment in that regard. The white paper also pointed out that the relative balancing of the minimal invasion of privacy compared to the significant, the greatest interest of the government in this particular fight against

terrorism.

We're not talking about local crime, we're not talking about even organized crime. We're talking about terrorism where I don't have to say it, there are lots of compelling national interests at stake.

So the government's interest in this particular question is at its very greatest compared to the minimal invasion of privacy, even if it were protected under the Fourth Amendment. I think that the key question is, is that outcome reasonable under the Constitution, a reasonable search, seizure? And I think the answer would be yes.

MR. MEDINE: I think we have time for a quick five minute round and still come in on time.

A lot of these programs were developed outside the public view and we certainly have seen that there's been a very strong public reaction to the programs.

What steps could be taken to consider privacy and civil liberties concerns as these

programs are developed and also public acceptance concerns, because obviously we answer to the American public, as we go forward in developing these types of surveillance programs?

MR. LITT: I'm going to punt on that question in the sense that, as you know, this is one of the things that the President has asked the intelligence community and you to look at.

MR. MEDINE: We're seeking your guidance.

MR. LITT: And I think that rather than offer views right now on how that could be done, I think I'd just say that this is a process that's ongoing and we're very sensitive to see whether there are ways that that can be done.

MR. MEDINE: No other comments?

Going back to a question that was raised in an earlier round about the age of data in the 215 program. Do you track, and I'm not asking you to reveal which cases you believe there have been success stories in the use of the data, but in those such cases, do you track the age of

the data that was used to determine whether it was five year old data was necessary, whether three year old data might have sufficed?

I know last week there was some administration testimony that you might be willing to accept a three year retention period instead of a five year retention period. Was that based on a study of the effectiveness of the data?

MR. DE: We have tried in view of current discussions to do the best possible assessment as to where the greatest value has been gleaned in the past.

And so it's some of that evaluation that has come into play in the public statements that three years probably would be where the knee of the curve is in terms of the greatest value.

Historically it's been difficult to piece together. As you can imagine it's quite complex to figure out where any particular piece of data, phone record in a particular query, five years ago came from and how available it was in subsequent steps in the intelligence process. But

folks have tried their best under the current circumstance to make that evaluation, and that's where that three years comes from.

MR. MEDINE: I know there's been a great interest in more transparency with regarding how these programs operate, and currently providers to the government of 215 data are restricted in their ability to disclose government requests.

Would you support reducing that nondisclosure period to 30 days after a request?

MR. DE: We'd probably have to take that into consideration as the government as a whole.

MR. LITT: I guess my view is that arbitrary limits really don't take account of operational realities. And obviously most limitations that I've seen allow for renewal.

I would think that requiring us to go back every 30 days in what could be a lengthy investigative period might put a burden on us. But again, we'd have to look at specific

proposals.

MR. WIEGMANN: And I think it's unlikely that the need for secrecy in these contexts in intelligence investigations is likely to fade after a 30 day period.

MR. MEDINE: And a final question is, I just wanted to follow up on an answer I think Mr. Litt gave earlier in response to Mr. Dempsey's question about the corporate store, the information that's collected under 215 as a result of a query.

What are the standards that govern when that collected data can be queried? That is, is there a RAS determination, is there a 12333 criteria? What restricts access to the data? And also is there an audit trail for requests, inquiries into that database?

MR. LITT: Actually I don't think I gave any such answer so I'm going to kick this to Raj, who might know the answer.

MR. DE: That data would be subject to our background minimization procedures that are

there. There's something called use 18. This a Department of Defense, Attorney General approved set of guidelines.

But to your auditing question, everything that NSA does in terms of queries of internal data is auditable and so we think that's an important protection that we have in place. And the law applies here as well.

MR. MEDINE: All right, thank you.

Ms. Brand.

MS. BRAND: Thank you. Concern was recently raised to me about the absence of a privacy officer at NSA.

Could you tell me two things. First of all, how soon do you think you will have one? What is your process for appointing one? And what would that person's role be in programs like the ones we're discussing?

MR. DE: So today we in fact have a privacy officer and a civil liberties officer separately. But a decision was made to put those positions together in a role that would be a

direct report to the director.

This was announced over the summer and we've been proceeding with the hiring process. If I recall correctly I think the request for resumes and for interest closes in the first week of November. It's been publicly advertised. And from that point forward we will proceed expeditiously with the hiring process.

The one thing I would I would note though is not only are those functions ones that we think are critically important, today we also work very closely with the DNI's Chief Civil Liberties and Privacy Officer.

I think the attention, focused attention that such a person could bring at the NSA as programs are developed would be an effective tool going forward.

MS. BRAND: I think you would be well served to make that process as expeditious as possible.

I wanted to ask a general question in probably the two minutes I have left. With

respect to changes to the way the FISC operates, both in terms of transparency and adversarial, just to lump those together in the interests of time, what changes could the administration support?

MR. LITT: Again, not speaking for the administration as a formal position, but I think we have articulated that we are open to some kind of a process for allowing the FISC to seek amicus participation in cases that present important legal or privacy concerns.

We have both practical and legal concerns that need to be worked through in the context of how one accomplishes that, but I think that we are open to that.

In terms of transparency again, there are already requirements for providing opinions to Congress. We're already working on declassifying opinions. It's not something where you can just snap your fingers and say this opinion is going to be released.

As you know, any judicial opinion is an

application of law to a set of facts. And it's frequently, as Judge Walton, who's the Chief Judge of the court has said, it's frequently very difficult to separate out the classified facts from the unclassified portions that can be released.

I think we take very seriously the idea that it's appropriate to get as much of these into the public domain as possible, it's just, speaking as one who's been personally involved in it, it is a very, very time consuming and difficult process and risks creating a document that is either incomprehensible because of all the redactions or affirmatively misleading because important parts of it are left out.

MS. BRAND: When you say you can support some kind of a mix, do you mean literally an amicus process or do you mean some version of the special advocate that has been suggested?

MR. LITT: As I said I think there are both practical and legal concerns with a special advocate. I think there's an Article III issue

with respect to the standing that a special advocate would have in the court.

I think that there's also a sort of precedential issue that we're very concerned about.

MS. BRAND: Precedential you said?

MR. LITT: Yes. There are all sorts of warrant requirements that are traditionally done ex parte and an argument was made, I think this was made by Chairman Rogers at the hearing last week, are you going to set up a process that provides more protection for foreign terrorists than for Americans who are the subject of criminal search warrants.

I think this is the sort of thing we need to think through. I think that a proposal to have the court have the ability to draw on lawyers who can in an individual case present opposing arguments I think accomplishes the need that people feel that there be alternative arguments presenting in a manner that is much less legally problematic.

MR. MEDINE: Thank you.

Ms. Cook.

MS. COLLINS COOK: I'd like to follow up on this conversation. We'll be having an entire panel devoted to this. The next panel will be discussing the operations of the FISC.

But I think many of the proposals that we've seen are predicated on the notion that because the process is not currently adversarial it lacks rigor. Folks have pointed to what I would call a win loss record of the government in front of the FISC.

And I think it would be helpful to the following panel if Brad or Raj, whoever is situated to talk about this, can talk about how the FISC operates and the process of seeking authorization for a program like this, whether it's helpful at all to simply look at a win loss record.

MR. WIEGMANN: Yeah, so the FISC has come under a microscope obviously as a result of this, the recent disclosures. But we want to say

on behalf of the Department of Justice, the National Security Division represents the government in front of the FISC.

These are regular, life-tenured Article III judges. They apply the same standards and approach to doing their work as they do in their regular cases, whether criminal or civil cases, that they're handling during their regular work the rest of the year. They're sitting on a rotating basis so that means, I don't know, how many, 13 judges or whatever on the FISC? Eleven judges Raj tells me. They are coming in and rotating through and doing a FISA docket in an individual week.

I could tell you they apply extraordinary rigor and care to every single matter that they look at in this process.

The Executive Branch has already applied a lot of rigor and care in making these applications in the first instance. I mean whereas an ordinary warrant can be approved at a much lower level, or a Title III wiretap, these

warrant applications can only be approved by the Attorney General or the Assistant Attorney General for National Security. They go through a lot of review on the front end.

And then as Judge Walton, the Chief Judge of the FISC, has explained on the back-end the fact that the court may have granted an application doesn't mean that it hasn't been modified.

And I think that he's publicly revealed in a letter that upwards around 25 percent of the cases that are submitted to him involve some significant modification beyond just a typo or something like that. But that's a much higher number than you would have in the context of regular Title III applications where I think the overwhelming majority are approved without change.

So I think actually if you look at just the, quote, unquote, win loss record it shows that the FISC is applying a very rigorous standard of review. But you would expect in this context, you wouldn't expect the government to be filing a lot

of frivolous applications to conduct foreign intelligence. You don't want, I think, a Justice Department that's bringing and getting, you know, 50 percent win rate or something, or 50 percent rate, because that would reflect a problem in terms of us applying for things that really were not justified in the first instance.

So the FISC really is not a rubber stamp. If you look at the opinions that have been released is the other thing I would say, we have declassified some opinions now. You can see the extent of review on some very complex and significant constitutional issues that they've looked at in conjunction with the bulk programs.

And they really are looking to scrutinize to make sure that all of the collection, to understand the highly technical issues that are sometimes presented in these cases and to ensure that the Constitution and the requirements of the statute are being followed.

So I don't know if that answers your question or if Raj and Bob want to.

MR. LITT: I just want to emphasize what Brad said about the review that the Department of Justice gives these before they ever get to the FISA Court.

MS. COLLINS COOK: I understand. That gives small comfort I would say to folks who are concerned about the lack of an adversarial process and I think y'all have made very clear the professionalism with which you approach internally and the high levels of accountability. You're talking Senate confirmed individuals who are signing off on each and every one of those. I understand that.

MR. LITT: No, but it's relevant to assess, to put the so-called win rate in context, which is to say things don't ever get made, applications don't ever get made to the FISA Court unless the Department of Justice is very, very confident that they are legally well-supported. And they give them a wire brushing before they ever get out of the Department of Justice.

MS. COLLINS COOK: A final question. I

think the some of the proposals also speak to congressional oversight, and there again I think there's some perception that the semiannual report goes up to Congress and it's never looked at, and perhaps if a sunset is coming up then oversight is conducted.

Can you talk a little bit about your experience with day-to-day congressional oversight to the extent that that occurs?

MR. DE: Sure. So I would definitely like to put to rest any notion that it's not rigorous or frequent or exceptionally open, at least I can speak to NSA's perspective. We work with the Senate intel and House intel committees. It's hard for me to describe, but on a very frequent and detailed basis, sending people down to provide briefings, informal notifications and so forth.

As you know, pursuant to statute, the Executive Branch must provide all significant FISC opinions to both the intel and judiciary committees. NSA in particular is not only

responsive to the intel committees but we're also part of the Defense Department so we're responsive to the armed services committees. As I mentioned the judiciary committees are also relevant to us. And finally, given our role in cyber activities the homeland security committees of both the House and Senate perform oversight of us as well.

MR. MEDINE: Thank you.

MR. DEMPSEY: A couple of questions on 702, and then also related 12333.

On 702 collection of the content program, some of the communications that are acquired are communications persons reasonably believed to be overseas are to and from people in the United States. And it's my understanding that those are lawfully collected. It's not inadvertent, it's intentional and lawful.

But then once that data is in it can be searched looking for communications of a U.S. person. So you have very low, sort of front-end protections, then am I right to say, or let me put it this way, what protections occur then on the

search side?

And I understand Bob's point that if it's lawfully collected the rule is you can search it and use it for a legitimate purpose. But even with the 215 data you've imposed this RAS standard and it's lawfully collected. Zero constitutional protection but you've nevertheless surrounded it with a lot of limitations.

What are the limitations surrounding the incidentally but advertently collected U.S. person communications?

MR. DE: So maybe I can start just with the initial premise that you raised. So you're correct that we must target non-U.S. persons reasonably located to be abroad.

But one important protection is that we can't willfully target a non-U.S. person in order to reverse target a U.S. person, which I know the panel is familiar with, but just so other folks are familiar with that.

Our minimization procedures, including how we handle data, whether that's collection,

analysis, dissemination, querying are all approved by the Foreign Intelligence Surveillance Court.

There are protections on the dissemination of information, whether as a result of a query or analysis. So in other words, U.S. person information can only be disseminated if it's either necessary to understand the foreign intelligence value of the information, evidence of a crime and so forth.

So I think those are the types of protections that are in place with this lawfully collected data.

MR. DEMPSEY: But am I right, there's no, on the query itself, other than it be for a foreign intelligence purpose, is there any other limitation? We don't even have a RAS for that data.

MR. DE: There's certainly no other program for which the RAS standard is applicable. That's limited to the 215 program, that's correct.

But as to whether there is, and I think this was getting to the probable cause standard,

should there be a higher standard for querying lawfully collected data. I think that would be a novel approach in this context, not to suggest reasonable people can't disagree, discuss that. But I'm not aware of another context in which there is lawfully collected, minimized information in this capacity in which you would need a particular standard.

MR. DEMPSEY: Minimized here just means you're keeping it.

MR. DE: I'm sorry?

MR. DEMPSEY: Minimized here means you're keeping it, doesn't it?

MR. DE: It means -- there are minimization requirements, both in terms of how it's collected, how it's processed internally. I mean we can go into more detail in a classified setting. How it's analyzed and how it's disseminated. So the statute requires minimization to apply in every stage of the analytic process.

MR. DEMPSEY: Okay. Am I right, the

same situation basically applies to information collected outside of FISA? So FISA collection inside the United States, 12333 collection outside the United States, but those communications collected outside the United States might include collections to or from U.S. citizens, U.S. persons, and again, those can then be searched without even a RAS type determination, is that right?

MR. DE: I think, yeah, I don't know if we've declassified sort of minimization procedures outside of the FISA context, but there are different rules that apply.

MR. DEMPSEY: One question on that because we're trying to keep to the five minutes.

MR. DE: If I could just --

MR. DEMPSEY: We have asked about, in fact months ago, several months ago we asked about guidelines for other types of collection, and where do we stand on getting feedback on that?

Because you said 18, for example, is the minimization provisions for collection outside

the United States, and that's pretty old. Where do we stand on looking at how that data is treated?

MR. LITT: I think we're setting up a briefing for you on that. I believe we're setting up a briefing for you on that. We did lose a few weeks.

MR. DEMPSEY: No, I understand. I was wondering if you could go beyond saying we're setting up a briefing.

MR. LITT: Well, I mean we're in the process of reviewing and updating guidelines for all agencies under 12333. It's an arduous process. You know, it's something that we've been working on for some time and we're continuing to work on it.

MR. MEDINE: Thank you.

Judge Wald, for the last round.

MS. WALD: Okay. This is another 702 question. Because of the pretty generalized nature of the certification requirement that the Attorney General and the DNI make under 702 yearly

I think it is, maybe it's biannually, and the statutory authorization for very much I'll use short-term category type of targeting that's shown to the FISA Court, and the pretty standard, as I understand it, minimization procedures that are required in 702, there has been some suggestion that the meat of 702, if there is to be any control on it, lies in the so-called tasking orders, which are then approved internally by the government but never shown to the FISC Court, you know.

And according to some of the information or some of the opinions of outsiders, including some of the providers, these don't get any kind of outside look on whether or not they really do strike the right balance between the certification, the category targeting, etcetera, certainly for privacy purposes.

So it has been suggested that there be some review outside of the government on the tasking orders, at least in maybe not an individualized 702, but in any kind of large

categories. Maybe it would be after the fact, maybe it would be along the RAS.

Do you have some reaction as to whether or not any mechanism of that kind is, from your point of view, tolerable, or what are the downsides?

MR. DE: Maybe I can just start with the basics of how 702, targeting the mechanics, work today.

MS. WALD: That would help because not only do some of us have questions about it, but the more you read the newspaper articles it seems to me they don't understand it either.

MR. DE: So we have at NSA internal requirements that the targeting rationale to establish that the target is a non-U.S. person reasonably located abroad be written, documented. That has to at least have multiple levels of approval inside of NSA before it's effectuated. And then every 60 days the Department of Justice and the Director of National Intelligence review each and every documentation of every single

targeting decision that takes place.

Now I know that's not getting to the question you asked but at a minimum folks should understand that there is a multi-agency review of every single targeting decision made.

MS. WALD: I don't -- I am interrupting, but am I correct though that the targeting can be, at least this was debated when it was re-authorized, the targeting can be a very broad, I mean it isn't always a particular individual, it can be a broad target.

MR. DE: I think what we've said is what goes to the Foreign Intelligence Surveillance Court are certifications that aren't individual selector-based targeting decisions, but what I was speaking of in fact are quite specific.

And probably to get more specific, we need to do it in a different setting, but the targeting decisions that are made by individual analysts, reviewed by the Director of National Intelligence and reviewed by the Justice Department are in fact quite specific.

MS. WALD: So therein lies any control over keeping the targeting to that which is useful but not overly-broad?

MR. LITT: Yeah, so if I can just emphasize here what we're talking about is targeting of non-U.S. persons --

MS. WALD: I understand.

MR. LITT: Outside of the United States. And it's a rather extraordinary step like we have --

MS. WALD: But it brings in incidentally, it can bring in U.S. persons.

MR. LITT: Of course it can and so can lots of other things that the intelligence community does.

And I think it's a rather extraordinary step that we have in this country judicial involvement in the targeting of non-U.S. persons outside of the United States. And I think it's very important to bear in mind the potential operational consequences of increasing that judicial involvement.

When FIA was passed I think there was a conscious decision made as to what the proper balance is between judicial involvement and operational necessity. And I think that if you start to say, well, the FISA Court needs to approve every targeting decision, you're going to bring the intelligence community to a halt.

MR. MEDINE: Any final questions?

Well, I want to thank all the panelists this morning for a long but very, very helpful session, so we appreciate you appearing before the board.

We're going to take a lunch break now and resume at 1:15 on a panel that will address the Foreign Intelligence Surveillance Court. Thank you.

(Meeting adjourned for lunch)