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)

MR. MEDINE: Good afternoon. We are now going to start the first afternoon session and the topic again is the Foreign Intelligence Surveillance Court.

We're pleased to have as witnesses James Baker, who's formerly with the Department of Justice, Office of Intelligence and Policy Review, Judge James Carr is the Senior Federal Judge with the United States District Court of the Northern District of Ohio, and formerly a FISC judge from 2002 to 2008, and Marc Zwillinger, who is a founder of ZwillGen, PLLC, and a former DOJ attorney at the Computer Crime and Intellectual Property Section.

I understand that each of you have brief prepared remarks, so please go ahead and then afterwards we will have, as we did in the last panel, rounds of questioning, five minutes this time for each of the board members.

But please go ahead, Mr. Baker.

MR. BAKER: Thank you very much, David. I'd like to thank the board for inviting me back.

It's truly an honor to be here and it's an honor to be able to discuss these kinds of issues in this type of setting. So I appreciate the opportunity.

I just have a couple of quick comments really. The focus of our discussion today is on Section 702 of the FISA Amendments Act and Section 215 of the USA PATRIOT Act.

And I would just say that while these are very important statutorily authorized, judicially reviewed, warrantless surveillance programs involving the collection of communications and communications-related data with respect to many Americans, they're really only part of the story, and I think that was discussed this morning in the panel that I was able to attend.

In particular, as the panel was aware, the government conducts surveillance activities using a number of different authorities, especially including outside the United States under Executive Order 12333.

And I would submit to the board that as you're evaluating these issues you think broadly about them because they do, the privacy issues that you're confronting do pop-up in a number of different contexts.

And as another example, even with respect to telephone records, telephone calling records, there are several ways, eight to ten by my count, sometimes depending on how you count them, eight to ten different ways that the government can go about obtaining the same types of records that you're talking about when you're talking about 215.

So 215 is critically important with respect to collecting these types of records, but it's only part of the story. So I would just urge you to think broadly.

And as I mentioned the last time I was here, I would also urge you to think broadly because the topic that has not been discussed very much is cyber and the need to think about the critical privacy issues and the data collection

issues as they pertain not only to counterterrorism and foreign intelligence, but also to cyber. And I'm happy to talk about that at length if you're interested.

The other quick point I would make at the outset is having to do with the Foreign Intelligence Surveillance Court that I worked closely with for many years when I was at the Department of Justice, and I can elaborate at length if you want me to.

But you know, in many ways I would say, notwithstanding much of what has been written in the press, the FISA Court is a national treasure. It has done its job in an exemplary fashion during wartime. And I think that has not been said enough, and so I just want to say that at this point.

However, the FISA Court is not some type of super inspector general over the whole apparatus that we have to collect intelligence that's, you know, multi-billion dollar enterprises conducted by thousands of people. That is not

what the court does.

And I think with respect to 702 and 215, I would submit that I think we've reached the outer limits of what you can reasonably expect a court to do in this setting. And I'm happy to discuss that at length.

At the end of the day, to my mind, it is the responsibility of the President, the Executive Branch and Congress to conduct management oversight and control over these types of activities. I'm happy to talk about transparency and the issue of whether we're going to have an advocate or something like that in the questions.

So thank you very much.

MR. MEDINE: Thank you, Mr. Baker, for coming back with us again. Judge Carr.

MR. CARR: Yes, like Jim Baker, with whom I did work for five or six years, I can't recall whether you had left before I did or not, Jim, but in any event, I'm pleased to be here and be part of the conversation.

This comes about, as you may be aware, that as a result of an op-ed that I happened to publish on the 23rd of January, I think it was, making what I consider to be a very modest proposal, which I will repeat this afternoon, to improve the, both I think the processing of certain applications before the court, and I would hope as well perhaps to enhance public confidence in some of the decisions that the court reaches.

And that proposal is quite simply that Congress give the FISA Court judges either the discretion or perhaps direct them to obtain the services of outside independent counsel when the court is presented with something that's new and novel.

And this would happen on very rare occasions. I mean one of the things I want to emphasize is how infrequently this kind of representation would be necessary.

The vast majority of FISA applications are simply fact-based. There's a very low probable cause standard, affiliated or working on

behalf of a foreign government or a foreign-based terrorist organization. That's the probable cause showing.

Once it's made, we have to issue the order. We do not have discretion to second guess the government's purposes or reasons. To that extent it's very much like a search warrant or Title III order.

But on infrequent occasion I felt as a sitting judge when Jim Baker, and he was the one who would do it, would come to me and say, Judge, you better pay special attention to paragraphs 62 to 73 because this is a new technique. There's something new or unusual about this that takes it outside of the ordinary really quite straightforward and typical and routine FISA application.

The government would do that. It would do it for good reason because it knew that we had to trust its integrity in order for us to function effectively and have confidence in what they were saying to us.

That requirement became codified in the first draft in 2008 of the Foreign Intelligence Surveillance Court rules. And the government is required by those rules in that situation to call to the courts attention in that sort of situation to call that circumstance to the court's attention, and I'm sure it does so.

That seems to me to be a good trigger point for a judge either to exercise his or her discretion or perhaps for Congress to mandate when that notice, Rule 11 notice, is given, that then the court calls upon one of what I would envision to be a very small cadre of pre-cleared attorneys, probably in the Washington area, probably with some sort of experience in this area, I would certainly hope so, so that they wouldn't have to spend a lot of time learning how the wheel turns, as it were.

But that individual could come in, in that circumstance when called upon to do so, to represent, and I was once asked who's the client, I think it's to represent the interests of the

Constitution, the Fourth Amendment, and the rights of all of us to communications privacy.

But it would be a very infrequent occasion when this would be necessary. And again, I want to underscore that.

And I think that the benefits to the court and to the process would be quite substantial. First of all, we judges are accustomed, it's how we work, through the adversary process. And what do you say, what do you say? That's how we usually make decisions in most of what we do.

Secondly, when the government wins, close quote, when the judge says, yes, you can do this or that, it has no interest in appealing. It does not need to get that order reviewed. It's not going to go to the FISA Court of review and say, by the way, we won, but nonetheless look at it.

However, in that circumstance limited to when there's a new or novel technique or some other aspect where the court has called upon an

individual, outside counsel, then that individual would be able to appeal and secure appellate review, which does not presently exist.

And an appellate review I think, and certainly in my day-to-day functions as an ordinary Article III judge, is very important. I get reversed. And there are times when I do get reversed, I say, my gosh, I was wrong, thank goodness they're there.

And then finally, and this has occurred to me since I first wrote that op-ed piece, it seems to me that this outside counsel, I haven't really got a name for it yet, could also perform an important role when there's an issue, a troublesome issue of noncompliance.

Once again the government is required to report instances of noncompliance. It did so when I was there. In every one of the those instances it was fairly trivial. It wasn't troublesome. However, Judge Bates, former presiding Judge Bates's lengthy opinion that was released earlier this summer suggests that there

may be instances where reports of noncompliance are of a sort that, once again, as a judge of the Foreign Intelligence Surveillance Court it might be useful to have the discretion to reach out to somebody to assist the court in understanding the issues and ensuring that what went wrong has been fixed and does not have any serious cause to it, or if it does, see that that gets fixed.

And at some point I hope to be able to talk about the role of the legal advisors because their work for the court is absolutely crucial. I don't think it's well understood by anybody outside the court, and the role that they play is extremely important. And I hope perhaps to have a few minutes to talk about them and their role and where it fits in everything, so.

And one final thing, Jim sort of alluded to this, but it's my view that we should all keep in mind when talking about foreign intelligence collection, the function of those agencies charged with that responsibility, and then the activity of the judiciary, and it's a

very limited activity under the Foreign Intelligence Surveillance Act.

If you look at Article II, and of course that's the article in the Constitution that establishes the office of the President and gives the President his responsibilities and authority, you don't find the word judge in there at all.

Now this is a very unique circumstance where the third branch actually plays a role in overseeing the activities of the Executive in an area in which the Executive constitutionally has exclusive responsibility, for the conduct of our foreign affairs and protecting us against foreign dangers and threats.

So I look forward to your questions, and once again it's a real pleasure and an honor to be here. Thank you.

MR. MEDINE: Thank you, Judge Carr.

Mr. Zwillinger.

MR. ZWILLINGER: Thank you for inviting me as well, especially thank you for seating me on the same side of the table as Judge Carr. This

might be the first time I've been on the same side of anything with a FISA Court judge, even if it's a former one.

As the board knows over the past thirteen years I've helped dozens of clients respond to government demands for customer data, both in criminal cases and under FISA.

My clients have ranged from small app providers to large tech companies like Yahoo and Apple. And although my representation of Yahoo before the FISA Court is largely why I'm here today, my comments are entirely my own and are not on behalf of any client.

That said, my client work has given me a unique view into the position of providers, Internet service providers who receive demands under FISA and has helped me see two aspects of the process which I believe are inconsistent with the core principles of our legal system.

First the overbroad cloak of secrecy that applies to everything FISA-related and the lack of a true adversarial process. Together

these issues pose difficulties for providers and by extension their users and the public.

To begin with when providers are served with classified FISA orders or directives they receive an entirely unfamiliar process containing very few specifics, which they can review only for a brief period of time before they have to hand it back to the government.

Yet based on that mere glimpse, they're being asked to disclose, compelled to disclose the most private user communications they carry.

And due to the secrecy providers have few places to turn for advice. While some have experienced counsel that can help determine if a request is routine, of the type that Judge Carr referenced, or novel, providers with limited resources struggle to even understand much less react accordingly to the process they get.

Yet providers are the only parties with the statutory authority and the opportunity to challenge these orders before they're executed.

Indeed Section 702 is designed right

now to make them the last bulwark against potential government overreaching because the court is not given the authority to do a full lawfulness review of a Section 702 directive unless a provider first initiates a challenge.

But a decision by a provider to challenge must be made alone under acute time pressure with sensitivity to what's at stake, with little context and while under a gag order.

And when providers do bring a challenge trying to meaningfully litigate in an adversarial way in the FISA Court it is an uphill battle. Even now the rules for filings have barely been tested. The logistics of handling classified litigation are very difficult, and filing documents with the court frankly has always been a little bit like trying to get a letter to Santa Claus. It requires a lot of blind faith. The rulings come down the same way.

And even when appearing before the court, the government regularly submits ex parte papers that a provider is not permitted to read,

even if it's represented by a lawyer with the right clearance.

Indeed, this happened again recently. My second case in the FISA Court is a declaratory judgement action brought by five providers seeking the right to disclose the number of intelligence process that they have received, just the numbers for each form of process.

And to oppose this relief the government has made a secret filing to justify why that disclosure will cause harm, harm that would outweigh their First Amendment interests, but it's refused to let even cleared counsel see that filing.

As you can imagine it's hard to respond effectively to something you cannot read, which means that even in the adversarial proceedings the court is still hearing only one side of the issue.

In light of these issues I think relying on providers who have to toil in secrecy and fight in the court with one hand tied behind their back as the last check on our government is

not ideal, which is why the creation of a special advocate, one who would have the same access to classified materials as the government could make a real difference.

As Judge Carr pointed out and Judge Robertson before him pointed out in the last hearing, judges are used to making decisions after hearing both sides of an argument. That's the way our system is structured and that's what makes the decisions informed and legitimate.

An advocate can help ensure that the other side of the argument, not just in the extremely novel cases, but in bulk collection cases and other cases as well, the other side is represented. The advocate can weigh in on the novel issues that come up before the court and serve as a potential resource for providers who want to challenge compulsory process.

We need look no further than some of the odd logic in some of the recently declassified decisions to see what happens when the court and the government work through the issues without any

balancing input.

And even if the decisions wouldn't have come out any differently, even if the court had heard from an advocate, adding an opposing voice would give the process more legitimacy and restore some faith in the court's decision-making.

I look forward to our further discussion of the special advocate and other issues related to the court.

MR. MEDINE: Thank you, Mr. Zwillinger.

We'll start the questioning with Judge Wald.

MS. WALD: Thank you. I surmised from the morning panel that the government, as well as many outsiders, have commented, are reasonably comfortable with the idea of the FISC Court being able to call for an amicus to help them on particular novel issues of interpretation.

I also think that Judge Carr and many other people who have commented on the outside are suggesting something that's a little bit stronger, a little bit more energetic than that, namely that

you would have a body of outside counsel.

So I'd like to pin down a couple of things, initially with Judge Carr but certainly with other peoples' reactions too, and that would be if you had such a body of advocates with secure clearances on the outside, do you think that it should be entirely in the discretion of the FISA judge to decide when he or she wants that kind of help?

And more specifically, I think, because Judge Carr raised the problem of appeal, and I think that most of us whose experience is familiar with regular Article III, nothing meant by regular, but Article III courts is that the appeal is a very, very necessary part of the process.

Now there have been constitutional questions raised by other people about whether or not apart from the provider if you try to give an amicus or appointed, somebody appointed from a panel of secured lawyers the right to appeal you might run into constitutional objections.

So I think those two basic questions

about whether or not you would leave the initiation of the appointment of such a person entirely in the hands of the FISC judge, and whether or not once that person was in and had participated in the lower court proceedings, should that person, that advocate, whatever you want to call them, can that advocate constitutionally be given some right of appeal?

MR. CARR: Well, let me say to try to analogize, I do not think that an office, an outside office that reviews every single application is necessary.

MS. WALD: No.

MR. CARR: My thought is, how I envision this, have a relatively small number of attorneys, something like a CJA panel in ordinary criminal cases, Criminal Justice Act panel, who will in time gain experience because of their small number, who are completely wall-to-wall security cleared.

Mr. Zwillinger raises something that I hadn't really thought about but by all means I

think that individual should have as complete access to everything that the court is hearing as the Justice Department prosecutor has, that there should be no withholding, no secret filing or whatever.

And I actually hadn't thought about the constitutionality of being able to appeal, but one of the most important aspects of what I'm proposing, because that would give the opportunity for further review by a three judge panel, Foreign Intelligence Surveillance Court review, would give those three judges a chance to look at it again and ultimately perhaps secure a Supreme Court review.

But I cannot answer your question about that. I'm not sure I should as a judge in any event, but nonetheless, I don't know.

And finally, thinking about this further I think that both under some circumstances it should be necessary for the judge, don't let the judge have discretion.

In other words, when what I call a Rule

11 notice is given, and I don't know whether it would cover -- I think it would cover something like the PRISM program and so forth, that was certainly my intent, but also give the judge the option, sort of two hand.

And so it's not just when a Rule 11 notice comes in, that could be a trigger, but then the judge can retain discretion to reach out. But it would be a small group of lawyers pre-cleared, gain experience, and again, I think used relatively infrequently.

Or perhaps, this just occurred to me, when a provider has an interest and the provider wants to appeal, perhaps the provider could also request that the court appoint an outside attorney.

MR. ZWILLINGER: If I could jump in on that for a moment though. I would undoubtedly be one of those attorneys. I've been before the FISC twice. I'm the only private attorney to be before the court of review. I don't think it's enough.

That is, you talk about the

constitutional questions of letting somebody have the standing to appeal, the court believes that it doesn't have the power to force the Executive to make classification decisions differently.

So the Executive is not going to provide this private counsel with full access to the classified material that would be necessary, and certainly not on a historical basis. That is, maybe for the particular case, but an advocate would know that two years ago the Solicitor General stood up and made a representation to the court that, for example, as happened in re Directives case, that there is no database of incidentally collected U.S. persons' communications.

And only an advocate who had been in several cases would know that the representations the government is making in one case may be inconsistent than the representations that are made in another.

So as much as in my business interests, I would love for there to be a small group that we

would have exclusive right to practice before the court, I don't think it would satisfy the interests of really protecting the Constitution because, by definition that group is going to be limited.

I would love for the special advocate to be able to bring the help of outside and the type of panel you described to bear on a particular case, but I think there has to be someone with an institutional interest that would look across multiple cases and be able to challenge the government's programs, not just in the one case that they may be admitted to practice.

MR. MEDINE: Thank you.

Mr. Dempsey.

MR. DEMPSEY: First, Jim Baker, do you have any thoughts or comments on what we've been talking about here?

MR. BAKER: Sure. I'll just try to be brief.

I mean on the one hand, so you're

trying to balance I would think, speed and agility and the ability of the government to move quickly without adding more process. And the process was discussed a little bit today, but there's a lot of process already. So we're going to add more, in theory, under any of these proposals.

Another issue is intruding on the President's Article II authority to an even more significant degree.

Everybody agreed I think, when FISA was enacted that this was what everyone was doing. This is what this act is all about. It was justified for a variety of reasons back then. You know, there may be reasons to have it now, but we have to be mindful that that is what's happening.

And I am worried about delegating to others, whoever it may be, the authority to disclose information, the classified information to yet another party.

I also worry about having an outside panel. And the concept of an advocate versus an amicus on a case-by-case basis we can talk about

later. But the main thing I'm worried about frankly is just leaks of information.

So one of the things, it is hard to prosecute a leaks case. So the criminal is there, but it's hard to actually use. Something that everybody who's in the system has to deal with if they decide they want to leak something is the fact that they may lose their job. They have skin in the game that's real, that's important to them. It's important to their families. And they have to think long and hard about whether this issue is something I'm going to try to leak something about because you can lose your security clearance if you leak and they still can't prove it, if you have a situation where you can't prove a case.

So I'm worried about this at a variety of different levels, and I can respond more specifically to your question.

MR. CARR: If I could speak to that because something just occurred to me. It seems to me that, first of all, perhaps you could create these people as some sort of, this small group as

somehow federally employed and appointed like the federal public defender.

More importantly, it just occurred to me as Jim was saying, I mean there's never been a FISA leak by anybody affiliated with the FISA Court, as far as I'm aware.

And then I'm not talking about a large number of people. But as importantly, a lawyer might be difficult to prosecute, but it wouldn't be very hard to take his license and his livelihood were he to leak. And so I think that's something to keep in mind.

And Jim actually raised at lunch the idea of a federal appointment. The more I think about the risk of losing a license, plus the public shame and disgrace, and the potential risk of being prosecuted, I think at some point you have to have confidence in the people who pass these kinds of security clearances, that they will do the job that their oath binds them to do and maintain classification.

I'd like to ask one little, just raise

the question, and it is in response to Judge Wald. I don't know, can Congress mandate, I mean Mr. Zwillinger's concerns about the withholding of classified information for this outside counsel, whatever you call, I mean can Congress include that and say that that person shall have the same access to all documents and information classified or not that the government provides? I don't know. That is another constitutional issue.

MR. BAKER: Judge, if I can just add, you know, I'm not a CIPA expert but, you know, by and large in the Classified Information Procedures Act setting in a criminal case the government cannot be forced to disclose information to a defendant, but the government can be forced to make a hard decision about whether to prosecute the person or the sanction they may suffer for not disclosing the information to the defendant may be dismissal of the case.

I don't know how it would work in this context but at the end of the day I don't think -- I think it is a significant constitutional issue

about whether you can force the government to disclose classified information to somebody that the Executive, the President does not want to.

MR. DEMPSEY: Although would the analogy in this situation be basically, the court would in essence say, just as in CIPA, if you want to prosecute this person you need to make this information available in this way. If you want to get your order you need to make this. I'm not going to rule on this until I'm sure that I've had both sides of the story.

MR. BAKER: Yeah, you'd have to figure that out.

MR. DEMPSEY: The judge is sort of nodding his head.

MR. CARR: As a matter of fact, it would make sense, condition, you want this order, well, we're going to play with a level playing field and all the cards up on the table. And that may be a way around it.

MR. DEMPSEY: One quick question, there are two, I think, related ideas in play here.

Some people talk about the special advocate, some people talk about amicus. Is it possible that you could have a hybrid of this, that sometimes you would have the classified lawyers, this sort of cadre, handful of people pre-cleared, etcetera?

In at least one case the FISCR, the FISA Court of Review has invited non-cleared amicus to comment on a question of law. Is there any possibility that that could happen in the first impression or whatever, when the application is first presented that the court could say, all the details are secret but there is a question?

Is the law, the one where the amicus participated in an unclassified context had to do with the wall. So you could have a hybrid of both of these. Do you feel that, or yes or no?

MR. CARR: I was trying to think whether the, for instance, the PRISM program itself, because it raises clearly Fourth Amendment issues, I think it was you or somebody this morning pointed out the reasonablness clause of the Fourth Amendment. And I think that may well

be in play.

I think Smith is not a particularly reliable basis. That was a pin register and so forth. My problem is I'm not, as somebody else mentioned, I'm not sure you can so easily untangle the secret from the, quote, pure question of law.

Mr. Zwillinger may have a much better grasp of that than I do.

MR. ZWILLINGER: I have the same view. Just an actual example in the 2008 case the question was whether the lawfulness and the constitutionality of the directive, the court relied heavily on the minimization and targeting procedures to say that the procedures in place were sufficient to provide constitutional protection.

The provider never got to see the minimization and targeting procedures, and had it not been for the leaks it's not clear we'd ever have seen them. So to argue even if you're in the case or as amicus without seeing some of the factual basis makes it very difficult to present a

constitutional argument about whether the safeguards are sufficient.

MR. DEMPSEY: Okay, thank you. Thanks.

MR. CARR: Because many of the circumstances that I have in mind raise new and novel methods of collection. I'm going to point at this point because it's public now, the whole PRISM idea itself.

And so there's an intersection between the technology keeps running ahead of the law, both in Title III and everywhere else, and that's part of the problem too. I'm not sure that it can be quite so finely sliced.

MS. COLLINS COOK: Building on something that you've just talked about right there with the technological advances, what is your understanding of the FISC's current ability to use technical experts, technical consultants?

Is that something that the FISC, I think we've heard competing views as to whether or not the FISC can already do that, does it do it, should it do it more?

And I'm here thinking about new technologies, or to try and avoid what we've heard to be a problem of miscommunications from technologists through to lawyers through to judges. So I ask the question whether there's already that capacity.

MR. BAKER: Well, keep in mind I'm not in the government anymore, so. But I would say, I mean you've put your finger on a very important issue, this translation, the game of telephone where things get translated from technologists to lawyers to judges. That's a real problem and a significant problem.

My experience was that if the court had a question we could bring in any expert from the government to talk about any technological issue that was required.

I guess just thinking about it, it seems to me that if the court wanted to bring in an expert from the outside, perhaps from one of the companies that Marc's talking about, I don't see any reason why that could not be made to

happen, if they wanted to actually speak to someone who's, you know, connecting wires together through machines and things like that.

I don't see that as being something that would not be possible to do. You'd have to bring in someone who has a clearance. You'd have to figure out what kinds of questions you're going to expose this person to, what kind of information. There could be some security issues around that I could see, but I don't see that as being something that shouldn't be possible.

MS. COLLINS COOK: Does anyone else want to opine on that?

MR. CARR: If I could say, well first, and again I don't know back in 2002 part of my experience as a rookie FISA Court judge was to visit agencies and be shown and told about what now of course probably is outdated, is the flip-phone or the old car clunky phone, technologically.

And I can recall one instance where we had the opportunity and we took it to become

informed about a particular kind of activity. Obviously I can't go into any detail, but I'm quite comfortable with the idea. Certainly you can reach within the government, and I don't see why we couldn't reach outside the government to get that kind of -- so we simply understand what they're talking about.

MS. COLLINS COOK: When y'all were discussing CIPA as a possible analogy I just wanted to follow up on that briefly because CIPA true, the government at the end of the day has the ability not to bring criminal charges.

There may however be other alternatives for the government to pursue such as immigration consequences, PNG, you can envision a variety of things that the government could do, and you're talking about a situation where you've identified who you believe to be the wrongdoer.

Does the analogy hold if you're talking about the FISA Court where you have a hybrid preventative mission of many of these authorities, as well as an investigative?

If my question makes sense. It just strikes me that it may not be the truest analogy to the FISC situation.

MR. BAKER: I mean I haven't thought through it completely, I just brought up the CIPA example here.

But I am worried about, yes, that first of all the President being forced to disclose classified information and then what happens if he decides not to. I think that's a big issue. I don't pretend to have the answer here today, but I think that raises real, real concerns.

For the President to give up the ability to obtain some type of otherwise lawfully authorized, statutorily approved type of collection that's consistent with the Fourth Amendment. Obviously you have to persuade the judges about that. I don't know. I don't know about that. It's a real hard issue.

MR. CARR: And again, I haven't thought about it until about seven or eight minutes ago, but it does seem to me as a judge, I mean we

would, as part of the ordinary process, we would say, look, I've got questions. I would call one of the OAPR attorneys and say, look, I've got a problem with this. And it would be a fact kind of a problem, it wouldn't be a technological kind of problem.

But it does seem to me, I have the ultimate authority. They have to give me, I think, what I'm asking them to give me if they want to get my approval.

It's my understanding also that if I turn them down they can't simply show up next week to the next person, they've got to come back to the same judge who's turned them down.

MR. BAKER: Or appeal.

MR. CARR: Or appeal, absolutely. And so again I think it's something that would certainly bear looking into by people who've thought about it and will think about it more than I have this afternoon.

But the idea, look, if you had this, I'm going to call it independent counsel, okay,

rather than special advocate because that has a different connotation, or amicus I think has a different connotation, but a small cadre.

And if I say I want that person to have all the information you have, Mr. Baker, then he has a choice. He can say, judge, okay, we're going to appeal and find out if you can do that, which may be the way to go. I mean that's the way we do things as Judge Wald knows. If you don't like what I do, go find three appellate judges, they'll tell me.

MR. ZWILLINGER: One thing Judge Carr's comments raised for me though is that the role of the FISA Court as approver as opposed to resolving an adversarial dispute, Judge Carr said that in his time on the FISC there was not as much of an adversarial role for the court and there weren't these bulk collection decisions. So seeking approval from the court, he had the right to contact anybody he wanted in the government and ask for information.

As someone who's been in an adversarial

role before the FISC I find the ex parte contacts between the government and the FISC very difficult to deal with and overcome. The fact that the same judge who may have been involved in deciding that the bulk collection is lawful, then be assigned to the case to decide whether there's going to be an adversarial challenge.

I mean it's not a different pool of judges. It's not a magistrate issuing a search warrant and a United States District Court judge ultimately deciding if there should be suppression.

So we're going in front of the same pool of judges who have both an approval role and an adjudicatory role and their ability to call in ex parte contacts and get information from the government may be different in an adversarial proceeding than in an approval of an surveillance proceeding.

MR. CARR: Well, but on the other hand when the PRISM application first came in the subsequent application, in all likelihood did not

go before the same judge, and that judge had the independent authority to decide whether or not it could be approved. So it's a different sort of process.

It doesn't return to the same judge because we're on rotation, these 90 expirations or whenever. Once in a while I would get something I'd had a year or two before, but it was very rare that I got the sequential. And I don't think it would be necessary in that situation where you go in for renewal of something to go find the same judge. In fact, I think it would not be.

MR. ZWILLINGER: My point is more that the judges are playing two different roles. They're working with the government, the Executive Branch to approve a surveillance or say come back, you haven't answered this, or I need some expertise on that, and they're working through the process of approval, but they're also the same judge, the same court that listens to an adversarial dispute whenever either a provider wants to bring a challenge or if we create some

sort of additional advocate or amicus to being a challenge. We have to talk about the court's dual role and how to sort that out, I think.

MR. CARR: Well, I used that term deliberately because I don't see the difference between what I did as a judge on the FISC and what I did as a magistrate issuing search warrants or as a district judge later issuing Title IIIs.

I mean maybe the word approve, but the process and review is the same. In that situation I'm often the judge who winds up hearing the suppression motion, and the law is quite clear I can do that. So I don't see that there's that much distinction, in fact, I don't think there's any between the judge's job as a FISC judge and the judge's job as an Article III judge or an Article I judge magistrate in issuing more conventional warrants and orders.

MR. MEDINE: Thank you.

Ms. Brand.

MS. BRAND: Thanks. I'd like to switch gears a little bit from the adversarial process to

transparency. It's been the subject of some of the other recommendations. And these questions are more directed to Jim and to Judge Carr.

How feasible is it for FISC judges to write opinions in the first instance with an eye towards declassification or redaction later?

Just assuming for a moment we're talking about prospectively as opposed to retrospectively, is this an easy matter, complicated? Can it be done?

MR. CARR: Well, first let me say it was my experience, I mean I don't know about the other judges with whom I served or judges today, writing an opinion as we ordinarily understand, that was a very unusual event. Because once again, it's like with an ordinary search warrant, you don't write an opinion. You look at it, if there's probable cause you say, you issue it, a Title III order, you issue it, and a FISA order, you issue it.

MS. BRAND: In the unusual circumstances though where there is an opinion.

MR. CARR: Again, when a judge, part of my, implicit I suppose, when a judge felt the need to actually write an opinion, and that's often triggered by the notice from the government that there's something going on that's unusual, and by the work of the legal advisors. They too will alert us to issues that call for further consideration and reflection. I don't remember the number of, quote, opinions, maybe a few pages, maybe several pages I wrote, but it was a handful. And I think that's probably -- so part of it is in thinking about transparency, it's not like an ordinary court with ordinary cases where day in and day out you're writing opinions.

MS. BRAND: Right, but I'm trying to figure out where there is an opinion, how easy is it to -- because what you don't want to have is a redacted opinion that's nonsensical because of the redactions, right. So how easy is it to write something that could be understood later in some way in unclassified form?

MR. BAKER: So for example, in the

court of review, the first court of review decision from '02, I think it was that clearly, was written, in my opinion, it was clearly written by the judges to publish it, because they boiled down the classified stuff into a couple of different sections, so that the legal analysis and the historical background and so on and so forth, they were able to put forward in a way that made sense. It wasn't like a piece of Swiss cheese. You could understand the logic and everything that was going on and the classified stuff because it was concise. And so --

MS. BRAND: You're talking about the wall case?

MR. BAKER: Yes, exactly, yeah.

MS. BRAND: How translatable, because that case clearly amicus participation was feasible, right, and there was an opinion that was public. So there was something about that case that lent itself to public participation and publication thereafter.

How translatable is that more broadly?

I mean how --

MR. BAKER: Well, if the court knows, so if you were to have some act of Congress that said, to the extent practicable, opinions of the FISA Court shall be published or shall be presented in a public, in a form that can be readily published or something like that, if they were sort of forced to do it basically, I think they could do it in many instance.

There will be some instances where it will be much more challenging. In some of the very technical ones where the facts of the case are interwoven with the legal analysis, that's going to be harder.

In the FISC review decision it really was a mega legal issue. There were a couple of cases, if I recall correctly, that were at play, but it really wasn't a factual or really heavily technical kind of issue. It was much more of a pure legal issue. So but my guess would be if the court had that idea that it had to do that.

Another option might be, you know, the

court shall release an unclassified summary of the key rulings of a case or something like that. Sort of like headnotes or something where the key --

MS. BRAND: Well, let me ask you about that because we heard from another judge that he would rather not see summaries because a summary isn't always a full picture of what the opinion would say, and so from that perspective redaction is preferable to a summary.

Judge Carr, do you have a view about that, if there were going to be an unclassified summary versus just a redacted version of the opinion, which one is better?

MR. CARR: Understanding that no two judges might agree on whatever view I might have thinking about this for the first time, again, it all depends. What is the issue? Does it really involve something that is classified or is it simply, I mean can you recast it in a way?

I think it's impossible to predict in advance how difficult or easy it might be.

However, were there a default or at least the likelihood at some point of publication of part or all of a decision, I think certainly a judge could go into writing whatever he or she wrote with that in mind and perhaps deliberately compartmentalize, write the opinion with an eye to that.

But to try to tell you would it be easy or difficult, it would certainly depend upon the particular issue and the setting in which it came up. It might be easy and it might be almost impossible.

And I kind of like Jim's idea of a summary. Without further detail, this is the issue of law and we have approved, I have approved this. Or if the court now sits en banc, and I don't know if it ever has, but it has that authority, which I think is very worthwhile.

But I can't really answer your question directly, and I'm sorry.

MR. BAKER: If I can just add, you're trying to find, it seems to me you're trying to find balance here between disclosing,

unnecessarily disclosing classified information that would harm us and providing adequate transparency so people can understand what's going on and have confidence in the system.

The summary is like a balancing type thing. I mean on the one hand you're not going to, you don't want to have no transparency and on the other hand you don't want to have T.V. cameras in the courtroom either, right. So it's an option.

And what might make sense is, you know, sort of a couple of different options for the court to pursue or have available to give transparency that they could figure out which is the best fit in a particular case.

MR. MEDINE: I have a question for each of the panelists which is, what is the role of this outside person, whether they're an advocate, or an amicus, or a staff attorney or whatever, when they appear before the court?

And it's sort of really two questions. One is, is there a charge to oppose everything the

government proposes?

And then secondly, how do they evaluate assuming that they engage with the government, how do they evaluate which arguments to make?

There are statutory arguments, there are constitutional arguments, there are factual arguments. How do they make those decisions and who guides them in making the strategic decisions they make in involving themselves in a case?

So maybe we'll start with Marc and go on down.

MR. ZWILLINGER: I don't think they should oppose everything the government seeks. I think the goal of this isn't to make it harder for the government to protect the country. The goal of it is to make it simple for the government to protect the country while respecting the Constitution and to have somebody pointing out on the other side what the constitutional balance is versus the pure needs for, you know, security or surveillance.

And I also think they'd lose

credibility before the court if they're just opposing everything, as opposed to getting across the message when this is important.

As to how to decide what cases to get involved in or what arguments to bring, you know, I do think the first person who occupies the office should probably play a large role in figuring that out. But it would occur to me that novelty is one thing that's certainly there, bulk collection, something that even if it's --

MR. MEDINE: So I want not as much focus on when they should get involved as what positions they should take once they're involved?

Again, do they argue the Constitution, do they argue statutory noncompliance? I mean lawyers strategize, but they partly strategize based on who their client is. How does this particular person make those decisions?

MR. ZWILLINGER: Right. So to try to get at that in a short answer I would think you've got it right as to who their client is if they view their client as the, you know, either

American public or in some cases, you know, the human race who has this sort of interest in sort of human dignity and privacy in their communications, their client is to offer the perspective of those individuals who can't be there to speak for themselves as to whether their surveillance is appropriately narrowed or necessary. And that may be both constitutional and statutory.

I find it hard to say today how they would choose between them. But I would think they would be empowered to make both those arguments, statutory noncompliance and constitutional problem.

MR. CARR: Yeah, certainly I think that they would have the authority and ability to make whatever argument they thought was appropriate, just like a lawyer does in any other instance, whether it's in a trial court or in an appellate court.

I think that the lawyer would be able to make whatever argument he or she thought would

be plausible, credible and perhaps successful, in a unique situation calling points to the court's attention that the government isn't and that lawyer thinks would be worthwhile.

But you raise an interesting -- a thought occurs to me, and that is, and I think the system I'm trying to propose could enable this, lawyers often when confronted with new or difficult issues talk to other lawyers and get their input. What do you think? I mean I think it's a natural source that a lawyer in that situation would go.

So I think this is getting a bit more elaborate I realize the further we talk, but on the other hand, within the confines of what I'm suggesting I think you could also enable this small group, just like a small federal public defender's office, they talk amongst themselves. They're privileged. Nobody can make them disclose it. You bounce ideas off.

And I think that would be very important in an area where -- I mean part of the

problem is when these issues come up in front of the FISC, nobody has been there before. You don't have precedents. And you have to think things through in a seminar kind of way.

So I think that's one way lawyers would -- I'm sure Marc does that with his clients and others in his office. What do you think? And that's how it would honed.

I don't think we can prescribe a template for you as to how that would occur. But again, that lawyer would have as much opportunity to raise whatever arguments the lawyer thought were appropriate as the government in terms of access to classified information, and now as I think about it, at least within that small group, talking amongst themselves and sort of jointly coming up with how they go about representing.

And finally the question asked, no, I don't think that that lawyer would be called upon to dream up arguments just to dream up arguments in opposition. He could well say, you know, we have no opposition to voice to the government's

request. End of discussion.

MR. BAKER: As I mentioned, and I'll just be brief, there are lots of issues associated with the creation of this type of function, office, whatever you're going to call it. But if anything, I mean, it would seem to me that the one thing you would want to do is make it clear to the American people that this office is independent and can decide whatever legal position it wants to take in any particular matter. If it wants to oppose the government, it can do so. If it wants to say, okay, no objection, whatever. And if it wants, constitutional issues, statutory issues, factual issues, whatever.

I think you would just have to leave it up to the people in that office or whoever it's going to be to decide whatever approach they're going to take. They have to be independent.

MR. MEDINE: Thanks. I think we have time for another brief round, if we keep our questions within our five minutes, starting with Judge Wald.

MS. WALD: Okay. I've just got really -- sorry. I've just got one question, and I'm returning to the appeal question.

I recognize some of you haven't had the chance to really research it or don't wish to comment, but I want to raise this question. We've been talking about the fact that the FISA Court is a kind of unique animal. I mean it is, I mean I think it's thought of or its conceptualists thought of it as an Article III court, but as has been pointed out it does have some sort of auxiliary, whether it's preventive or approval kinds of functions.

Here, as a former Article III judge, I think I share with Judge Carr, the problem is that this court inevitably must and has pronounced on constitutional questions, questions of statutory interpretation, which I think inevitably become or have to become part our, to the extent they're disclosed, have to become part of our jurisprudence.

So I think the appeal question is so

important to me because not only, I think, some of the FISC counsel have, you know, opined on it, that there may be constitutional questions, so has the Congressional Research Service.

They are applying, you know, absolutely a typical, traditional Article III standing in a situation where the court is deciding Article III questions, but in its original conception it's devoid of one of the most important points of Article III courts, namely people who have an interest in the proceeding not being able to have any voice, for good reason. I understand the secrecy that's involved in national security.

But I guess I'm trying to pick your brains if there is any way to try to solve that question, because to leave these, the highest form of jurisprudence, namely constitutional questions, sometimes questions of statutory construction at a point where they can't be availed of the process which every other part of federal jurisprudence has, namely, you know, an upper tier, even to the FISC, to the FISCR kind of thing.

Some people have suggested a kind of certification but that's had its opponents too. They think you can't do that constitutionally. You've got any positive thoughts on how this --

MR. ZWILLINGER: I'll take a shot at it. I hate to keep coming back to the 2008 court of review decision, but the government argued in that case that there wasn't standing for the providers to challenge. And the court ruled that since Fourth Amendment rights were at stake, the question of whether the provider could litigate those on behalf of users was a prudential standing doctrine, not a constitutional standing doctrine and Congress could waive the prudential standing doctrine and it had done that by putting the standing provision for providers in Section 702.

So I don't see the hurdle quite as insurmountable. If we agree that there are U.S. persons who have Fourth Amendment rights and they would have standing and someone else can litigate that issue on their behalf, it's a prudential question which Congress can waive, not a strict

constitutional one. At least that's my interpretation of that decision and my offer of help.

MR. CARR: In less legalistic terms, because I'm not sure I fully understand the concept of prudential standing, but it seems to me that there a couple of different circumstances.

One may be an instance where there in fact is a target, a person who's named in the order. And that's easy. You can obviously appoint.

Or it seems to me that you could appoint, that that person could be designated to represent the interests of persons affected by this, potentially affected by this order. I mean I think that's what you're saying. They have bona fide interests.

And there's a scrap of doctrine that may not be applicable that you can comment on. Judge, isn't there some doctrine that says where you have a situation that is capable of repetition but will be evading review unless you go ahead and

decide it, even though arguably the particular circumstance is now moot.

I mean, I hadn't thought about the Constitution issue but it does seem to me -- and also Congress gives courts its jurisdiction.

MS. WALD: Congress created the original FISC and in a sense you might say decided that this body of people, for good reason I'm saying, couldn't be informed and become a regular participant certainly if they have terrorist, you know --

MR. CARR: I think the more serious and unanswered constitutional question is can a court play any role in overseeing Article II activities? Congress, the courts and the Executive have all agreed, yes, the FISC is a good thing and FISA is a good thing and we don't want to push it one way or the other, which is something I would suggest to the people proposing what I would suggest may be fairly radical changes, keep in mind all it would take would be the Executive saying, no, we're not going to go along with this. Go to the

FISA Court of Review, whatever it says, and ultimately the Supreme Court. And the Supreme Court might well say the whole structure collapses. Who knows? I mean that's never been tested and I don't think we want it to be tested.

MR. MEDINE: Mr. Dempsey.

MR. DEMPSEY: Jim Baker, you said in your opening remarks, hopefully I'm not misquoting you, but I think you said something along the lines of, we've gone as far as we can go with the FISA Court as, my words, quasi-regulatory body. Would you expand upon what you were referring to.

MR. BAKER: Well, I was referring mainly to Section 702, but I think it also applies to Section 215 as well, which is really, I think, I said the outer limits of what we can reasonably expect a court to do, and to not, we shouldn't think of them as some sort of super inspector general that's, you know, conducting oversight, free-ranging oversight of the activities of the intelligence community.

I just think there are significant

constitutional issues with that. I think there are a lot of practical issues with that. The court's just not resourced to do that. The judges are not trained to do that in that way. They just play a different role.

And so I just, I'm trying to set expectations, I'm urging you to set expectations in a realistic way with the American people about what you can reasonably expect the court to do.

The same applies to Congress. I mean, what can the members of Congress and their staff reasonably be expected to do when it comes to conducting oversight of these agencies.

And in my opinion it's primarily the responsibility of the President of the United States to conduct effective management control and oversight of the intelligence community. That's what I was trying to drive at.

And I think if you, to go back to the original point, if you look at the structure of 702, you've got the court approving these procedures, several different types, looking at

the certification, but not really engaging in review of individual determinations and so on. And then you have sort of after the fact review of things that have happened. I just think you've gone pretty far in terms of what you can ask a court to do to conduct oversight of the intelligence community.

MR. DEMPSEY: I actually have no other questions on this round, so I'll yield. I appreciate the witnesses being here. It's been very helpful. Very helpful.

MS. COLLINS COOK: I did want to take you up, Judge Carr, on an invitation you had given us earlier, which was to talk about the legal advisors and what role they play, because I think there's definitely a sense, and I mean no offense, having been a law clerk, but that these are junior attorneys who are law clerks. And I'm wondering if you would talk a little bit more about who the legal advisors actually are and what role they serve.

MR. CARR: When I started in the court

in 2002 there was one legal advisor. When I left I think there were four or five, I can't remember.

These are, they are neither law clerks nor magistrates, okay. It's a unique role that they perform. I think I can speak for myself when I say, and I'm the author of a treatise on electronic surveillance so I know more perhaps than most FISA judges going into it, but they know more about FISA, FISA law and national security law, the workings of the agencies than any individual judge can. And we rely upon them and their judgement to assist us in making decisions.

To give you an example, they get by FISA rule, FISC rule, seven days before we get an application, and they review it carefully. It's called the read copy. And Jim will confirm, I'm sure, there's a lot of push back between the legal advisors on behalf of the court and OIPR.

I know from personal experience there's a lot of push back between OIPR and the agencies. As someone said this morning, they don't want to present junk because if they do, we're going to

lose confidence in it, and it's going to be much more difficult unless they are straight up with us.

But the legal advisors, and not infrequently I would come in and let's say I would have X number of cases set on my docket, and that number grew substantially when I was there. But I would be told this case, that case, the other case and another case are off docket.

And it's my distinct sense that it was off docket, in other words would not be formally presented to me for review because of the interaction between the legal advisors and the OIPR attorneys and the agencies, whom I believe the legal advisors called them directly with questions and problems.

That was a core part of their job was rigorously to vet the applications. And one of the things that I think should be considered would be that the number of instances, the instances in which an application is submitted for review by a legal advisor but never presented to a FISC judge

for consideration, that those two should be registered, recorded and published because I think there would be -- I mean was it a large percentage? No, but it was a, Jim, would you agree with me, fairly regularly cases would come off docket.

MR. BAKER: Or they'd be, they'd either come off completely or they'd be postponed to another week because we were trying to resolve some question that the legal advisor had raised, yes.

MR. CARR: Right.

MR. BAKER: It would take us some time to finish that analysis.

MR. CARR: But I do think it would not be that difficult to give every read copy a number and then that keeps that number and when it comes off docket, it never comes back, they decide not to present it, and there are instances like that, I assume because of push back from the legal advisors. And that would, if nothing else, show that the rate of rejections in terms of the

overall operation of the court is higher than the simple turndown by a judge.

But I mean to say that these are law clerks, they occupy a unique role. And then we have great confidence in them. They work for the court, but in a very important way they help ensure that we make the decisions we should.

Very often they would write a memorandum for us about some aspect. And then, of course, we would sit down and read these things. And they're not two page search warrant applications. They're 40, 50, 60, 80, 100 pages. Very thorough, like Title IIIs, every bit as lengthy and thorough as a Title III.

And we would often have questions, and I would call an OIPR attorney and say, look, can you give me this or that.

And on occasion I would actually have hearings. I would question the agent and the lawyer under oath, always on the record, even though it would never be public. And I'd make a finding and I would determine that my questions

had been answered, so.

MS. COLLINS COOK: Thank you, all three of you for being here today. I appreciate part of what we're doing here is attempting to educate ourselves, part of what we're doing is attempting to educate other people who might be thinking about this, so I appreciate the thought and the time that you've put into your answers.

MR. CARR: And certainly speaking for myself, if there are other questions that the agency has, feel free to communicate with me. I'd be glad to answer them.

MR. MEDINE: Thank you.

Ms. Brand.

MS. BRAND: Thank you. I wanted to follow up on something that I asked the government witnesses about this morning and there wasn't a full, we didn't get to do a full answer on that panel, which is going back to the 215 bulk metadata collection and the RAS standard.

Jim, I think you were in the audience for this discussion about if there were a

requirement that the government submit to the FISC after the fact the RAS selectors.

So this phone number is now a selector and here's the paper trail that is the basis on which the selector was established.

What would the court do with that? I mean first of all, do you think that the court could do something useful with that? Would this be an actual check on the system, or would it overwhelm the court? Can either of you speak to how that would work in practice.

MR. BAKER: I don't see how it would overwhelm the court and --

MS. BRAND: How it would or would not?

MR. BAKER: Would not.

MS. BRAND: Would not, okay.

MR. BAKER: I don't see how it would overwhelm the court. You just have an Excel spreadsheet, you write down the selector, you write down the basis, the little field off to the side, date, time, all this kind of stuff, and you submit it to the court on a regular basis so it's

not too onerous for the government to comply with because I think that is a real issue.

And then I would imagine that the court would look for patterns to see if things were going along in a way that they, that was consistent with their understanding of what they were thinking when they approved this thing. And it would be an additional check.

To me, I have to say I don't see that as that onerous of an additional obligation. And I do think it would be useful for the court to have additional transparency. And it seems like it's something that would give the American people additional confidence that what's going on is legitimate and appropriate.

MR. CARR: I would think to do that you would have to first of all, the analogy is to the periodic progress reports that all Article III judges get with a wiretap, review, minimization. Again, it's all in the record, ex parte. Put them under oath, how is the investigation going, are you getting anything. I make a renewed finding of

probable cause for the Title III tap. Necessity, you're doing a good job at minimization or you're not.

So it does seem to me that this is a function that Article III judges would be familiar with performing in a similar way.

The one thing that occurs to me though it seems to me for it to be useful you would have to go back to the particular judge who issued the PRISM order, whatever the order was.

MR. BAKER: This is 215.

MR. CARR: Pardon?

MR. BAKER: This is 215.

MR. CARR: 215, yeah. To go back to that judge because that's the judge who gave the original authority, rather than whatever judge happens to be there that week.

Again, I don't know. But I suppose in time any judge would develop enough familiarity to have enough handholds to evaluate the reasonable articulable suspicion in this context.

MS. BRAND: And Jim, just quickly for

you that there was some discussion during Beth's question about the back and forth between the court's lawyers and the government.

Can you talk about the back and forth that happens within the government? I mean is there a quasi-adversarial process within the government before an application ever gets to the FISC? Who's involved in the application? Can you talk to that?

MR. BAKER: So it depends what kind of application, whether it's from the FBI or NSA, you're going to have different levels of review.

With the FBI you have review within the field office, you would have review at FBI headquarters. It would come over to the Justice Department. You would have review there. And then it would go to the FISC.

At NSA you're going to have similar type of review. Obviously there's no field office in that sense.

But look, I mean the review and the meticulousness and the care that people put into

these things is substantial. There is a lot of dialogue back and forth between every level, among every level of this. There's back and forth between FBI headquarters and the field. There's back and forth between DOJ and FBI, or DOJ and NSA. There's a huge amount of back and forth.

And I always took it as a huge amount of my responsibility to make sure that I maintained at all times the credibility of the Justice Department in front of the FISA Court so that we were transparent with the court about what was going on so that the court knew that we cared deeply about the accuracy of these applications. That when we made mistakes, as we did, we brought them to the attention of the court. That we tried really hard not to make mistakes.

And so it was really, you know, the Justice Department, again in my opinion, doing its job, executing its responsibilities under the Constution as delegates of the President to help him take care that the laws are faithfully executed. Congress passed this law, it's our job

to enforce it. We're going to do our best to make sure that it's enforced in the right way. And if we think that the agency hasn't met the standard, then we're going to tell the agency they haven't met the standard yet and they've got to do X, Y and Z to do that.

So I mean I think that this system has worked extremely well so far, but it's clear now and it's painful to me to see that some percentage of the population of the United States doesn't think that, and so we need to take that seriously and figure out how to deal with it. And that's your job.

MR. MEDINE: Thanks. In the interests of keeping, because I just want to ask one final question, which is the point was made earlier that this outside party, advocate, amicus might have a role in compliance reviews. What role would that be and how would that play out?

MR. CARR: Well again, in my thinking about it, I mean once again, I mean many times compliance, a noncompliance notice is really quite

straightforward and quite simple. But in the event that you had something that was more complex and you wanted to be really sure that the problem had been identified and addressed and would not recur, again I think at the very least the FISA judge should have the opportunity to have this independent counsel participate in an adversary mode with the government prosecutor and conduct a hearing the way we do with a suppression hearing or whatever, and then make a decision.

One would hope that the decision ultimately would be okay, things weren't as bad as they looked and it was good faith and it's been fixed.

But I do think that there would be a role for the attorneys whom I envision participating in the process from time to time.

MR. MEDINE: Other panel members have a comment on that?

MR. CARR: It's not a career enhancing move for somebody in an agency to make a mistake, to get it wrong. And one of the things that

impressed me as a young magistrate about the FBI and DEA and so forth, and I had the same kind of, I grew up politically in the 60s. I had apprehensions about the government and FISA secret court. And one thing I can assure you has impressed me from day one and throughout my activities in the FISA Court is the people who do this work want to get it right. Not just the lawyers in the Justice Department, but the agents out in the field.

And the other thing I want to say is, I alluded to this before, I know that at least the FBI on frequent occasion was not happy with them because they were not going forward to present something that the bureau very much wanted it to.

It's not an adversary relationship but it's not a hand in glove relationship, or it certainly was not when I was on the court. One did not have that sense that they were just presenting anything that the agency wanted.

MR. ZWILLINGER: Just to comment briefly, I would just be very careful about using

the independence of this office to start getting involved too far in what might lead them to be captured by Executive Branch activity.

That is, if we believe there's some role for an adversary in this process, some role beyond what the legal advisors who sound like they're both brilliant and helpful play, then that person should be, should retain some of the independence, and they shouldn't play too many roles or positions in this so that they can both challenge from an independent point of view and convey that independence to the American public.

MR. MEDINE: I want to thank the panel for giving us a unique insight into the operations of the Foreign Intelligence Surveillance Court.

We'll take a break and resume at 2:45.

MR. CARR: May I just say one thing that occurred to me this morning?

MR. MEDINE: Sure.

MR. CARR: And also before the Senate Judiciary Committee, let's all keep in mind what a remarkable country we live in where we're having

this kind of conversation about these issues, and what a remarkable institution we have in the Foreign Intelligence Surveillance Court, because I don't think any other country has anything like it. Can you imagine this conversation occurring anywhere else in the world? And I think we should all keep that in mind and take pride in that.

MR. MEDINE: Excellent point while we go on our break. Thank you.

(Off the record)

MR. MEDINE: All right. We'll be starting the final panel which involves academics and a former member of Congress.

We're pleased to be joined by Jane Harman, who's the Director, President and CEO of the Woodrow Wilson Center and a former Member of Congress, Orin Kerr, who's a Fred C. Stevenson Research Professor at George Washington University Law School, Stephanie K. Pell, who's the Principal in SKP Strategies, a 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 at Perdue University, and Stephen Vladeck, Professor of Law and the Associate Dean for Scholarship at American University Washington College of Law.

To the panel members, I understand you're free to make a brief statement and then we'll do another round of five minute questioning on the panel.

So Congresswoman Harman, if you'd like to start.

MS. HARMAN: My apologies for being a few minutes late, but I'm delighted to be here. I consider myself one of your grandmothers. I was a principal co-author of the Intelligence Reform Law in 2004, which established you.

And one of the tragedies I think history will record is that you were not fully functioning until May of 2013. That is about eight and a half years lost of a very, very critical mission.

And let me just say that the goal in

the law, and certainly my personal goal, was to have a group inside that would make certain that privacy and security, or that liberty and security were reinforcing values in the policies and practices that we established under the law.

And if ever that function were needed it is right now. It is unfortunate, at least to me, that you are one of the best kept secrets in Washington. I know you're making a massive effort to get out there and I commend you for it, but I think the need is urgent.

And you uniquely, among the different groups now looking at some of our policies and practices, I think are in a position to make sure from the inside that we are doing the right things.

Let me just make two other points. One, I was in Berlin, Germany this week, no, last week, a week ago today at a dinner of top policy types and think tank leaders and business people, all of whom were shocked and horrified by the revelations in European newspapers.

When I told them that there was a Privacy and Civil Liberties Board in the United States and it is now holding hearings and I'm testifying next week, they looked stunned, and said, gee, that's wonderful. I hope that a group like that will also be in touch with foreign governments.

And so I put that out there. I'm not sure whether that's in the mandate or it isn't, but it might be interesting to think about connecting to those folks and maybe forming some common cause about ways to look at the practices and procedures of different countries.

And finally, I would just offer my own observation about all of this, which is that we need, this isn't maybe your mandate, but our government needs crisis management 101. It seems to me as a recovering politician that when bad stuff is coming your way, when, let's just imagine some guy named Snowden has taken a lot of stuff from the government and it's dribbling out, you get ahead of it, and you figure out a frame, and

you figure out a context, and you talk about what else could come out and what it means.

And this is just free advice again from somebody who spent 17 years in the United States Congress. Some crisis management function at the highest level of our government I think could be helpful, along with a very robust Privacy and Civil Liberties Board.

So I'm delighted to be here. I don't know that my testimony will be as technical as my well-qualified colleagues, but I have been in this game for a long time and I passionately hope that things turn out well for our country and that we have both security and liberty to look forward to.

MR. MEDINE: Thank you, Congressman.

Professor Kerr.

MR. KERR: Thank you for the invitation to testify here this afternoon.

The FISA statute is premised on a search warrant model, putting Article III judges in the position of judges evaluating search warrant applications. And that model isn't

working because the search warrant model is premised on the judge serving essentially a ministerial function.

When a judge reviews a search warrant application the judge is looking for probable cause, looking for particularity, but is not trying to conduct a comprehensive review of whether the statute is being applied correctly, how the statute should be interpreted and what the constitutional implications might be of the warrant, if issued.

That doesn't work in the high technology area because technology is simply changing too quickly.

Judges are therefore being asked to resolve difficult issues of interpretation which they are just not competently equipped to answer in the context of an ex parte application such as a search warrant application.

And the various proposals that were discussed earlier this afternoon at the FISC panel were really about various ways that the FISC could

be restructured to make amendments to the warrant model.

The special advocate approach is one approach, encouraging disclosure of interpretations is another approach. And both of those are I think, are interesting and important and promising ideas for how to reform the Foreign Intelligence Surveillance Act to deal with new technologies.

Let me suggest two other approaches. One, which has been discussed and implemented, and the other which has not been.

One approach is that of sunset provisions, having the government's authority lapse for a certain number of years and then expire, putting the burden on the government to seek renewal of that power. I think sunset provisions which were originally designed to have, sort of act as a testing time to see if the government still needs that power a few years later.

Today instead, in light of new

technologies is really a way of ensuring that the government can go back to Congress, or rather has to go back to Congress to seek approval for any new interpretations of the law.

So combining the sunset authority with disclosure of interpretations that the FISC is taking is, I think, one important step.

Another approach which has not been suggested so far would be a rule of lenity for foreign intelligence surveillance law. You may be familiar with the rule of lenity in the criminal context. The idea is that when interpreting a criminal statute judges should adopt the narrower interpretation of the criminal law, and that requires if the government wants to adopt, have a broader interpretation of the criminal law they have to go to the legislature and have the legislature enact it. The idea being that the laws are ultimately up to Congress, not up to the courts.

A rule of lenity for surveillance law would serve a similar function. The idea would be

if the government goes to the FISA Court and says here's an interpretation of the law, if it's a close call the default should be for the FISA Court to reject the interpretation and to tell the Executive Branch that they have to go to Congress to get Congress's approval for that interpretation of the statute.

This would force the Executive Branch to go to Congress and not try to seek approval of new programs from courts that are poorly equipped to analyze the questions here, especially involving the normative desirability of these programs.

Effectively the sunset provisions and a rule of lenity working together with disclosure would force the Executive Branch to keep going back to Congress as technology changes to have Congress whether to approve or disapprove any new surveillance programs. Thank you.

MR. MEDINE: Thank you, Professor Kerr.

Ms. Pell.

MS. PELL: Thank you to the members of

the board for inviting me to testify today. It's quite an honor.

Putting on my hat as a former congressional staff member, I'd like to raise two process or transparency points that I think relate to some of the discussions on both of the earlier panels.

We heard on the prior panel the idea that the FISC having had or currently having a mechanism to seek review of outside technical experts.

I think that is an excellent idea but it is an equally important resource for staff members and members of committees. In my experience working on reform of the Electronic Communications Privacy Act, which was not done under essentially working with classified information, myself and my colleagues were able to contact outside experts, professors at universities, people who had worked in the telecommunication industries for decades, in order to get a view of current technology and its

capabilities and where that technology was going in the future.

Now, of course, we heard from the government also and it shouldn't surprise anyone to hear that the government's views often did not a hundred percent comport with the views of these outside experts.

What I'm saying shouldn't be either surprising or seen as a criticism. The government of course is an advocate. It has a very important mission to do and it's going to present the views of technology in a way that best represents its positions.

But what these outside experts could do in addition to often getting a different view from government, was help the committee look towards the future to understand where the technology and its capabilities were going so that in the course of trying to write statutes that wouldn't become obsolete with the next new iPhone model, we had the necessary information for forward projection.

Secondly, and this point goes more to

the discussion on 215 and something, Judge Wald, you raised on the first panel about things that have been said in different press outlets by different experts regarding the fact that the government's interpretation viz-a-viz bulk collection and relevance was perhaps novel or a little idiosyncratic, certainly not something that even people who perhaps were experts in surveillance law could read that statute and say, oh, I could see how the bulk collection authority would be operating under this statute.

What I'd like to raise is a problem that occurs from a process level, as a committee staff member especially on the Judiciary Committee where certainly we hear classified information and we often need briefings, to have briefings behind closed doors, but committee staff members and members interact with nongovernmental stakeholders who have real interests in how these statutes are written and how they affect the privacy interests of the general public.

When you have a situation that a

government's legal interpretation essentially is hidden from public disclosure, the dialogue that must occur between the staff and the committee members and these nongovernmental constituencies frankly can be very dysfunctional.

Because when you discuss why you want to make a change to a statute but are not able to talk about what you think that change will do, it can have the effect of having those nongovernmental constituencies ironically argue for changes in the law or reject proposals that are not in their interests.

I think that raises a very problematic process question, calls into question the integrity of the legislative process with respect to legal interpretations of statutes that must remain essentially hidden from public disclosure. Thank you.

MR. MEDINE: Thank you, Ms. Pell.

Professor Spafford.

MR. SPAFFORD: I'm not a scholar of the law but of systems and I studied systems for many

years and find ways where they can be exploited or where they can be bolstered. And I'd like to present to you two high level thoughts about systems viewing this.

The first is we've heard from many people today and over the past many months about how carefully this is controlled. It's vetted. The requests are scrubbed. The information is closely guarded. And we can perhaps take that as given and realize that we do have a number of people who are working very hard in the nation's defense and the nation's interest.

The concern with privacy however is that if those systems are constrained and controlled within a very small private, closely held group then it is possible that under political circumstances or stress they can swing out of control beyond what we intended.

And this is by no means unusual given the country's history. We look at things like the Alien and Sedition Act, the Japanese internment in World War Two, the COINTELPRO investigations, the

McCarthy hearings, and President Nixon's enemy's list is just a few where government systems were then used for political aims or for aims that were then later ruled unconstitutional.

So what we need to do is look at where are the points at which this can be controlled, where are the points at which we should observe to make sure that this system cannot be subverted.

And we're lacking in the transparency and the openness necessary. We don't have the adversarial capabilities. The fact that people who have these orders served against them cannot talk about them, cannot bring them up before a court are all considerable problems in terms of righting any wrongs or oversights. That should be addressed.

In particular we have heard how some of our elected representatives are unable to hear all of the information about these programs, to engage their cleared staff and to have conversations with each other about some of the issues involved.

To my knowledge we have not elected any

terrorists to Congress, at least not of the kind that we're looking for. We are not in a position where we have terrorists in the judiciary, or terrorists operating our ISPs. To prevent those individuals from helping to safeguard our privacy and our constitutional rights is really counterproductive to the interests of the nation.

So I would suggest that you look at that as one thing that might be considered. In general I believe that classification is over-used. Anything that's classified should be classified only to protect the safety of a party or for operational efficacy.

It should not be used to hide things from the American public. Things that are classified when they come out, the American public should say it's too bad we lost that capability but they shouldn't be ashamed of what our government is doing. And we have seen instances of that I believe in the last few months.

The second comment that I'll make very briefly about systems is more technical. I

circulated to you a set of fair information privacy practices that have been put together by the U.S Public Policy Council of the ACM.

These help govern good privacy and databases. I would ask that you look at those as you consider possible changes. The more of those that are upheld the better we protect the privacy of information.

And the more information we collect the more likely we are to collect noise, particularly if we have that information stored for a long time. In any system the more we try to avoid false negatives, that is missing cases of things we're looking for, the more likely we are to generate false positives.

And there is a concern as well for the American public that in the process of trying to be sure that we stop every terrorist threat we cast a net that is too likely to engage those individuals who are involved in unusual but not illegal behavior.

And I'll be happy to answer your

questions later. Thank you.

MR. MEDINE: Thank you, Professor Spafford.

Professor Vladeck.

MR. VLADECK: Great, thank you, Chairman Medine, members of the board. It's a pleasure to be here. You know, given the lateness of the hour and the far more interesting nature of your questions I'm going to try to be very brief.

We've heard a lot already today about the idea of a special advocate and so I thought I'd focus my short opening remarks on that proposal.

I suspect the members are familiar with a Congressional Research Service report that was I think disclosed last week about constitutional concerns with the special advocate. And I thought I'd briefly address the three major ones that the report raises.

First the report suggests that a special advocate would raise Article II problems with regard to the appointments clause and how

that office is set up. I actually think this is perhaps a non sequitur.

I don't really think there's any current proposal, including the Leahy-Sensenbrenner bill that would actually constitute the special advocate as anything remotely resembling what the Supreme Court referred to as an officer of the United States in Buckley versus Valeo. I'm happy to elaborate on that but I actually think this is a bit of a red herring.

The second bucket of issues that the CRS report raises is concerns about adverseness in the FISA Court and in FISA proceedings. Of course this has been a structural concern in FISA since long before the current controversies. Indeed Judge Silverman when he testified about FISA in 1978 raised this exact concern as a constitutional objection to FISA.

I'm happy to elaborate more on why I am not convinced that this is a problem. I think the only relevant point for now is that a special advocate would not exacerbate any adverseness

concerns that currently exist.

That is to say there may be adverseness concerns under 702, under 215 with FISA as currently constituted, having an adverse party only should ameliorate those concerns and not make them worse.

Instead I actually think the hardest issue raised by the CRS report and the one that I do think is the biggest head scratcher for the special advocate is the appeal question. So the Supreme Court just said this summer in the Proposition 8 case that a party must have a direct stake in the outcome in order to appeal an adverse decision by a lower court, as within the Article III system. And I for one am pretty confident that the FISA Court is part of the Article III court system. And obviously I think some of the current proposals would not invest the special advocate with such a direct stake in the outcome.

So it seems to me that there are two responses to the problem posed by the Perry decision. The first is to create a direct stake

in the outcome. That is to say to actually have the special advocate not just representing some amorphous undifferentiated interest, but to actually represent U.S. persons whose communications might be intercepted pursuant to the surveillance being authorized.

That might raise policy questions that are difficult to think about. Certainly we have precedent in our legal system for such sort of separated representation, Guardian Ad Litems are a good example, class counsel under Rule 23(b)(2) class action, even for example, the habeas lawyers for the Guantanamo detainees, who routinely have access to classified information that cannot be shared with their clients.

So one possibility around this problem is simply to create that direct stake. The other is to avoid it. And so I suspect there's been some discussion among the board about the idea of certification.

That's one possibility where you could have the FISA Court certify particularly difficult

legal questions to FISCR. This could be modeled, for example, on the Supreme Court certiorari statute 12542, which allows for circuit courts right now to certify questions for the Supreme Court, quote, at any time, unquote. And whether or not a party is asking for such certification.

Another possibility would be to borrow an example from the bankruptcy context and actually bifurcate the FISA Court's decisions into those that the FISA Court is allowed to render as a final matter. Those could be sort of cases not presenting novel questions of law or reauthorization cases, in which case the FISA Court would be empowered to act finally, and those in which it could actually only issue a provisional report and recommendation that actually had to be confirmed by the FISA Court of review on appeal. That's how the bankruptcy court system works right now with regard to core and non-core proceedings. I think that's another way to sort of get around the problem.

The larger point, and then I'll stop,

is that I think the appeal question shouldn't distract from the advantages that having some kind of adversarial participation in the FISA Court itself would bring, even if we can't ultimately solve how we allow them to appeal if and when they lose.

Thank you very much.

MR. MEDINE: Thank you, Professor Vladeck.

Ms. Cook.

MS. COLLINS COOK: Thank you all for joining us today. All right, I'm having the same problem that one of our panelists had earlier today.

I wanted just to go back to something that the first three panelists discussed and that's the issue of congressional oversight. I think you've seen an evolution over time in terms of congressional oversight. You see it both with respect to the addition of the Judiciary Committee as receiving reports, exercises an oversight function in addition to the intel committees.

I think you also see it in a movement away from a traditional, fully-informed standard up to the hill to specific reporting requirements, a whole range of specific reporting requirements.

And my question is a general one, which is, do you think that we're in the right place right now in terms of congressional oversight?

And I would separate between an ongoing oversight function and the need to legislate or reauthorize in a sunset situation. Or should Congress be taking a fresh look at how it exercises its oversight capabilities?

And I guess just going left to right might make sense at this point, my left to right.

MS. HARMAN: Your left, so that would be me?

MS. COLLINS COOK: Yes.

MS. HARMAN: Okay. It took me awhile. I think it's a great question and I think it's something that has to be revisited, but I was there. I was working in the Carter White House when FISA was passed in 1978. I wasn't part of

the hardy little band that on a bipartisan basis that crafted the law. But I was impressed by the fact that the basis of FISA is a robust functioning of all three branches of government, Executive Branch policy reviewed by the FISA Court and overseen by the Congress. That was the deal.

And that worked very well, my impression until 9/11. And then the event of 9/11 but also the fear of ongoing 9/11s caused the Bush Administration to feel that we need a dramatically enhanced response or aggressive, an aggressive approach, not just a response.

And they ignored FISA for a couple of years, which I only found out afterwards, although I was a member of the Gang of Eight. And Congress pushed back and amended FISA to catch up to technological change. And FISA and other laws, PATRIOT Act and other things that have been mentioned, certainly Executive Order 12333, although it's not a law, are in place now.

So what is my basic answer to you? I think robust oversight is crucial. I think it

should extend beyond the intelligence committees, although I think they have a special role because they have a special understanding, or are supposed to, and I hope I did, of what the challenges are.

But I think because of the reach of these programs all members of Congress should have some role in oversight. That's number one.

I think the challenge is the changes in technology. Others on this panel know a lot more about that than I do. But it is very hard to craft either a law or an oversight regime that can anticipate, you know, what iPad or iPhone 6S is going to look like and what capabilities it might have that iPhone 5S doesn't have. And I don't mean to limit it to one manufacturer.

But what else is going to be out there that we can't imagine, or I can't imagine? Remember, I'm the grandma, these kids can probably imagine it.

MR. KERR: Just briefly, because this is a great question although, in large, outside of my expertise. But one issue that I think matters

a lot is whether, what is the reference point that Congress is looking at the question from?

So if there is a sunset provision or if the FISA Court is taking a conservative interpretation of the law, the Executive Branch has to go to Congress and has to get comething from Congress. It has to persuade.

And when the Executive Branch is in a position of needing to persuade, that is going to lead to better oversight than the opposite. So if the FISA Court is taking an aggressive interpretation of the law, it's relatively difficult I think for the legislative branch to give the kind of oversight that it needs when it's effectively trying to say, okay, what might be going wrong that nonetheless has been approved by the FISA court? It's a difficult position, I think, for the legislative branch to be in.

So one of the benefits I think of the sunset provisions and the rule of lenity idea is it effectively means that the Executive Branch has to go to the legislative branch and make the case

affirmatively. And I think that's just going to lead to better oversight.

MS. PELL: And I'll sort of take the end of what Professor Kerr said and when the Executive Branch has to come to the legislative branch, the legislative branch has to stay engaged.

If there are continual reasons to be viewing things because they are sunsetting or the Executive needs to ask Congress for something on a regular basis, the staff are going to stay engaged, the members are going to stay engaged. It's going to be a priority. And I think it needs to be a priority. Thank you.

MR. MEDINE: Thank you.

Ms. Brand.

MS. BRAND: Thank you. Just to follow-up on Beth's question about congressional oversight. Those of you who were here for the previous panels heard me ask about the proposals to have a return requirement to the FISC where the government would have to go and tell the FISC what

it was doing after the fact. So it's not congressional oversight, it's judicial oversight.

And I have a somewhat cynical view that sometimes reporting requirements are a fig leaf and not particularly effective oversight because, you know, they impose massive, massive personnel burdens on the Executive Branch and then it goes into a black hole and no one ever looks at it.

So that was the reason for my questions earlier. And I would have the same question I guess about congressional oversight. If, you know, very granular, there is already a lot of congressional reporting under FISA, and if it were increased even beyond what it is now to include some very granular reporting, what would Congress do with that information and does it actually enable a greater level of oversight than already exists?

So I guess maybe for Congresswoman Harman and Stephanie.

MS. HARMAN: Well, if I weren't an optimist I wouldn't have served in Congress for

seventeen years. I think Congress is capable, I think members are capable, not equally capable. I think committees are capable and it's a tragedy that we seem to be basically ignoring the regular order, the committee process in at least this Congress and the prior one.

But I think the intelligence committees and other committees of jurisdiction could staff up to do this well, even the granular stuff. There are very smart people that are sitting right here who could be hired with the focus on this, and there are members who really care about getting it right in both parties. And obviously the public is now intensely clued in. And once the Privacy and Civil Liberties Commission becomes a household word, you're going to keep attention focused.

So I think this is doable. Yes, it will take a commitment of resources, and not just financial resources but brain cells to do it right.

And I think the challenge is going to

be that the goalposts keep moving, that it is going to change because the capabilities of both our technology and what the bad buys can do are evolving and keeping on top of that and understanding what that means and then understanding what the requirements are, not just what does the law say, but who should we be focused on and how should we be doing this?

And again, it might just, in two years or ten minutes, not just be bad phone numbers and bad email addresses, it could be something in the cloud that I can't even imagine, or something beyond the cloud.

MS. BRAND: Okay, thank you.

Stephanie.

MS. PELL: Obviously you want reporting requirements or information to be useful but without it what can Congress do?

I found one of the most challenging aspects of reform of criminal investigative authorities was just getting accurate information about how technology functions, about how often

the government was using certain types of authorities.

Those kind of metrics for dedicated staff and members, and they are there, is very, very useful, but if it's not there, you know, where is your starting point?

MS. BRAND: Do you have a view, any of you, on what type of information is not currently provided that could be provided that would be useful?

MR. SPAFFORD: I wanted to add to that that reporting is not sufficient because with the technology and with the complexity I can craft a report that says everything and means nothing to the people who read it because they don't have the background.

Unless we allow those with expertise in the area and time in office, and this is largely staff function, the ability to ask questions to be brought out to either the court or to elected representatives, they aren't going to actually be able to understand what's going on with some of

the very complex technical issues.

And so again, I come back, I have this concern that reports have kept staff from being able to even be briefed or aware of these things or to discuss it with members. And many of the members have backgrounds in law, or education, or other issues, where they don't understand the technology and they really depend on the staff to help them to get to those bits of information.

MS. BRAND: Professor Vladeck.

MR. VLADECK: I mean, I think there's also an incentives problem, right. So I think, you know, I mean we can all, I think, agree that everyone's working on what they see as the best interests of their constituents.

But the problem is that when this is all happening in the dark, you know, I don't know what the incentive is for members to go down in the skiff and spend hours and hours going through materials that they may not even understand.

You know, I think last Tuesday's HPSCI's hearing we brought this out quite sharply.

I mean, I think when you have the Chairman of the House Intelligence Committee saying it's not a violation of our privacy if we don't find out about it, you know. I mean the question is how do we change that mentality, not just among, you know, the popular discourse, but among the members who are tasked with this oversight function.

And then part of that is not just better reporting and better opportunity to actually engage the reporting, but also some mechanism through which it's more in their interest to exercise the oversight, as opposed to just sort of keeping things under the rug.

MS. HARMAN: Could I just add one thing because I thought your question wasn't just about reports, I thought it was about oversight.

MS. BRAND: Where the reporting enables oversight.

MS. HARMAN: All right. But oversight is much more than reports. Oversight is, it can be offensive too. It can be asking questions, requiring people to come up and report, reviewing

materials.

I mean, back in, you know, in the antediluvian days I'm told that Mike O'Neill, who was the Chief Counsel of HPSCI for years in the 80s, read every single FISA application, read every single FISA application. Now that to me is pretty darn good oversight, assuming he knew what he was reading, and he's a very smart guy. He's still around.

Yo, I mean that would be impossible now. There's too much going on. But it seems to me that the right people motivated the right way with adequate resources, and part of that is the determination to focus. And I think, don't sell members short. Of course, why wouldn't I defend members? But don't sell them short.

Some members are keenly interested in this and can make it a priority to focus on this. And I think we need a staffing pattern that enables those members to do that. But I think there are members who have been and are and will be very conversant with intelligence and know how

to do oversight.

MR. MEDINE: Professor Spafford, earlier you said that there was a concern that the more information you collect to avoid false negatives, the greater the risk of false positives.

One could read that as an implicit critique of the haystack model that the administration has advanced for Section 215. If that's the case do you have an alternative for accomplishing the same goals without the haystack?

One option that was discussed earlier today is to access information at the provider level, using I guess a federated search model or something similar to that.

What are your thoughts on potentially, I guess, technological solutions that avoid the problem that you seem to be concerned about?

MR. SPAFFORD: It's difficult to give specific examples without delving into specific systems.

I will say that in general from what I

have seen in the open press, the theory is collect all of the information in case it's useful and then mine all of that.

And the problem there is it's possible to collect huge amounts of information that have no bearing or lead to false results. In fact, it can obscure the results because it introduces noise.

An example of this is the analysis that uses the three hop collection for contacts. What I have seen, and I do not have personal experience with this, but what I have seen mentioned is that a two hop analysis is much more accurate. A three hop analysis begins to pull in people at car rental agencies and hardware stores and pizza places and actually introduces more noise.

It would reduce the amount of searching, the amount of data necessary and some of the concerns to have a more tailored approach.

But fundamentally at its heart it's a question of, where are our values here? Is this such an existential approach that we have to

collect every bit of information that goes across every communication line in hopes of catching every last person who has harbored an inimical thought?

Somewhere there needs to be a little bit more balance where we're willing to use traditional police and intelligence methods for safeguarding ourselves and not try to head everything off in regards for helping with privacy.

MR. MEDINE: Thank you. Professor Vladeck, earlier you talked about one potential model to get appellate review and the Foreign Intelligence Surveillance Court of the bankruptcy approach, which is that the lower decision is not really final until reviewed.

How would you square that with the exigencies of surveillance needs where having a non-final order if it doesn't permit the government to engage in surveillance could actually delay critical surveillance activities while the review process goes forward?

MR. VLADECK: Sure. I mean I think it actually wouldn't be that difficult. I mean you could analogize it to a preliminary injunction but just sort of reverse it, right.

So the idea would be that an interim order by the FISA judge would be sufficient to allow the government to act on an interim basis pending review and finalization by the FISCR.

And then, you know, I think the idea would be that would sort of solve both problems. It would allow the government to act once they make the initial prima fascia showing to the FISA judge, and then it would allow for subsequent retrospective review by FISCR without running into the problem.

And that, you know in the bankruptcy context, I mean the bankruptcy court has the power to issue interim orders pending confirmation of their report. And so I think you could just borrow that analogy and work it all the way out.

MR. MEDINE: And when would you have this apply? I mean we've heard that there are,

the vast majority of what the FISC does is routine requests that don't raise novel legal or technological issues.

Would you have these bankruptcy model approach in every single request to the FISC, and if not, how would you determine which requests it applied to?

MR. VLADECK: Well, see the whole point of the bankruptcy model is to actually divide classes of cases, right, and so the bankruptcy model divides what are called core proceedings from non-core proceedings.

And in core proceedings, which might be analogous to the sort of non-interesting FISC cases, the bankruptcy court does have the power to act finally and without any appellate oversight.

And then it's only in the non-core proceedings in the bankruptcy context that you have that review.

So it seems to me you could have some trigger, so some of the proposals include any decision turning on a significant question of law

or a significant departure from prior.

I mean there are ways to sort of make that threshold work, and it could be whether it's a novel interpretation. It could be whether it's application of an existing precedent to a new set of facts.

I mean, you know, I think the devil's in the details but I think you could find a way to agree on a sort of a trigger that would sort of sort cases into one of those two categories.

MR. MEDINE: And I guess because if you get to the FISC review on that basis, which I understand, how do you get to the Supreme Court? I mean the Supreme Court does seem to raise a case in controversy question of going from the FISC review up to the Supreme Court because you don't have that lack of finality that you would have had from the lower court.

MR. VLADECK: Yeah, I mean I think the Supreme Court issue is still a problem. You could presumably solve it the same -- not the same way but sort of an analogous way. I mean so it's

already the law under 28 U.S.C. 1254(2) that all of the circuit courts can certify questions to the Supreme Court at any time. It would be, you know, a four word amendment to 1254(2), right, in parentheses, including the FISA Court of Review. All right, that was more than four words. Right.

And then you know, presumably that wouldn't provide for mandatory review. It wouldn't provide for automatic review, but it would also allow FISCR, if there were cases where FISCR thought it was a sufficiently important question to raise it to the justices' attention, FISCR could then send it to the Supreme Court. And the Supreme Court say we don't care. I mean that's, you know, the Supreme Court hasn't answered a certified question since 1981, you know. I mean I think it's their prerogative to ignore FISCR, but at least FISCR would have the ability to try to get their attention.

MR. MEDINE: Thank you.

Judge Wald.

MS. WALD: Okay. There's been a lively

debate on some of the outside commentator on 215 as to whether or not it is sufficient to have, let's say, the representative democracy model for big, bulk programs like 215.

You know that is, we have elected our members of Congress, if they set up a system for review, be it the Gang of Eight, Jane, or be it something broader, then that's it and, you know, the people just have to live with that.

Of course, one problem with that always is that even if you adopt this, theoretically the peoples' resort is not to elect the same people if they don't like the same people, but if they don't know about the program that's in there, that particular exit strategy is not worth that much.

But the deeper thing is, is that the right model or is the model which some people have written about that when you get to a program, not the individual warrants, but when you get to a program that really encompasses a large portion, you know, of people and inevitably a large portion of innocent, people who won't have any terrorist

implications afterwards, is it not necessary, even at the cost of a little risk to the possible tight security, for that to be disclosed, not in its operational details, but in the fact that, yes, we do have the bulk program that goes to X, Y, Z?

I'm wondering about your thoughts, Jane, Representative Harman. We've known each other a long time. And Stephanie, and anybody else that wants to.

MS. HARMAN: Well, first of all, Pat, Judge Wald, let me salute your decades of service to our country. You are certainly for women lawyers, the gold standard.

I was teaching a course at Harvard Law School about a week ago and a young woman, we were talking about this, she said, well, why should we trust NSA or any government agency to put the technical side of this together? Why should we, and then why do you trust them?

And I said, well, I start with this, there are bad guys out there trying to attack us, let's just talk about the terrorist piece of this,

and I want to know who they are and disrupt them before they do that. My assumption is most of them are in some foreign place and are not U.S. persons, but at any rate some of them could be.

So Congress tried to design a system, and I think did so pretty well, building in safeguards and court review and congressional oversight.

Now the system got a lot bigger since 9/11. Is it the right size? I don't know. I don't know if it's the right size. But I know I'm not the person, or if I were a member of Congress now, or even as, you know, the lowly, beat up President and CEO of the Wilson Center, just kidding, I'm not the right person to decide what the size is. I'm much better at designing the safeguards so that whatever size it is, there aren't abuses.

And I'm pretty persuaded we've got to have haystack. Again, I don't know what should be in it. If the question is should everything be in it? No, everything shouldn't be in it. The right

things should be in it. What are the right things? Somebody, again, with more technology knowledge should decide that, subject to review by the court, the FISA Court and maybe the Supreme Court ultimately, depending on how we structure this. And I am for Supreme Court review so there has to be standing and that has to be provided for somehow.

And the congress. Congress after all writes the laws. So I mean maybe that's an oversimplified version of it.

But back to that Harvard Law School student, I trust our government, subject to safeguards, to do the right thing to keep our country safe.

MS. WALD: Let me just clarify or just follow-up, okay. And that is, for instance in 215 one of the criticisms, even by some isolated members of Congress is we didn't even know that 215 was meant to encompass a bulk selection.

And so the question -- but then one answer is, ah, but some people in Congress did. I

don't know whether, you know, an inner group was told that this was a contemplated use. And so they knew it, etcetera, but maybe not until the thing was passed and you began to get --

I know later on re-authorization, memos were sent up from the Department of Justice explaining it, but apparently not everybody read them even though they could have read them, etcetera.

So I guess, yeah, I'm getting to this question. I only raised it because it is a philosophical question. I think of whether or not there are what some people call secret law that when it's being passed --

MS. HARMAN: Oh, what? I think I missed that.

MS. WALD: When it's being passed everybody doesn't debate in the public debate about what's really involved. And I understand the security risks. They can't obviously debate about a lot of security.

But the question of whether or not

there's some level at which they should know that something that you don't read the ordinary meaning into could encompass a very novel and extensive program to be in the debate.

MS. HARMAN: Well, I don't want to dominate this, and again, there are very competent people here.

But what did I know and when did I know it? As we were debating the PATRIOT Act a lot of it was controversial, and what the White House requested, the Bush White House requested, was cut back by Congress and several sections were sunseted, as you've just discussed. Whether sunset is the best mechanism, I don't know but it requires congressional review.

And 215 was one of those. And there were also controversies about the so-called library provision about whether grandma taking out a library book was subject to some kind of scrutiny.

But at any rate, this stuff was debated. It was re-debated. I don't know how

many members paid attention. I didn't view this as secret law. What precisely was the process to get the information I think was discoverable by members of Congress. I don't think it was hidden. And I think somebody not on the Intelligence or Judiciary Committee who really wanted to figure out how 215 works could have found out.

And again, in defense of Congress, a lot of stuff going on, people get distracted and this wasn't the public issue that it has become in recent time.

And that again is why there needs to be a robust Privacy and Civil Liberties Commission. This is the kind of issue this commission, had it been fully functioning in -- well, you weren't there when PATRIOT passed, but when PATRIOT was re-authorized, or the controversial provisions where you were there, you could have, if you had been there, focused attention, held hearings, done more to educate Congress and the public about what was at stake and influenced how the changes were made.

MR. MEDINE: Mr. Dempsey.

MS. WALD: Ms. Pell, I just wondered if she had anything to add to this quickly.

MS. PELL: So I'll try and narrow down a little bit to your specific question about an interpretation of a statute like 215 that authorizes a type of bulk collection that would not be readily apparent, even to a surveillance expert who read the statute.

Sort of putting on my former national security prosecutor hat, so much of intelligence oversight does, and it probably does have to happen behind closed doors.

That being said, I think we really need to push ourselves and the Executive Branch needs to be pushed, which we saw you doing this morning, to figure out how it is possible not to hide interpretations of a law that are perhaps idiosyncratic or novel.

And when I was thinking about this issue in preparing to testify today what bothered me in terms of dialogue and exchange between staff

members and their constituencies back in the 2009 timeframe was the inability to explain to those constituencies, nongovernmental stakeholders why, what would happen to language if it was amended in a certain way so that there wasn't really meaningful dialogue going on and you have the potential for constituencies who are very interested in these issues, lobbying or supporting language that wasn't necessarily in their interest.

And I think that's a bit of a broken process but a hard problem to cure because the Executive Branch is going to say there's going to be harm to national security if this legal interpretation tells people that we're collecting bulk, collecting metadata. And there's the rub, but I think we need to push.

MR. MEDINE: Okay. Mr. Dempsey.

MR. DEMPSEY: Thanks very much to all of the witnesses for coming today and trying to work these issues through with us.

Professor Kerr, do you have any

thoughts on this question of review or call it appeal?

You've written extensively on appeals in the criminal context of court orders for surveillance. In the FISA context here where there's some interest in creating some process for getting from the judge to the FISA Court of Review and at least making issues available to the Supreme Court, should they take them or not, what are your thoughts in terms of what would be the best way to structure that, or could that be structured that's at least as constitutional as the rest of FISA?

MR. KERR: It's a good question and a difficult one, in part because the constitutional questions hinge in large part on an understanding of the search warrant application process and the ex parte application process, which is almost entirely unexplored in the case law.

How should we think about an application for an ex parte court order? Is that like a case in which case it's an exercise of the

judicial power and we need to think of it in the traditional Article III ripeness, case in controversy way, or is that just some sort of an extra issue that goes before a judge that does not require the traditional Article III strictures to be followed.

We don't really know. So just thinking from a constitutional standpoint it's really difficult to know what the constitutional parameters are here in terms of what is permissible. There's just a tremendous gray area and I don't think there's going to be a lot of certainty one way or another.

I tend to be somewhat skeptical that the Supreme Court specifically could serve a useful role here, in part because everything the Supreme Court's doing is on the record, all in open court. It's difficult for a court of nine justices to have an oral argument where they're sort of, you know, bandying about hypotheticals on an area where there's a lot of classified issues. I just don't know how procedurally that might

work.

And in part my idea of the rule of lenity playing a significant role here as a way of avoiding this problem entirely. I think if you have the initial court decision --

MR. DEMPSEY: Although wouldn't your rule of lenity, that allow the government, the government would have the right to appeal still so actually you end up with a situation in which you in a way are perpetuating the current system where if your rule is applied, it's not like you immediately go back to Congress, you go to the FISCR and then you go to the Supreme Court.

MR. KERR: Well, I suppose you could have the process end at the FISCR rather than go to the Supreme Court. So you could have more equality there, where it's not that one side sort of can do more than the other side.

So, yes, I think you have the same problems with the Supreme Court trying to step in. And, of course, one reason we've never had this issue is the FISCR has only handled a few cases,

so the Supreme Court has never been in a position to review that.

But I'm more optimistic about the idea of having public disclosure of the FISC or FISCR interpretations of the law combined with some sort of sunset provision that forces this to be hashed out in Congress than I am having nine justices of the Supreme Court try to answer these questions, so.

MR. DEMPSEY: Professor Vladeck.

MR. VLADECK: I was going to say, I mean I think it's very important to not generalize. I mean I think, you know, I would draw a very sharp distinction between original FISA, in which I think there is the strongest analogy to the warrant context, and 215 and 702, which look nothing like warrants of any conventional understanding.

And in the context of 215 and 702, I think it is telling that Congress actually expressly provided for adverseness, right, that in both statutes the recipient of a 215 order, the

recipient of a 702 directive is given the, you know, express right to participate adversarial before the FISA Court, to appeal adverse decisions, including to the Supreme Court.

So, you know, I think the adverseness in the 215 and 702 context is actually, you know, satisfied until you get to the appeal question, which I was talking about before.

And in the warrant context, I guess I just, I'm less circumspect I think than Professor Kerr, only because I have a hard time seeing how the issuance of a search warrant is what the Supreme Court called an extrajudicial duty. It strikes me as a quintessentially judicial duty. I mean if the warrant clause of the Fourth Amendment requires a neutral magistrate and not just a neutral government officer of some vague description to sign off on a warrant, it seems to me that a warrant is part of the judicial process and that the adverseness is sort of justified, whether you buy it or not, by the fact that there's a subsequent proceeding in many cases that

will allow for --

MR. DEMPSEY: But could you even go so far as to say, I mean I'm not a constitutional law scholar, which will become apparent in a second. Is it possible to say that because of the Fourth Amendment that actually the case and controversy concepts are quite different in the warrant context?

Because we've said even though there's no party judges do this. This is appropriate for judges, even in the absence of a traditional case or controversy. And it's right there explicitly in the Constitution. No one's ever, FISCR, no one's ever really asked how do we get warrants before judges in the first place? Is maybe that's the answer, that it's right there in the Fourth Amendment?

MR. KERR: I don't think so. In part because the case law of the Supreme Court, at least in talking about the neutral magistrate requirement, has suggested that it doesn't, the neutral magistrate doesn't need to be a judge,

doesn't need to be a lawyer. It could actually be somebody who's a court clerk, could in theory, there's been some suggestion in the cases, be somebody inside the Executive Branch who could count as a judge for Fourth Amendment purposes issuing search warrants.

And this goes back to the difficulty of just trying to figure out how to categorize search warrant applications. Is it a traditional case? Is it something that's just another duty? The fact that you could have a non-judge issue a search warrant, to me takes it somewhat, at least from a constitutional standpoint, outside of the traditional sort of tripartite system and suggests it may not be a judicial function. But it's really a gray area.

MR. VLADECK: And it's usually appealable. I mean, I think, right, I mean at least in the federal context, right, if the government's, you know, there are extraordinary contexts where you can pursue, right, where you can seek to challenge the denial of a warrant

application.

MR. KERR: Actually traditionally the understanding has been no, that denials of applications are not appealable.

Now there's been some disagreement in the Title III setting. They've said that you can appeal it. That's another murky area, so it's just, again, just a gray zone.

MR. DEMPSEY: We've zoomed off into speculation.

MR. MEDINE: Ms. Cook.

MS. COLLINS COOK: I'd like to turn to a slightly different topic. Our statute requires us to consider the need for specific actions taken by the U.S. government to protect against terrorism and balance that need as against privacy and civil liberties concerns.

And one thing I think is very difficult to articulate is what makes a program effective. It can't simply be that a program is effective if it has thwarted five plots, if it's thwarted ten plots. And I would throw open to the panelists

what other types of metrics or concepts we should be looking to and to determining whether specific actions or programs are effective.

MS. HARMAN: Well, I don't think thwarting plots is the only metric. I don't know how you measure deterring plots.

But having that program, the right sized program, whatever that means, in effect and a lot of oversight of that program. Oversight also adds value. In addition to curbing abuses, it could help enhance the program in some way. It could point out some deficiencies and lead to amendments imagining the oversight is from Congress. So I think the metrics have to be more complex than this.

But I superimpose over this something I've said a couple of times. One is the changing technology, which is very hard for any of the, Congress, or the courts, or the Executive Branch to keep on top of, but which is something the bad guys plotting against us are keeping on top of. So it's an imperative to factor in changing

technology.

And the other part of it is, and again this is not directly to your question but it relates to your question, the need to be sure that the public supports what we're doing. And that again is the role you have.

I do not think that privacy and liberty, that privacy and security are a zero sum game. I think you either get more of both or less of both. I've said this repeatedly. You probably know that. And that's your job is to make sure that we get both.

And I think unless it's perceived that we're getting both there's going to be constant anger and second-guessing and drastic remedies proposed, which at some point might take hold and then we lose both.

MS. PELL: I'm not an intelligence analyst so I do hesitate to answer this question. But this morning I believe Raj De, the General Counsel from NSA, made a very interesting statement which I doubt the government will want

to elaborate on publicly, but that was that the Internet metadata bulk collection program was ended.

And I thought, well, and that had been public. But he seemed to indicate that it was ended because it wasn't seen as effective or providing a level of intelligence that the telephony metadata program was.

And so I was very curious, and again, I don't expect the government to talk about this in public, but what was that metric? Are they getting bigger pictures of terrorist groups or cells or activities because of what this telephony metadata program is doing versus what the Internet program was doing? Probably something you could inquire about behind closed doors.

MS. HARMAN: Could I just -- I don't think that's -- I thought the change in collection had to do with the FISA Court saying that the incidental collection that was going on was outside the scope of the law and that's why it was cut back and, in fact, what had been collected was

destroyed.

And I think it is very important that the law be as precise as possible. And I thought this was a great victory for the worried public about how oversight works. So I obviously didn't hear his testimony but I think that's what I imagine he was talking about.

MR. SPAFFORD: There are things that can be measured such as the cost of all of the storage necessary to hold this five year haystack that's being built-up, the cost of all the equipment, the personnel to do the collection, to do the maintenance, to do the searching.

There can be other kinds of costs that are calculated for protecting all of that. For instance, the NSA has spent a lot of money to build a very large data center in Utah. How much of that is for this purpose, they can perhaps answer in a classified setting. That's one thing that can be measured.

You can measure the number of successes. You can measure the number of

failures. And hopefully they can produce some measure of the number of false incidents that they have investigated and spent time and effort on, how much has gone into that.

From that, you can draw some calculation as to the cost per success and the cost per failure. Thereafter is a policy decision as to are we spending enough, are we spending too much for one of these incidents?

And that requires getting a full accounting of what things have been prevented. Apparently this collection is largely being or totally being directed towards anti-terror activities and the accounting that we've seen of the number of thwarted terrorist activities in the U.S. seems to be small relative to the investment involved. But that's a decision, you have to get the values and that's a policy decision that's well, certainly beyond my pay grade.

MR. VLADECK: I'd also just add very briefly, I mean you know, in the due process context the Supreme Court has said efficacy is not

just a function of the government's success rate, right. Efficacy is also a function of the cost to the government of providing additional process.

And I think it's impossible to divorce efficacy of particular surveillance programs from any attempt to actually figure out what the actual downside would be of adding additional safeguards, of adding additional protection. You know, because I think that's part -- I mean efficacy is not just sort of accuracy, it's also sort of a lack of false positives on the individual right side as well.

MR. MEDINE: Ms. Brand.

MS. BRAND: Thank you. I have a policy question that may have, may or may not have constitutional implications for Professors Kerr and Vladeck and anybody else who wants to weigh in.

With respect to the advocate, or amicus, or whatever you want to call it, in the FISC there is an appeal to that. There's something I like about it. But I think it's much,

much more complicated in its implementation than most of the bills or proposals recognized.

And as I've been thinking through the many, many levels of detail about how the thing would be implemented, to my mind a lot of sort of sub-questions turn on whether the advocate is someone with procedural rights in the process or someone who is called upon to give their view of a question of law for the court's benefit.

So Orin, do you have a view about whether the advocate, or Professor Vladeck about whether the advocate is somebody who should, as it would be in a true adversarial process, have a right to participate in every single aspect of the proceedings, to see every single piece of paper presented to the court?

You know, there was some discussion about the back and forth that goes on between the FISC's lawyers and the government. Should the advocate be privy to all of that communication like they would in a regular litigation context, or what?

And do you think whether the person has procedural rights or not dictates whether or not there's an Article III question here?

MR. KERR: So on the policy question it's not obvious to me that the details of procedural rights would make a major difference. And in part that depends on what the role is of this special advocate, when they're brought into the case.

I assume we're thinking of, you know, once in a while there would be a particularly significant issue on which we would want the special counsel or however you --

MS. BRAND: Let's just posit that it's the person is only involved in novel or significant cases.

MR. KERR: Right. As long as, I think it's important that they be given the full factual picture, so they would be given access to all of the underlying facts.

And in Marc Zwillinger's earlier testimony he talked about those challenges. But

once that, once all the facts are out there, at least for that counsel, it's not obvious to me that there is that much of a need for the procedural rights, as long as the issues are fully litigates.

That may just be a question though that Marc Zwillinger would be in a better position than I would to answer, but. And it's also not clear to me that giving procedural rights would make a difference from the Article III standpoint in creating adversariality.

MS. BRAND: Well say, for example, that the government did not give access to the special advocate on some piece of information, does that person have a right to it?

Does the person have a right to object if the court goes and talks to the government without including the person?

I mean those are the kind of rights that a party in litigation would have. But, you know, would all of those same rights apply here or would the person really just be called upon to

provide their expertise but not to necessarily participate in a truly adversarial way? That's sort of one of the basic questions.

MR. KERR: Yeah, I mean, I suppose there's questions of once you have the right to access the information do you have litigation over whether that right was fully complied with. Sort of thinking in the criminal setting, you know, like a Brady violation or something like that where the litigation over the major issue leads to litigation over all of the sub-issues.

And that I would think is just a practical question of how likely is that to be something that interferes with the core function of the special counsel.

So I don't have a strong sense of what the right answer is, just given how -- I think really it boils down to would the judges of the FISA Court take this as a priority and make sure that the special counsel is receiving the information, or is it something where that would not be a priority.

And I would imagine establishing in a statute that this is an important priority, that this is something that the counsel is entitled to might make sure that the FISA Court judges do that without a need to require litigations on all these sub-issues, but that's just, I think, a practical issue that may just depend on how it works.

MR. VLADECK: And I would just add briefly, I mean, I think the closest Supreme Court case I can think of on point is FEC vs Akins, right. In Akins you have the court saying that informational injury in that case suffered by voters, right, was sufficient to confer standing because they couldn't undertake their responsibility as voters without the information, right.

So it seems like a sort of similar kind of procedural injury without sort of a direct personal stake. I mean, I'm not the first to suggest the Supreme Court's stand on jurisprudence isn't exactly a straight line.

But I do think, I mean, I do think

there are procedural issues to work out, and much of them I think would depend on whether, whatever you call this position, is in fact invested with specific representational obligations viz-a-viz those whose communications are intercepted, in which case I think all of these issues become much more joined, right.

I think there would be no question in that case that they would have procedural rights, that they would be able to appeal, for example, denial by the FISA Court. Or if you don't, if they have abstract interests in the proceedings, I think that would get harder.

But I share Orin's view that I think most of the work would be done just by having them in the room. And then Congress could presumably create the disclosure obligations, not to the opposing counsel, but to the court. And then it would be the court's responsibility and the court's ability to hold the government to account if they failed to comply with those disclosure obligations.

MS. BRAND: Thank you.

MR. MEDINE: I wanted to return to Congresswoman Harman and Ms. Pell on the question of going forward.

The challenge that Congress has in enacting legislation that authorizes secret activities, I mean, it seems almost like a contradiction. How do we write laws that authorize programs that we don't want to talk about in public?

And assuming it's an entirely legitimate function and it's a democratic function and assuming the government will fully comply, but how do we write an authorization for a program that we can't talk about?

MS. HARMAN: Well, we can talk about part of the program. We can talk about the purpose of the program. We can talk about the framework for the program.

Certainly I recall very specifically in the debate on the FISA Amendments in 2008 that's what we did. Maybe a number of members of

Congress weren't paying much attention, but it was out there on the airwaves what the issues were. Certainly the telephone metadata program had been disclosed by the New York Times and then partially declassified by President Bush in late 2005, and there was conversation out there.

So Congress can do that. That it, that should happen. There should be public hearings, as there now are public hearings about competing versions of some potential fixes for the laws that we have.

Yes, a portion of this is classified. Exactly how it works is classified. Why do we want to tip our playbook to the bad guys? And I think that can be explained publicly too. I think if you poll people, and probably we have but I just can't remember what the polls showed, I think Americans want two conflicting things, but they're really not conflicting.

One, they want their privacy protected. Well, good luck with that. I mean the private sector knows more about Americans' privacy than

the public sector does.

But they also want to be secure and they want laws that will catch these bad guys and prevent or disrupt plans to hurt us.

So I think that debate about purposes and framework is properly in the public domain. It should be made clear in the public domain that some of the innards, you know, how the watch works will be kept classified because we don't want to tip our hand.

But again, if there's adequate safeguards and if there's transparency in disclosing, as has been proposed, how many searches have been made, how many Americans were involved, what were the outcomes in sort of a bulk way, not compromising individual privacy, I think people will be comforted or should be comforted.

And just one last point, if we don't do this, if we blow up the bulk collection program totally and we say we're going back to the law enforcement model and only after something happens are we going to go after folks, as soon as

something really bad happens, and oh, by the way it could happen even with this program, the pendulum is going to go the other way and we're going to start collecting and at our disadvantage at that point, all kinds of stuff, possibly without the safeguards that we could build in properly now.

MR. MEDINE: Ms. Pell, do you have any additional thoughts?

MS. PELL: One additional thought, and I'll borrow from criminal investigative authorities. In the ECPA context it took a long time I think to be able to have a good conversation about how to amend statutes to deal with location data.

And part of that challenge was there weren't a lot of opinions by courts at various levels discussing how the government sought, under what authorities the ability to collect location data.

Over time more of those opinions, most of them at the magistrate level, but nevertheless

with anylsis, came out. If in fact we're able to get to a place where, for example, there are FISA Court opinions that are declassified or summarized, we have the basis of a conversation, facts and legal analysis to have a dialogue that members can talk about without worry of disclosing classified information, where interested constituencies or stakeholders can bring concerns based on what they see in those opinions. It will take a little while but that's one way forward.

MR. MEDINE: Thank you.

Professor Vladeck, earlier you mentioned 702 and providers' ability to come in to court. One can read the statute to say the providers can only challenge the program but not the specific tasking orders.

Is that your view, and if so do you view that as a shortcoming of the statute?

MR. VLADECK: To be frank, I think because it's never been litigated, you know, I think it can be argued both ways. And I would have hoped that a provider would have tried to

litigate it in the other direction.

You know, we learned from the letter from Judge Walton to Chairman Leahy that in fact no recipient of a 702 Directive has ever challenged it.

You know, I do think any opportunity for more presentation of adversarial argument and briefing in the FISA Court, at least after the government has been able to obtain the authority ab initio is worth pursuing.

And I actually think we didn't hear anything to the contrary from the government witnesses this morning. You know, whether you would need that on top of a provision for some kind of special advocate, I think, is an interesting question because you'd have maybe potentially a redundancy problem. But in the absence of that, certainly, I think, you know, it would be a relatively easy sell to Congress to do that.

I think the harder sell is getting the recipients to actually use it. And I think that's

a question worth pursuing as well.

MR. MEDINE: All right, thanks.

We have eight or ten more minutes if people have a couple of more questions.

MS. WALD: Yeah.

MR. MEDINE: It looks like Judge Wald is ready and eager.

MS. WALD: Okay. My first question is for Professor Kerr. I wonder if you think, given the present status of 215 was originally not known to us. It was in operation for many years before it became publicized. Now there's a great deal, we know it's there and there's a lot of people going back and forth. There are several proposed reforms, in quotes, on the hill.

And the question is still there, at least one of the bills says stop the program, you know, the Leahy bill, move to a different way of doing it.

I'm wondering if you think your two precepts that you laid out earlier, namely sunset and a rule of lenity have any application, if so,

what to the present status and debate over what to do with 215 right now?

MR. KERR: Well, there is no rule of lenity right now so --

MS. WALD: No, I know that, but I mean there should be or there's some principle there that could be applied to what do we do with 215 right now, that we know about it.

MR. KERR: Yeah, and certainly my understanding is that Section 215 sunsets in 2015, I think. So that provision will be, you know, that will have to lead to a debate at some point over the next two years over whether this program is desirable or not. And the government's going to have to make its case.

You know, we could wish that it was something that happened in the next few months rather than two years from now, because the debate, of course, is current now and who knows what the picture will be then.

But so the sunset provision, I think, does play a very important role over the next two

years in figuring out, ultimately Congress answering this question of whether to approve the bulk collection program or not, and if not, what are the alternatives.

MS. WALD: Well, your original explanation of the rule of lenity was that if the FISC Court got something that appeared to be a novel interpretation or that appeared to be at the extreme edges of an interpretation they should tell the government to go to Congress and get a specific authorization. Does that have any application to the present situation?

MR. KERR: Yeah, well, if there had been a rule of lenity in place that the court had considered at the time I would think that the answer would be that they would not have approved the bulk collection program under Section 215.

I think they should not have approved it, at least based on the arguments that have been made so far, even without a rule of lenity, just considering it as a fifty-fifty question.

So we would not have been in the

situation that we're in with the FISA Court having already approved the program, sort of putting the difficult burden on those that are trying to amend the statute in the other direction, if there had been some sort of a rule of lenity in place.

MS. WALD: But as it comes up for re-authorization, which it does apart from the sunset every, I forgot what the period is, but do you think that's the point at which the rule of lenity might apply?

MR. KERR: So I'm thinking of, just to be clear, the rule of lenity being Congress instructing the FISA Court to interpret the Foreign Intelligence Surveillance Act in that way, sort of by default adopting a narrow interpretation of the statute rather than a broad interpretation.

MS. WALD: Yeah, but I thought you had suggested that when it came to FISC in the beginning, and I'm just saying would that have any application when you're having re-authorizations they would say this is sort of an extreme and

novel interpretation, go back, go to Congress and get a specific authorization.

MR. KERR: Yeah, so it certainly could enable the FISC to back off of an earlier interpretation if that's in place.

MS. WALD: I still have one second?

MR. MEDINE: Yes.

MS. WALD: One question, a quick one to Professor Vladeck.

I want to make sure, 702 is kind of a complicated program and if you can speak for yourself or for any of the NGOs that you may have had contact with, how would you characterize the main concern of outside groups about the way 702 operates? Because I think we're all agreed they had congressional authorization to begin with so it's not a 215.

MR. VLADECK: So I wouldn't dare speak for anybody other than myself, and even then --

MS. WALD: Okay, that's good enough. That's good enough.

MR. VLADECK: And that's subject to my

wife's overruling.

But I'll just say my biggest concern about Section 702 is the volume of communications of U.S. persons that are at least ostensibly available to be picked up, quote, incidentally, unquote, right, that 702 bars targeting but seems to contemplate, based upon my understanding of our technological capacities, the collection of data on a scale that makes the incidental acquisition of U.S. persons communications not just likely, but certain, and a very large number of those communications.

So my biggest concern is that this sort of intentional targeting requirement is a bit disingenuous.

MS. WALD: So how would you correct that?

MR. VLADECK: I mean, I think, there are a couple of possible ways to do it, but they all get to the same place.

One is to not allow the government to file for a directive if they have reason to

believe that a certain percentage of the intercepted communications will actually involve U.S. persons.

One is to not just require minimization requirements but actually to provide what the baseline minimization requirements are.

I mean think there are, you know, there are a number of different ways to attack that problem. I think the threshold issue is that it's just too likely that communications are being accidentally picked up or incidentally picked up, even when the government can't go after them specifically. And so I think there are any number of ways to scale that back.

MR. MEDINE: Mr. Dempsey, any final questions?

MR. DEMPSEY: If I could.

So Professor Kerr, did I hear you correctly to say that you do not think that Section 702 bears the weight that's been put upon it in terms of authorizing the bulk collection program? Is that what you were suggesting? Did I

catch that?

MR. KERR: No, I was referring to Section 215.

MR. DEMPSEY: 215, yeah 215. That's your view?

MR. KERR: I think the arguments that have been put forward and are found in Judge Eagan's opinion are not persuasive based on just an understanding of the current statute.

And I could say that when news was disclosed that the bulk collection program had been authorized under Section 215, I scratched my head and wondered how on earth did they get there based the on the statute that was written, which was sort of understood as a grand jury subpoena power, and on its face requires that the authority be limited by the grand jury subpoena powers, only a grand jury subpoena for documents, if it would have been issued, that is a requirement of the Section 215 authority.

And I imagine a prosecutor going to, trying to defend a grand jury subpoena for every

telephony metadata piece of information in the entire United States and not getting very far, to put it gently, before a judge in a case if there was a motion to quash file.

So I just don't think it's a persuasive interpretation of the statute, at least based on the arguments that have been put forward so far.

MR. DEMPSEY: Let me ask you a question about minimization. You've written about issues about minimization in the context of government acquisition of stored data in the ECPA context.

Do you have thoughts about minimization in the FISA context, focusing on content collection, particularly where in the context of where there have been reports, we alluded to them this morning, that the government collects stored data in transit as it's being moved from server to server.

What are your thoughts about sort of building a minimization structure that would be constitutionally sound for the FISA side addressing stored content, either stored content

that's actually in storage or stored content that's captured while it's in motion?

MR. KERR: Yeah, I think it's a difficult question in part because the meaning of minimization in the national security context, it strikes me as a different idea than the meaning of minimization in the criminal setting.

Where in the criminal setting you're really worried about making sure that information is not ever possessed by the government, never held, and certainly never disclosed in public.

And in the national security setting it's a totally different set of concerns. It's more than just is this going to be part of the database, how long is it going to be retained?

And we're more comfortable with the idea of it sort of being in a database somewhere subject to certain requirements as to when the database is going to be queried.

So one perhaps non-answer to the question is it strikes me as such a different question that it's not clear to me that the same

principles should apply.

And I would also point out that, for example, in Judge Bates's opinion on some of these issues in Section 702, his constitutional analysis was one possible way of approaching it, but it struck me that there's a lot of other ways that I can imagine other courts interpreting the same issues.

So there's a complicated issues raised by how broad is the surveillance, how broad do you take the foreign intelligence exception to the Fourth Amendment, assuming that that is an established exception, how broadly do you take that?

It's a lot of murky questions that would regulate that. And it's much more complicated, I think, than the similar criminal setting.

MR. DEMPSEY: Would you say it's possible we're bumping up against constitutional limits if there is such a different -- minimization in the criminal context is

constitutionally premised. I mean, it flows from the scope and particularity requirements. So if it's constitutionally-based, could we be running up against, without robust true minimization in the foreign intelligence field, could we be sort of running up against constitutional -- certainly constitutional issues, but I don't know if you would go so far as to say constitutional problems?

MR. KERR: Yes, absolutely. So there are a lot of different constitutional issues that are implicated here. There's, you know, obtaining contents of people's communications which is obviously going to raise Fourth Amendment questions.

There's the reasonableness requirement, how that would apply in the national security setting.

But there's not only the rights of those that are U.S. persons communicating with other U.S. persons, which has been the primary focus in the statute so far, but there also may be constitutional issues raised when a U.S. person in

communicating with a non-U.S. person. That half of the communication was presumably a constitutionally protected communication, and that has not yet received much attention at all.

So there are a lot of important issues that are complicated that are certainly in play.

MR. MEDINE: Any other final questions?

MR. DEMPSEY: Thank you. Thank you very much to all the witnesses.

MR. MEDINE: Thanks to the witnesses on this panel and all the witnesses today, as well as the board staff that made today's hearing possible.

The board encourages all interested parties to submit comments at regulations.gov relating to the topic of today's hearing.

A transcript of the hearing will be posted on our web site at pclob.gov.

And I now move that the hearing be adjourned. All in favor say aye.

(Aye)

MR. MEDINE: Unanimous motion, the

hearing is adjourned at 4:20 p.m. Thank you very much.

(Whereupon, the hearing was adjourned)

CERTIFICATION

I, LYNNE LIVINGSTON, A Notary Public of the State of Maryland, Baltimore County, do hereby certify that the within-named witnesses personally appeared at the time and place herein set out, and after having been first duly sworn, according to law, was examined by counsel.

I further certify that the examination was recorded by me stenographically; that this transcript is a true record of the testimony given by said witnesses.

I further certify that I am not of counsel to any of the parties, nor in any way interested in the outcome of this action.

As witness my hand and notarial seal this _____ day of _____, 2012.

_____

Lynne Livingston

Notary Public

My commission expires: December 10, 2014

S

U