THE ASPEN INSTITUTE

ASPEN SECURITY FORUM 2013

COUNTERTERRORISM, NATIONAL SECURITY, AND THE RULE OF LAW

Thursday, July 18, 2013

LIST OF PARTICIPANTS

MICHAEL ISIKOFF
Investigative Journalist, NBC News; Author

RAJ DE
General Counsel, National Security Agency

NEIL MacBRIDE
U.S. Attorney for the Eastern District of Virginia

JEH JOHNSON
Civil, Criminal Trial Lawyer
Former General Counsel of the Department of Defense

JANE HARMAN
Director, President and CEO, Woodrow Wilson Center
Former U.S. Representative

ANTHONY ROMERO
Executive Director, ACLU

* * * * *

MR ERVIN: All right, everybody, if we could start making our way back into the auditorium and get started. All right, everyone. Well, as I think most of you know -- I think nearly everybody here this morning was here last night, so you know that I'm Clark Ervin, the director of the Homeland Security Program here at the Aspen Institute and the director of the Aspen Security forum. Thank you very much for being here.

Just a couple of quick administrative housekeeping things that I want to say right now, because otherwise I will forget. Of course given the composition of our audience and speakers there is a lot of security consciousness, appropriately enough. So, the security detail has been picking up bags that have been unattended. So if you could please take your bag with you when you step out of the room and also if you could insert a business card right on the reverse, that will allow the security detail to return it to you afterwards.

Secondly, many, if not most, of our speakers and moderators are themselves authors, including Mike Isikoff, and so we are selling -- available in the back there thanks to Explorer bookstores here in Aspen are the books of many of the speakers and moderators. So I commend that to you -- to those of you who are interested.

With that, the title of this panel, as you see, is Counterterrorism, National Security, and the Rule of Law. And I think this one sentence that I drafted, the tension between what the law demands and what the national defense requires is in essence what this panel is all about. And to moderate this panel we are very pleased to have one of America's premier investigative journalists, Mike Isikoff.

Mike joined *NBC News* in 2010 as the national investigative correspondent, where, as we all know, he covered among other things the Boston Marathon Bombing and the Newtown Shooting Massacre. He appears regularly on *NBC News* and *MSNBC* programs. And he also the author, speaking of books, of two bestselling books, *New York*

Times bestselling books, *Hubris: The Inside Story of Spin, Scandal, and the Selling of the Iraq*, co-written with David Corn, and also *Uncovering Clinton: A Reporter's Story* on the Monica Lewinsky matter.

With that, Mike Isikoff.

MR. ISIKOFF: Thank you, Clark. And I want to thank you again for assembling such great panels. Every year you get newsmakers and future newsmakers to serve on these panels. Last year, for example, I served on a panel with Paula Broadwell. We went on. And while I don't expect any of our distinguished panelists to be making news quite like that this year, I think they all will be in the spotlight in some form or another.

Very quickly, to my left, Raj De, is the general counsel of the National Security Agency, which puts him right in the hot seat of all the issues that have been at front and center since the Snowden disclosures. Before that, Raj was the staff secretary for the president, President Obama. And my understanding is that gave him access to everything that went to the president's desk, which is pretty ominous when you think about it. And I first encountered Raj when he was a counsel for the 9/11 Commission, investigating what went -- what happened there.

To his left, Neil MacBride, is the U.S. Attorney for the Eastern District of Virginia and which has put him at the forefront of investigations on terrorism and quite a few media leak investigations, leak investigations involving the media, a subject I want to get to on this panel. Before that, he was a -- he served in the Justice Department in the DAAGs office and was a counsel to then Senator Joe Biden.

Jeh Johnson was the general counsel for the Defense Department until last year. And that gave him a legal overview about everything the U.S. Military and Defense Department was doing, a lot of which are the matters we are going to discuss here. Before that, he was the general counsel for the Air Force and an assistant U.S attorney, I understand hired in New York by Rudy Giuliani

back in the day that he was -- served on that.

Jane Harman needs no introduction to anybody here. She is now the executive director or director of the Woodrow Wilson Center. Served for how many terms in Congress?

MS. HARMAN: Nine.

MR. ISIKOFF: Nine terms in Congress. Was ranking member on the House Intelligence Committee for many years and then the Homeland Security Committee.

And Anthony Romero is the executive director of the ACLU and has been a consistent voice for civil liberties on all the issues we are going to talk about.

So let's start right off with the NSA program. I know some of it was covered in the previous panel. But I want to get into with Raj a little bit how it actually works. And I'm talking about the metadata program, which was probably the biggest disclosure by Edward Snowden, the fact that millions and millions of records of American's phone calls were being collected/stored -- I'll let people use the word they want -- by the NSA under a provision of the Patriot Act section 215.

Raj, walk us through exactly how this program works in practice, who has access to it, what those records can be used for?

MR. DE: Sure. Well, thanks, Mike. And thanks to the Aspen Institute and to Clark for pulling this all together. I'm especially appreciative because what I wanted to start out with is that I firmly believe that the U.S. government, the intelligence community, NSA in particular needs to be as transparent as possible, consistent with our need to protect national security. And obviously it's that last piece that's the rub and it makes it so difficult to talk about classified programs. But I would like to be as informative and helpful in this discussion as possible.

So with that -- and the reason I say that is my

job as the general counsel is to make sure our activities are lawful. But I think that the legitimacy of NSA's activities is just as important as the lawfulness of its activities.

So let me turn to the program you asked about, Mike. Even on the prior panel there was some conflation between the two major programs that were exposed. There are a number of issues that have been out in the press lately, but there's two major programs that were exposed. One -- and I will refer to them as the 702 program and 215 program.

Just to put it to the side, the 702 program is about the collection of content of communications, e-mails and phone calls, but it may only be targeted at non U.S. persons reasonably believed to be located aboard for valid foreign intelligence purpose. That is not what we are talking about with respect to the 215 program. To target the contents of the communications of a U.S. person under FISA anywhere in the world, whether it's in the U.S. or in the farthest flung corner of the world requires a showing of probable cause to a federal judge.

Turning to the 215 program, we call it the 215 program because it's conducted pursuant to section 215 of the Patriot Act. That provision allows the director of the FBI to apply to the FISC to obtain business records that maybe relevant to an authorized national security investigation. The FBI uses this provision for lots of different things. The only program that NSA uses it for in connection with the FBI is the business records metadata program that we are discussing today.

So what is that program all about? Before I get into the details, I think it would be helpful for everyone to understand what's the point of the program and why did it evolve. So in the aftermath of the 9/11 attacks one of the major issues that was exposed was a scene between our foreign intelligence collection and our domestic counterterrorism efforts. People in shorthand refer it to as the foreign-domestic divide.

The 9/11 Commission, for which I served as a

staff member, focused on this issue and the U.S. government over the past decade has taken a number of efforts to address this divide. Some of them institutional like setting up the National Counterterrorism Center and some of them utilizing certain programs like the telephone metadata program. The idea behind the program is to help connect when there is a foreign threat that may have a domestic nexus.

So how does it work? This program is about the bulk collection of telephone metadata, and what that means is things like numbers dialed, date and time of call and duration of call. It does not include any subscriber identifying information. There's no names associated with the numbers that are submitted to the FBI and to NSA. There is no locational data that is provided, whether that's GPS data or cell site locational information. And most importantly and probably most obvious there is no content.

I say that just so that everyone has a level set on the facts here as to how it's implemented. Pursuant to court order this data comes to NSA on a daily basis. It needs to be put pursuant to court order in a segregated database so it can't be comingled with other data at NSA. It has strict access and use controls that are imposed by the FISC. And so let me walk through some of those for you.

MR. ISIKOFF: Well, can I just --

MR. DE: Sure.

MR. ISIKOFF: I want to get back to this. But you talked about transparency here and understanding. And I want to -- and this is called the 215 program because of the provision in the Patriot Act. Jane, you were in the Congress when it passed the Patriot Act and 215 was definitely one of the issues that people were debating.

MS. HARMAN: Right.

MR. ISIKOFF: Did you understand when you voted for and supported the Patriot Act that it would be used

for the bulk collection of everybody's phone records in the United States?

MS. HARMAN: I understood that we needed to collect records in order to -- through all the means we've discussed in prior panels today in order to find those people in the United States or outside the United States who are linked to people in the United who are trying to harm us after 9/11.

And I voted for a provision that authorized people under strict supervision to figure out the best way to do that. I don't think as a sitting member of Congress and somebody -- I certainly know a lot about the intelligence business, but I'm not a trained intelligence analyst that I'm the best person to decide the parameters of the program.

But when I voted for it, one, Congress narrowed some of the initial proposals, and two, we sunsetted this thing. This thing has to be renewed every three years. And can I just add a little historical context, because I think it's important and I think a lot of people here do not understand?

MR. ISIKOFF: I just want to get you to -- did you understand that it would be used for the purpose that Raj is explaining here?

MS. HARMAN: I understood, well, business records could certainly be phone company records.

MR. ISIKOFF: All phone records in the United States.

MS. HARMAN: The -- exactly how it would be implemented -- I trusted people to implement it fairly because those in Congress who were on the relevant committees played -- certainly, I did -- a major role in overseeing what was happening. Now my knowledge -- I left the Intelligence Committee at the end of 2006, but then I headed the Intelligence Subcommittee of the Homeland Committee for another four years. So I stayed in this game. Did I oversee every single bit of it? No. Do I

think that maybe now, now that there is a much more public debate Congress should narrow some of these provisions? Yes.

Congress did narrow some of these provisions. There was the so-called library piece of 215 and there was a hue and cry about grandma going to the library and taking out a book and who could see that. And the reason the library provision was added is that there are often Internets at libraries. And in case anybody missed it, a lot of the way communication works between bad guys to bad guys is through the Internet and those sites maybe ought to be subject to the provisions of section 215.

So once it was narrowed to clarify that grandma was exempted, Congress did that in response to public outcry. People have known about this program. It was revealed in the *New York Times* in 2005. George Bush then finally partially declassified it. And I learned for the first time to my extreme dismay that in the first three and a half years of this program, which was developed by the Bush administration, the president had used his Article II authority -- he is the commander-in-chief -- to run the program rather than the provisions of law, FISA, which Congress enacted in 1978.

It's a fact that you ought to all know. FISA, the Foreign Intelligence Surveillance Act was passed by Congress in 1978 in response to the abuses of the Nixon administration and the recommendations of the Church Commission and it set up a careful system of a FISA Court, which I think you all understand how that works, composed of federal judges and intelligence committees on the Hill which were set up then to monitor these FISA applications. And it worked very well in my view through 2001.

And then the Bush administration yanked it and ran it in a different way. Congress after that, pulled it back under FISA. And I think -- I believe strongly that maybe the amount of metadata is excessive. I'm sure my buddy here Anthony thinks this. But -- and that ought to be debated and maybe the program should be narrowed. But there has been robust oversight over these years.

MR. ISIKOFF: Let me come back to Raj about the actual implementation, because I want to get back -- I want to be very clear on this. Who can access this data and for what specific purposes?

MR. DE: Certainly. And so I'll just add one fact, because facts are always good. We sent a -- I think this is in a letter that went to the Hill yesterday from the Justice Department. White papers classified were sent to Congress in December of 2009, in February of 2011 expressly describing the bulk collection use of this program. I can't speak to any individual member of Congress currently now as to their knowledge of the program, but I think that fact is an important one.

But getting to the use of the program; so in terms of access. Access is strictly controlled. And what does that mean? So in order to accrue the data one has to have a reasonable articulable suspicion that a particular selector, which is a phone number, has a tie to a specific terrorist group that is identified in a court order.

MR. ISIKOFF: So just a terrorist group. So if Neil MacBride calls you up tomorrow and says "I've got a foreign espionage investigation going on right now and I think my target might be about to leave the United States. I need to check out this phone number to see whether he is in communication with a co-conspirator, are you going to give him the information from that data collection"?

MR. DE: No. It will be illegal.

MR. ISIKOFF: You tell him, no, he can't have it?

MR. DE: That's right. Not only will would it --

MR. ISIKOFF: Neil, how do you get the information?

MR. MacBRIDE: Ask again. Please.

(Laughter)

MR. DE: We are friends, but not that close.

MR. ISIKOFF: How would you get the information for that investigation that you need?

MR. MacBRIDE: Well, the -- you know, let me back up from the specifics for a minute and quickly get to that, Mike. So in any investigation post 9/11 the FBI and the intelligence community and other government actors are working seamlessly in a way that really didn't happen before 9/11. I mean I -- when Jeh was general counsel we would have -- there were weeks when we had many occasions when we had to talk. We work closely with the Military, with Admiral McRaven community, with Admiral Gortney down in Norfolk, with various command forces. So there are conversations occurring across the defense intelligence, law enforcement communities in ways which are helpful in terms of permissible information sharing and dot connecting.

To your specific question, if there was a -- as I understand your hypothetical, if there was an operational terrorist within the United States, I would hope that we would already have their number and --

MR. ISIKOFF: Not a terrorist. I said a spy.

MR. MacBRIDE: A spy. Well, there certainly have been examples where there were individuals in this country. We have prosecuted a couple in my office just in the last year or so. One who was here as an unregistered agent of the ISI from Pakistani intelligence; another who was here at the behest of Syrian intelligence. And those individuals came to our attention, the investigations ensued and we were able to obtain the information we needed.

MR. ISIKOFF: No, but I'm asking a specific question about how you get records of phone numbers on ongoing investigations that have real-time consequences. It could be a spy investigation. It could be a drug cartel that's importing guns onto the streets of Alexandria and were used in five murders in the last

several months. You need this information right away and you want to know who is making phone calls to this -- who is making these phone calls. How do you get the information?

MR. MacBRIDE: Well, it's -- I think --

MR. ISIKOFF: You can get it, can't you?

MR. MacBRIDE: Yeah, and we do get it. And --

MR. ISIKOFF: And by a subpoena.

MR. MacBRIDE: Sure. By a subpoena, from an informant, from any number of ways. And so that in garden-variety criminal investigations, our ability to identify where an alleged bad guy lives or their phone number or their e-mail address our ability to find it is not all that difficult. Before we can --

MR. ISIKOFF: Not all that difficult and not all that time consuming. You can get it pretty quickly if you need it for an ongoing investigation, operational -- somebody is about to leave the country, you need that phone number in order to get a search warrant, you can get it pretty quickly, can't you?

MR. MacBRIDE: Well, it would depend on the particular case. But in contrast to what Raj is describing, which is sort of, you know, macro issues and bulk collection, your example I think contemplates a known individual who has been under the scrutiny or the view of law enforcement or other agencies. And so at the micro level it has not proved to be a difficult thing in our investigations.

MR. ISIKOFF: So I guess the question, Raj, is since Neil can get the information he needs pretty quickly for a lot of really serious investigations that have operational components, why can't you use the same method for the terrorism investigations that you are collecting this data for?

MR. DE: So I think the question -- the bigger

picture is, why can't the data just stay with the providers and then on a one-off basis go to them, right? That's --

MR. ISIKOFF: Which is what happens when Neil needs them for his investigations.

MR. DE: So just as a -- using a hypothetical example I think will be helpful, instructive for me anyway, is this came about in part after the 9/11 attacks. We realized that one of the operatives who had been living in the U.S. for some time in San Diego it turns out after the fact we learned had been receiving calls from a known Al-Qaeda safe house in Sana'a, Yemen.

So that's a -- I think that's a good example to use here. So we know there is a Yemini number, for example, that is a bad number, has a reasonable suspicion that it is tied to a terrorist organization. If we wanted to in short order try to figure out where that number may be connected to other numbers in the U.S. because we may have intercepted under another program the content of that communication to or from that number, the way that would play out in practice today if we went with the traditional law enforcement model, would be to need to go to multiple providers to ask them to search what number that number had been in contact with.

So as opposed to a subscriber of one of those companies, this would be a situation where they don't have the records handy for a Yemini phone number. They would have to do a search against their records against that number. So it's different than the hypothetical you posited earlier. So there is operational consequences there.

Two, in order to do the sort of analytics that need to happen on that data, the data needs to be aggregated to most effectively do that in short time. And so with three different providers that would also be additional step of bringing the data back, putting it together and trying to analyze it in short order.

And the third point I would make is today there

is no legal obligation for any of these companies to hold on to their data. They do it for their own commercial purposes. That's why it's called the business records exception. So tomorrow we could turnaround and any of these companies could decide that in their business purposes they don't want to hold on to these records. And so we could be faced with a situation which would equally impact the types of investigations Neil deals with, where we wouldn't have the data readily available. So those are some of the things we would have to think through if we went to an alternative model.

MR. ISIKOFF: Anthony, I think -- what I was getting at is probably what the ACLU has been saying, there ought to be specific targeted requests for this information. Raj has just said, "Well, that would create all sorts of problems. We don't know how long the phone companies would hold it for." Does he have a point?

MR. ROMERO: No.

(Laughter)

MR. ROMERO: I mean it's great to be back at Aspen, I should say that. I was last here debating Alberto Gonzales and John Yoo. And now I'm debating friends who serve in the Obama administration or who have served, and so much has changed and so much has not changed.

And to be clear to Raj's point, the program whether it's legitimate in the public eye or legal, the answer to it is illegitimate and illegal in our minds, both section 215 and section 702. Let's break it down.

The 215 standard -- it's really important to read the words of the law, "a statement of facts showing that there are reasonable grounds to believe that the tangible things" -- any tangible things that they conceive -- " that are sought are relevant to a foreign intelligence, international terrorism or espionage investigation" -- "relevant."

Now, it defies the knowledge or the

understanding of the word relevant when you are collecting every single phone call, metadata -- we will get into metadata. How is that limited to relevance when you are saying we got all the phone numbers that are made to and from American citizens? I don't think of the word relevant that way. My training at Stanford Law School had me think that the training of relevance was a bit more circumspect than everything, right.

Metadata, they say metadata is not content. Well, you know what? Metadata can give a lot of content. How long I stay on a phone call. How often I call my mother as she struggles with breast cancer. How often I struggle with my office. Who I call in the government. Whose private cell phones I happen to have, who I don't call at the office because we don't a log of my phone call from me to "blank" official in Justice Department. But I have a private cell phone, because we want to keep that somewhat between us, right?

That metadata when compiled in complete information can give you a very full picture of what my day is like, right? So I think that the Fourth Amendment does cover the protection of my metadata.

Now, let's also talk about section 702, right. Phone calls from overseas, from foreigners that don't have the same kind of standards that we have on the 215 program. Well, foreigners call Americans. Let me give you phone numbers that I have in my rolodex in my Blackberry over there, where they have my phone number and I have their phone number and I have called them in my 13 years as director of the ACLU.

I have direct phone numbers, cell phone numbers for Yasser Hamdi -- you might remember him. He was the subject of the Supreme Court case. David Hicks, in the Guantanamo. Mr. Al-Awlaki's father; Anwar Al-Awlaki who was killed by the American government by drones, including his 16-year-old son also an American citizen killed by drones. Let's get Jeh into this game. I happen to have the phone number of Mr. Al-Awlaki's father in Yemen. I have Moazzam Begg's cell phone number, who was also at Guantanamo.

I have the phone numbers for Khalid Sheikh Mohammed's wife and brother-in-law in Iran. We represent Mr. Mohammed in the 9/11 Commissions, the 9/11 trials at Guantanamo. We have contact with his wife and his brother-in-law. And Mr. Al-Masri, who was also held, rendered and tortured.

Those are all individuals that I have legitimate phone numbers. These are all cases in which I've been involved with. I call them; they call me. As an American citizen I have a right, an expectation that my communications with individuals for which I'm doing my zealous work to defend their rights ought not to be intercepted under any program.

Now, if you were to tell me, Raj, that my communications had not been caught up in the NSA surveillance program and that none of these phone numbers I have made or phone calls I've made and they've called me are not part of your vast database, I wouldn't believe you, right. Because I actually think that these are exactly the types of people that you are targeting. I have a legitimate right to interact with these individuals and I have a right, an expectation of privacy that my communications will not be intercepted by the government.

MR. ISIKOFF: Jeh, why can't Anthony communicate with his clients without you collecting -- you in your former job and Raj in his current job collecting the records of those phone calls?

MR. JOHNSON: I would say that Anthony absolutely can communicate with his clients. He has a right to do that. His clients have a right to do that. Look, I think -- I disagree with Anthony to say the program is illegal. In his opinion the program is illegal. In the opinion of all three branches of government the program is not illegal; you know, the people's representatives in Congress, the court, the FISA Court and the executive branch all believe this program is legal.

And it's important I think to put in perspective

two things. First, as was alluded to in a question to the prior panel, there is no expectation of privacy in metadata by itself. The fact that 212-373-3093 makes a phone call to some number in the 202 area code is known to the telephone company and lots of other people. There is no expectation in the fact of that call and the duration of that call itself. Clearly, there is an expectation of privacy in content, for which you need a warrant.

Second, the reality is that the NSA's surveillance program is probably the most regulated national security program we have. The two programs that have been declassified that we are talking about are regulated by the executive branch. Congressional oversight has been aware of how the executive branch has interpreted section 215 and the judicial branch, because it has approved it. That branch -- that aspect of the judicial branch that has been designated by Congress to hear these applications has approved of the manner in which this program is being implemented.

So there is the equilibrium. And if our national political leadership decides they want to change the equilibrium, that is their prerogative and their responsibility.

MR. ISIKOFF: I want to move the discussion along because we have got a lot of other subjects to go to. But I have two more quick questions for Raj on this subject. Number one, the Verizon order that was disclosed by Snowden that sort of kicked off this whole controversy is due to expire tomorrow. Is the NSA seeking a renewal?

MR. DE: I have nothing to say today about that.

MR. ISIKOFF: Will you have something to say tomorrow?

MR. DE: I think there will be something to say tomorrow.

MR. ISIKOFF: Will it be modified in any way?

(Laughter)

MR. DE: Tomorrow. Nothing further I can say on that at the moment. Nice try, though.

MR. ISIKOFF: Okay. And I have one more -- but that's -- we will back to you tomorrow in one form or another.

MR. DE: I am impressed with Anthony's rolodex.

MS. HARMAN: Could I say something in defense of Anthony?

MR. ISIKOFF: Yeah.

MS. HARMAN: I want him to continue to love me. I think there --

MR. ROMERO: I adore you.

MS. HARMAN: -- should be an expectation of protection of lawyer-client communications and that has always been the tradition and it is generally respected. There was a 1979 Supreme Court case -- it was referenced this morning -- that upheld a Maryland Supreme Court decision that there is no constitutionally protected expectation that phone numbers called will not be disclosed. That's the basis on which we should begin to talk about this.

But coming back to Congress, Congress can narrow or the -- whatever is the standard to go before the FISA Court to get an individualized warrant. That's what the Fourth Amendment requires. And there was something called the Safe Act, which was proposed in 2005, which I'm sure will be revisited. And I just put it out here since we are reading stuff. It would have provided -- it would have required that the court deal with -- that the case deal with specific and articulable facts, creating a reasonable suspicion that a particular person is an agent of a foreign power before the phone records could be seized or monitored.

And that's a tighter standard and I think

Congress will be looking at in some near lifetime tightening the standard. And I think that's totally proper and I think we need a national debate about this; and we are having one right now.

MR. ISIKOFF: Regardless of --

MR. ROMERO: Let's impact something for a moment; the'79 case that was referenced this morning and just now.

MR. ISIKOFF: Really quickly, Anthony.

MR. ROMERO: 1979. I mean how many years has it been, right? Think about it. It was a very primitive pen register. It tracked only the numbers being dialed, but it didn't indicate which calls were completed, let alone the duration of the calls. Our capacity to connect the dots on metadata is vastly different than what we saw in 1979. Let's let the court decide whether or not 1979 that decision is relevant or upholds this metadata program. That's exactly what the purpose of our lawsuit will be that we filed.

Now, let's also impact the three branches of government. Excuse me. No, I love Jane, but you got to forgive me; (inaudible) all the three branches of the government. FISA Court, come on? Twelve judges, eleven of them Republicans, right? No adversarial. All appointed by Chief Justice Roberts. There is no one representing the privacy interests of the people. It's only the government who represents in the FISA Court. Thirty-five years of jurisprudence; three opinions published.

MR. ISIKOFF: All right, Anthony, you have baited me here. Is there any form of surveillance that the NSA can conduct that you would approve of?

MR. ROMERO: Sure. Absolutely.

MR. ISIKOFF: What?

MR. ROMERO: It has got to be focused on the

subject of the surveillance. I mean the probable cause.

MR. ISIKOFF: Who would approve it?

MR. ROMERO: I mean we can talk about that, whether it's a FISA Court --

MR. ISIKOFF: Well, who should -- in secret.

MR. ROMERO: Yeah, a revamped FISA Court.

MR. ISIKOFF: You accept that it has to be in secret?

MR. ROMERO: A revamped FISA Court, totally fine. There is no -- even the chief justice of the FISA Court says, "We need an adversarial process. That's what our court system should be like. There is no adversarial process. We need more transparency."

MR. ISIKOFF: Who is the adversary when the government goes in and says --

MR. ROMERO: You can appoint one.

MR. ISIKOFF: -- we've got a phone number here that has been called by an Al-Qaeda operative in Pakistan.

MR. ROMERO: You can --

MR. ISIKOFF: We need to see who that person is right away." Who is the adversary if it goes before the court to argue no, no, you don't.

MR. ROMERO: You could easily appoint an ombudsman whose job it is is to preserve and present the privacy rights of the individuals. It should not be the ACLU. It could be a government official in charge with that.

MR. ISIKOFF: Last question for now on this subject. We can debate whether the privacy rights metadata are covered by the constitution or not, but Americans do have an expectation that their public

officials are going to tell them the truth.

MR. ROMERO: The truth.

MR. ISIKOFF: So when in March Senator Wyden asked the Director of National Intelligence, James Clapper, if you could give me a yes or no answer to the question does the NSA collect any type of data at all on millions or hundreds of millions of Americans and he answered, "No, sir," did anybody from the NSA come into your office and say, "We have a problem here. The director has just misled the Congress and the public about what we are doing"?

MR. DE: I think -- let me make a couple of points. But I don't --

MR. ISIKOFF: What's the answer to that question?

MR. DE: Yup, I'll give it to you.

MR. JOHNSON: I think he has a right or privilege to attorney-client communications --

(Laughter)

MR. DE: I think -- the first point is just the facts, because I think facts are important in the questions as well as the answers.

MR. MacBRIDE: I agree with Jeh.

MR. DE: He is the Director of National Intelligence, not NSA. So he is not my client and I wouldn't advise him.

MR. ISIKOFF: But he was talking about what your agency was doing -- is doing.

MR. DE: I think (inaudible) public record, Director Clapper has sent on record a letter to the Senate Intelligence Committee explaining what happened in that moment.

MR. ISIKOFF: After the disclosures by Snowden.

MR. DE: I think -- what I would say and I don't want to speak to -- I don't know and don't want to speak to what Director Clapper said. But I would say as a general matter, when long time honorable public servants make a mistake, sometimes it's a mistake. However, the premise of your question is true. The public expects honest answers. Both of those can be true.

MS. HARMAN: Yeah. I would just add, I have the highest regard for Jim Clapper. I wish we could roll back the video tape and his answer had been "I cannot answer that question in a public setting. If we move into a classified setting, I will answer that question completely."

MR. ISIKOFF: Let's move on, because there are other subjects that we need to cover here. And Neil, you've been very involved in leak investigations by this administration. Your office has overseen quite a few. In fact, as been widely reported, this Justice Department has brought more leak prosecutions than any other in American history and the record shows we have very little to show for it at this moment. You've got one I think success.

Last week when the Justice Department -- Attorney General Holder issued his new guidelines for the press and how it will handle leak investigations involving the press, and saying that many of the -- a few of the tactics and techniques that the Justice Department has used, the secret subpoena of the AP phone records, the use of a search warrant to get private e-mails from a reporter under the pretext that he was an aider or abettor of violations of the Espionage Act will not be used anymore.

And in the last paragraph of their new statement they said -- of their new policy they say, "Cases involving the unauthorized disclosure of classified information are inherently difficult to investigate and prosecute. They are time and resource intensive and they require a careful narrowing of the universe of individuals privy to the information and require proof of harm that

may itself result in further harmful disclosures."

It sounds like a recognition that much of what this Justice Department has been doing including your office has been misplaced.

MR. MacBRIDE: Not surprisingly, I didn't quite read it that way, Mike.

(Laughter)

MR. MacBRIDE: But happy to answer those questions. Let me step back for just a second. It's true my office, the Eastern District of Virginia has been involved in several leak investigations and prosecutions. The context for that is that -- for those of you perhaps from the West Coast who happily do not have to travel east to the nation's capital. The part of Virginia that my district covers is home to the largest footprint of the U.S. government in the country. We are home to the Pentagon, to the CIA, to much of the intelligence community.

We have the world's largest naval base down in Norfolk. We have hundreds and hundreds of federal government installations scattered across our district. We have thousands of acres of federal land. And that partially means that we have a bit of a national security bullseye on our back. It also means that when there are issues involving the unauthorized disclosure of national defense information, which I'll talk about in a second, which is a subset of a much broader group of classified information. That, my district is just sort of the obvious place to bring the investigation. So just a bit of context as to why we are frequently involved in these cases, number one.

Number two, I think a little context in terms of numbers is helpful. The numbers are not as large as some of the numbers thrown out in terms of various collection systems. But in the average year the Justice Department brings between 50,000 and 75,000 investigations, opens 50,000 to 75,000 investigations. So in the last five years the Justice Department between the criminal division

and the 93 U.S. attorneys offices have -- you know, conservatively we've probably opened 250,000-300,000 investigations. Against that backdrop, there have been a half dozen or so investigations of the -- into allegations of the unauthorized disclosure of national defense information.

So I think it's helpful just to sort of put in context that there is a whole lot else we have that occupies our time and attention in our day jobs beyond this, you know, small but important aspect of enforcing the law. And just a last sort of data point before getting to Mike's specific question. So there has been much that has been written and talked about about the over classification of information in the last decade since 9/11, and I think there's really no daylight between people of all -- you know, all sides and viewpoints that the government classifies too much information. I believe the president has called for lower amounts of classification.

That said, when you are talking about leak investigations and prosecutions -- we use that term really as a term of art, because it's a common misperception that there is a federal statute somewhere that criminalizes the release of classified information. That is not the case. There is lots of information that's classified that may even be sensitive that you read about in the papers every day. And it may be an annoyance to government officials. It may cause, you know, some level of alarm and concern by various constituents, but that doesn't mean that it is a violation of federal law.

The handful of cases that my office is focused on are a very small subset of the overall universe of classified information. And as the folks here on the panel know that, it's referred to as NDI, national defense information. And so in order to bring a criminal case for the unauthorized release of NDI, it's a fairly high threshold. You need to show that this is information that is critical to the national defense, that the release of which can benefit a foreign government and/or hurt the United States. And so --

MR. ISIKOFF: Have you gone overboard, Neil?

MR. MacBRIDE: No, I don't believe we have. I think that the attorney general and others have talked about the reason for the increase in leak investigations, again, against a background that we are talking about, a handful of investigations out of hundreds of thousands that have been done in the last several years.

But I think the reasons that have been given are a couple. Number one, referrals from the intelligence community, from the CIA and others, has increased in recent years. That I think is a reflection of a couple of things, and I think there is general agreement about this. Number one, a whole lot more people have access to classified information today than they did before 9/11, number one.

Number two, there has been -- and this has been discussed on the Hill and various public fora, and I'm not tech savvy enough to use technical terms here, but, you know, essentially internal IT systems within the government and the private sector make it somewhat easier to be able to, you know, determine who the source of a particular leak was. That's more -- that is increasingly true today in a way that it wasn't 10-15 years ago. And so the number of referrals to us from the intelligence community has gone up.

MR. ISIKOFF: Neil, and one of those cases is Jeffery Sterling. You've compelled -- you've sought to compel the testimony of James Risen of the *New York Times*. He has said absolutely under no circumstances will he testify and he will go to jail if he has to. You've appealed to the Fourth Circuit arguing there is no reporter's privilege, period, in criminal cases, which does seem to be somewhat at variance with the attorney general's comments last week about the strong support for Media Shield Law. If you prevail, are you prepared to put a *New York Times* reporter, James Risen, in jail for refusing to testify?

MR. MacBRIDE: So let me say a couple of things about that.

(Laughter)

MR. MacBRIDE: First of all, the administration including the attorney general strongly supports and has for several years a Media Shield bill, which has been pending in Congress.

MR. ISIKOFF: You've got a pending argument there is no reporter's privilege. You've argued that to the Fourth Circuit.

MR. MacBRIDE: Right. And if you will allow me; my understanding of the reporter's privilege -- Reporter Shield bill, which I'm told was actually reintroduced yesterday by Senators Schumer and Graham and a bipartisan bill has been introduced in the Senate, which would codify the new DOJ media regs, which I also will get to in a second. But my understanding of that bill -- and I haven't, you know, read it carefully.

MR. ISIKOFF: I'm not asking about the bill. I'm asking about the case that your office is bringing.

MR. MacBRIDE: Right. But I think I heard in your question is there an inconsistency that you support the Media Shield bill on the one hand and say that it's a matter of law that there is not an absolute right for any person, you know, reporter, non reporter to not provide evidence of a crime.

My understanding of that Shield bill is that it sets up a test, where a federal judge based on the type of case, is it a garden-variety criminal case, is it a sensitive national security case, is it a terrorism case, would make certain balancing tests. And the bill does not say that a reporter has no obligation to ever go into court and testify, is my understanding of the bill, that a test would be applied and is a very fact specific determination.

But the media regs that you mentioned, Michael, I think are really important and they are significant and they certainly are going to change the way we do business to some extent in these investigations. Those media regs

were a reflection by the attorney general that, you know, often times in Washington and elsewhere policy debates are really -- is much about means as ends. So many times actually there are shared ends if both sides agree to, but we may have friendly disagreements about the means to achieve those shared ends.

And so what the AG did over the last month or so was to have six or seven personal meetings and sit down with 30 or 40 members of the fourth estate to sort of roll up his sleeves and hear, "Okay, what is it that is giving you heartburn about the way we are doing business. What are the means that we have used historically that perhaps should be revised?" And there are a couple of them which are significant. And my -- I have not sort of canvassed the editorial pages of the nation's papers and magazines, but the response seems to have been more generally positive to these new regs. I don't know your own view, Mike.

But here are two real big changes in terms of how we will do business. Number one, if the government -- well, let me back up. It has always been the case that seeking records or testimony or information from a reporter is an absolute last resort. There has to be a compelling need for the investigation. If I can get the information through another source, I'm not allowed to go ask the reporter a question or to ask them to testify in the grand jury.

So there is an exhaustion requirement, which has been strengthened and it's more robust. The attorney general, you know, himself or herself needs to now sign off. It's not delegated down to somebody in the Department. But critically, the Department now if we wish to issue a subpoena, you know, for *CNN* -- you know, for a tape of a demonstration outside an embassy -- and that is the usual situation in which we are subpoenaing records --

MR. ISIKOFF: Can I bring you back to Jeffery Sterling and James Risen? Do you really want to win this case and be faced with the choice of whether you are going to put the reporter in the jail?

MR. MacBRIDE: So the case is pending before the Fourth Circuit --

MR. ISIKOFF: And if you win?

MR. MacBRIDE: -- and as a result it's a hypothetical. I need to wait --

MR. ISIKOFF: Do you want to win?

MR. MacBRIDE: -- to see what happens.

MR. ISIKOFF: All right. Let's -- we got -- we do have -- Anthony, quickly if you have one other point.

MR. MacBRIDE: Can I -- I'm sorry, can I just finish before Antony's point?

MR. ISIKOFF: Yeah. Okay.

MR. MacBRIDE: So here are the two big changes. Number one, if we are going to subpoena a reporter we now need to give advance notice to that reporter and the reporter -- whether it's to the reporter directly -- well, obviously you would have receipt of the subpoena. But if we are going to a third-party, we now need to tell the reporter and then the reporter has the ability to object, to come into court to litigate it if they want and a judge will work it out if there is a dispute, number one. Number two -- and this I think is referenced to --

MR. ISIKOFF: The search warrant.

MR. MacBRIDE: -- the search warrant case.

MR. ISIKOFF: The search warrant to Google.

MR. MacBRIDE: So it's -- the new reg says that unless a reporter is him or herself the target of the investigation that there will not be a search warrant sought for e-mails, phone records, et cetera. And the AG has made it very clear, the regs make it very clear that reporters are not going to be prosecuted ever for simply going about their very important business of reporting on

the news.

MS. HARMAN: So can we each speak for a second?

MR. ISIKOFF: Very quickly --

MS. HARMAN: Okay, all right.

MR. ISIKOFF: -- because we have got another big subject to come.

MS. HARMAN: But I mean --

MR. ISIKOFF: Yeah.

MS. HARMAN: I served --

MR. ROMERO: Which one?

MS. HARMAN: -- in Congress -- oh, do you want to go first?

MR. ROMERO: No, no, I just wondered what's --

MS. HARMAN: No, Anthony, will rebut what I'm about to say.

MR. ROMERO: No --

MS. HARMAN: And focused --

MR. ROMERO: -- I don't do that.

MS. HARMAN: -- on a lot of this for 17 years and I still focus on it. I think the press is by and large very responsible. I personally participated in a few phone calls to heads of offices saying, "Please don't publish information about the x, y, z program now. It would be harmful."

Let's understand what harmful means. Sources and methods when revealed can result in people dying. They can also result in our capability going forward against a target, let's say, the Iranian nuclear program,

being compromised. It is not okay, certainly not okay with me to have published information which reveals sources and methods. And I'm extremely worried about some of the Snowden stuff that hasn't come out yet, which may show some sources that we have in our current efforts to keep America safe and those sources could be killed.

So let's understand that. That does not mean a reporter X should go to jail, Michael. But the context is there is a responsible press by and large. I certainly respect that. I strongly support and did support the Press Shield Law. We have to find a better way to stop leaks of material that compromise our sources and methods.

MR. ISIKOFF: Okay. I want to move on to another subject here that's very big and important, and that's drone strikes and the future of our war on terror. Now, it has all been predicated on the authorization to use military force past after 9/11, which identified our enemy as Al-Qaeda, the Taliban -- the Taliban, Al-Qaeda and associated forces.

Jeh, you gave a major speech in Oxford last year looking towards the future, what the future is going to look like. But I am hung up still on the phrase "associated forces." Who are the associated forces of Al-Qaeda, who are our enemy right now?

MR. JOHNSON: Well, you are correct that for the last four years while I was in office the interpretation of the AUMF that we adopted in the executive branch referred to Al-Qaeda, the Taliban and associated forces. That was an interpretation by the executive branch that was endorsed by the courts in the habeas litigation brought by Guantanamo detainees specifically to include the concept of an associated force.

And it was also an interpretation of the AUMF that the Congress last year in section 1021 of the NDAA embraced. There were some in Congress who believed, "You know, we shouldn't just rely on the lawyer's interpretation of our prior statutory authority. Let's codify it expressly." Which they did in section 1021, which engendered some ligation. The Second Circuit

yesterday vacated the injunction in that case.

When I was in office -- and I want to point out that when we conducted military operations pursuant to that authority in places outside of Iraq and Afghanistan like Yemen, the Horn of Africa, every strike was briefed to Congress after the strike. And I would talk regularly to the lawyers on the Armed Services Committee and the members about how we were construing that authority so that they understood how their statutory authorization was being applied.

And so during the time I was in office that authority generally worked against core Al-Qaeda, you know, Osama bin Laden being the most prominent examples, other members of core Al-Qaeda, Al-Qaeda in the Arabian Peninsula and Al-Qaeda affiliated elements of Al-Shabaab.

MR. ISIKOFF: So three. There were three associated forces when you were in office.

MR. JOHNSON: Well, I don't know that I would -- those were the three that I had the occasion to evaluate most often. There were other instances where I would conduct a legal evaluation of certain other organizations, where we didn't go forward with a specific operation, but those were the three most prominent examples that were public that we regularly briefed to Congress.

Now, you referred to my Oxford speech. I think that we are at an inflection point, as one journalist put it, where we should no longer consider ourselves in a traditional armed conflict against Al-Qaeda and affiliated groups. And I think Benghazi is a prominent example of what I'm talking about, because you can't label the Benghazi attack as something conducted by Al-Qaeda and associated forces. It was more of a mixed bag.

And so in this period where I think we are headed in a new direction we need to evaluate in Congress what new authorities our counterterrorism professionals might need, and we are not just talking about drone strikes. We are talking about ability to conduct national security interrogations, pre-Miranda and other types of

things that domestic law enforcement, that the intelligence community should have to go forward with the future threats.

MS. HARMAN: Can I add something to this?

MR. ISIKOFF: Yeah, quick.

MS. HARMAN: I just want to give a shot out to Jeh, who has been fearless. This is not -- while he was in government and since in talking about this. Harold Koh is another example of somebody who has been fearless. And it's not easy. At the Wilson Center last week we had one of our national conversations about the AUMF, whether it should be mended or ended. And Bob Corker, a Republican from Tennessee, Senator, the ranking member on the Senate Foreign Relations Committee came down to the Wilson Center and said "Congress is being irresponsible." This statute which I sitting here voted for. Every member of Congress but one voted for it in 2001, was never anticipated to be in effect 12 years later and be the basis for all of our tactics against bad guys forever and ever.

And this is a debate Congress should have. And if Congress isn't having it, it's a debate the larger society should have, about what is the basis for our going forward view of who is attacking us and what tactics are appropriate and what's the narrative. Let's not forget that. What does the United States stand for? So I doubt anyone in this room really disagrees with that, and I just think it's time to get on with it. And I want to applaud Jeh for what he has done to set the stage for that.

MR. ISIKOFF: Jeh, in my colleague, my former colleague Dan Klaidman's excellent book *Kill or Capture*, he describes you being briefed about a U.S. Military drone strike in Yemen. Learning about it and afterwards saying "If I was Catholic I would had have to go to confession." What did you feel guilty about?

MR. JOHNSON: Now, look, any time I or any other national security official has to sign off on something that leads to lethal force, that should leave you with a heavy heart, period, irrespective of who the objective is.

And I want to talk about the op-ed in the *Times* today written by Mr. Al-Awlaki senior.

MR. ISIKOFF: Senior.

MR. JOHNSON: I read it. And the reality is that in a congressionally authorized armed conflict on occasion people who are not targeted by the strike are killed. The good news, to the extent there is any in armed conflict, is with our modern technology we are more precise, collateral damage is minimized. And so our government in May -- because a number of officials including the president, obviously, believe that if the U.S. government takes the life of a U.S. citizen, the government should acknowledge that -- acknowledged that the U.S. government was responsible for Mr. Al-Awlaki, for his son and for others.

And the way the attorney general put it, they were not specifically targeted. So the point I want to make is that for any responsible official of our government involving counterterrorism, and there were a number of them in this room, you read an op-ed like that and you get a pit in your stomach and you read it with a heavy heart. And if you don't, you should not be in involved in making these decisions.

MR. ISIKOFF: Absolutely. We have --

MR. ROMERO: I guess --

MR. ISIKOFF: Anthony, I'm going to let you answer, but there are -- there is limited time for question from the audience. So if anybody wants to pose one, now is the time to do so. And I got one right over here.

MR. MONSKY: Harrison Monsky from Foreign Affairs magazine. The *New York Times* has likened the FISA Court to an "almost parallel Supreme Court," in that it's issuing decisions and constitutional interpretations that will shape intelligence practices in the future. Should the -- do you agree with that characterization? Should the FISA Court be playing that role or should the Supreme

Court be taking on some of those cases?

MR. ISIKOFF: Raj?

MR. DE: So the FISA Court is operating as Congress established it in 1978. I think one important fact -- I assume everyone knows how it operates. There are -- these are federal judges, Article III judges. There is a federal FISC quarter review that has ruled rarely, but it has. I think the narrative generally that's out there is that the FISC is a rubber stamp, so few applications are rejected. And there is a handful of people in this room, including myself, who have practiced before the FISC and there is no way that that is an accurate representation.

I think the challenge for the government is how do we improve public confidence in a process that at least from where I'm sitting is working as intended, is working pretty well. The FISC has a full-time staff that is very competent. And if I can address the issue of the applications because I think that's -- something that's out there, certain number of applications are never rejected.

A couple of points; one, if anybody has worked on the criminal side, it's pretty rare that a Title III application is rejected as well. That's just the nature of the business because applications are so well put together through an iterative process. But two, in recent weeks we have started to open up a little bit more to discuss how the FISC process works. And there is something that many of you have probably heard of called a recopy.

So before we file an application with the FISC, we file effectively a draft application that can be days, weeks, months before a final application is submitted. And there is an iterative process with the court and with the judges as to what improvements they would require, what improvements they think need to be necessary and the government takes that into account.

So when -- and a final submission may not be made. And even when it is made, it pretty much accounts

for what the judges would have put in originally. And so it is a legitimate debate as to whether reforms should be made, but I think it's a canard that the number of applications rejected is somehow reflective of the process. And I just would like to make that point.

MR. ROMERO: I would --

MR. ISIKOFF: Any question right here?

MR. ROMERO: Oh, well.

MR. ISIKOFF: Did you want to --

MR. ROMERO: Yeah, let me get a shot.

MR. ISIKOFF: Yeah, okay. Well, before that, let's let Anthony briefly try and --

MR. ROMERO: To the extent in which there is a vigorous process within the Foreign Intelligence Surveillance Court, then let's make it real vigorous. Let's have an adversarial process in our legal system. And if you think it is tough for you to practice before it now, I would love to be in front of you -- opposite you. I think that's the way our courts normally work.

I think the fact is the numbers have not been revealed. I think it is fascinating; Google and all of you co-sponsors of this lovely Institute forum are now asking Congress and the Foreign Intelligence Surveillance Court to release more data on that information. Finally you understood that your self-interest as corporations align with your consumers' privacy interests. Congratulations on being late to the party, but good that you got there.

So let's get this information out. Now, I want to go out on a limb, right, because I have been a little bit watching this. I mean not that I'm already not on a limb, but let me fall off the limb.

(Laughter)

MR. ROMERO: I've been watching this whole debate about Edward Snowden. Maybe we can goose the question. I think he did this country a service. I have not said that publicly until this point. I think he did this country a service by starting a debate that was anemic, that was left to government officials, where people did not understand fully what was happening. I think regardless of where you come out on it, we have now a vigorous public debate.

We have six lawsuits that have been filed on the NSA program. We have Congress holding hearings yesterday, finally saying "what a minute, that's not the law I thought I had signed," including the author of the bill, Mr. Sensenbrenner. I find it rather troublesome when I find that the White House press secretary, Mr. Carney, goes at such lengths to say "he is not a human rights activist, he is not a dissident and he is not a whistleblower." Well, who made him king of the human rights community, right? I think actually Edward Snowden --

MR. ISIKOFF: I can't let this --

MR. ROMERO: I know. I'm starting it out --

MR. ISIKOFF: Excuse me. I can't let this stand without giving Neil MacBride, who has criminally charged Snowden, a chance to respond.

MR. JOHNSON: I think -- I have to say, I think it's a bad message for us to send to people who decide to take the law into their own hands they are doing a public service.

MR. ROMERO: I think when the system has not worked -- we have sued seven times to try to get the surveillance program before a proper court. We were kicked out of court. The Clapper versus Amnesty International court, where Don Verrilli, the Justice Department lawyer said it was a cascade of speculation when our clients said we think our data has been collected by the government. And since we had no proof that we had been surveilled, we had no standing.

It has not been for lack of trying, Jeh Johnson. It has been --

MR. JOHNSON: Courts are where these debates belong.

MR. ROMERO: And the only way we can get before the court -- the only way we have standing now before this court is because Mr. Snowden leaked the fact that we are clients of Verizon business network. Guess what? My Snowden fixed my standing problem.

MS. HARMAN: But Mr. --

MR. ROMERO: And our democracy -- regardless of whether or not you think he broke the law, regardless of whether or not you think he should be hauled to the Fourth Circuit, I think our country is better as a result of the revelations of Mr. Snowden.

MR. JOHNSON: That's anarchy.

MS. HARMAN: I think our country needs a debate.

MR. ROMERO: That is not anarchy.

MS. HARMAN: But I do not think --

MR. ROMERO: That is Daniel Ellsberg. That is --

MS. HARMAN: No, this is completely different from Ellsberg.

MR. ROMERO: No --

MS. HARMAN: This is a kid who had nothing to do with formulating the policy, from my likes is totally self-centered and narcissistic. But anyway, it's not just the information about these programs, much of which was in the public domain. It's a whole bunch of other stuff which compromises ongoing investigations, which I think is way off on this in one other point; that this guy needs to

seek public -- whatever it is -- asylum from other countries because he would be persecuted here is totally nonsense. A lot of Americans support what he did. He should come back and face a fair trial. He has been charged but he hasn't been convicted.

MR. ROMERO: Private Manning's treatment before he was prosecuted by our government was torture. Now, I want to say that I may not agree. We have yet not decided whether or not we will defend Mr. Snowden. That is yet to be. We'll see if he ends up in a -- we have nothing to do with foreign asylum applications. He can go find his help elsewhere. But I will say that I am personally grateful that we are now having the debate we should have had long ago. Because we have been doing this for 13 --

MS. HARMAN: Yes.

MR. ROMERO: I have been in my job for 13 years. I started the week before 9/11. And we have tried to have this very debate all throughout and we have not had it -- we've not had the hearings in Congress that we had yesterday. We've not had the six lawsuits that have been filed. We've never had standing up until this moment and we've never had our European allies -- now many of you are here in the room from British parliament I understand -- who now also seem to raise questions about whether or not the government intelligence efforts run afoul with the way we interact with our allies.

So I think for whatever it's worth, you know, I think we are better off today, now, knowing about the NSA program than we were back in March of this year. And so I just want to say that publicly.

MR. ISIKOFF: Do you want to weigh in?

MR. MacBRIDE: I mean briefly, just to say that the case Anthony mentions of course is an ongoing case, so I can't talk about that specifically. What I can say very clearly and unambiguously and forcefully is that the Justice Department does not pursue whistleblowers. That canard has been -- to use Raj's phrase, has been used -- and to use just the one example that Mike alluded to, my

district prosecuted and convicted a former CIA official last year, an individual who had signed nine nondisclosure agreements over the course of his career. He was convicted. He pled guilty. He admitted that he outed the name of a covert agent, that he outed the name of a highly classified program.

When you talk to people in the intelligence community, many of whom who are sitting here, what I'm always told is that the most damaging leaks involve outing covert agents and outing classified programs. The case that we prosecuted involved both. The individual when he made the disclosure never claimed that he was a whistleblower. That was sort of a self servicing mantle that was claimed years later.

MR. ISIKOFF: That's John Kiriakou.

MR. MacBRIDE: And when he was sentenced, the judge, Judge Brinkema, who is the judge in the case -- the other case you asked about, Michael --

MR. ISIKOFF: Yeah.

MR. MacBRIDE: -- said to him, you know, you are not a whistleblower.

MR ISIKOFF: We have a patient questioner in the audience here, who has had the microphone for --

MR. ROMERO: Go ahead, please.

MR. OSBURN: I love a good debate. Thank you to the panelists. I'm Dixon Osborn with Human Rights First. And the theme this morning seems to be about information and what should be disclosed, what shouldn't. And I wanted to ask you about a slightly different topic, which is torture. The Senate Intelligence Committee did a 6,000 page study of torture after 9/11. It's the most comprehensive document to be produced to date. They searched through 3 million documents. There are 25,000 footnotes.

But though it has been adopted by the

Intelligence Committee, it has not yet been voted for declassification and the reports in the press are that the CIA is pushing back very hard on that. Isn't this something that the American people deserve to know? The Senate Armed Services Committee does a similar study for the Military's role post 9/11 and that has been made public. But the intelligence community's role has not been made public.

MR. ISIKOFF: Jeh, you want to take a crack at that?

MR. JOHNSON: I think the answer to the question is yes. I think that the report that was done by the Senate Armed Services Committee is a very valuable, important report. I personally had a number of takeaways from it vis-a-vis the legal community in the Department of Defense. I think that the legal reviews that were done to authorize the particular interrogations at issue were not done in a proper way. I think that the senior lawyer of the Department of Defense should have been more personally involved in conducting those reviews.

And so I think that that study is an important valuable study and we ought to declassify as much of it as we can.

MR. OSBURN: I agree. Thank you.

MR. ISIKOFF: Any other question over here on this side? And then we'll get to you.

MR. KLINE: Kevin Kline (phonetic). I was going to ask Jane, how do we ensure a robust debate on public policy issues that involve intelligence operations when they are classified within certain members of Congress, so the oversight committees can't share with the other members of Congress?

MS. HARMAN: Well, the tradition has always been that the members of the intelligence committees -- which are leadership committees; you don't get on there unless your leader in our party put you on there -- were trusted with a lot of secrets that weren't shared with others.

The reason for that was -- and I come back to this -- sources and methods have to be protected.

MR. ROMERO: Absolutely.

MS. HARMAN: And I often joke that Congress doesn't leak because we don't have any information.

(Laughter)

MS. HARMAN: But actually some members of Congress do, and I was one of those members. Should Congress nonetheless even with perhaps a higher level of information shared only with the Intelligence Committee conduct robust debates? You bet. And Congress -- oops, two minutes -- is capable of doing this. Is Congress going to do this in the near-term? I doubt it.

And I think that is -- and that's what Bob Corker was saying; it's a huge abdication of responsibility. This is a bipartisan rant, folks, and it will take a bipartisan group -- I think starting with the intel committees and those folks seem to get along with each other -- pushing this thing. But there should be a debate.

Somebody suggested maybe we need a National Security Act of 2014. Think about that? The National Security Act, which the framework for most of our security apparatus was passed in 1947. No business on the planet could operate with a 1947 business model. We changed part of it in 2004 when we adopted intelligence reform. I was part of that. I'm very proud of what we did. It wasn't perfect. It was implacably opposed by Don Rumsfeld and the then chairman of the House Armed Services Committee, so we had to make some compromises. But at least it created a modern horizontal structure over 16 intelligence agencies.

Congress should revisit this issue. Congress should be responsible. And maybe out here and, you know, in Washington and wonderful places like the Wilson Center -- I'm totally objective -- we ought to start that debate, jumpstart the debate. And Anthony Romero is part of that

debate. He knows that. We've had lots of programs where he has participated. We need the civil liberties point of view. We need the point of view of the press. We need the folks who have been in and are in our Intelligence Committee, and we need the public perceptions.

And the last point I would make here is security and liberty are not a zero sum game. It's not that you get more of one and less of the other. They are either a positive sum game or a negative sum game. And if you don't like where we are, let's have another attack on America and then we will shred our Fourth Amendment and that would be a catastrophe.

MR. ROMERO: I agree.

MR. ISIKOFF: Last word, Jeh Johnson.

MR. JOHNSON: I think when it comes to leaks there really is a big picture point that has to be made. We have a 9/11 or a Fort Hood or a Boston Marathon and everybody in Washington ask, "What happened? What failed? How can we do better? You are not connecting the dots enough. They are all stove piped. We've got to do a better job of connecting the dots."

So our government sets out to do a better job of connecting the dots. And then you get a Manning or a Snowden, and people say, "What happened.? How can we do better? Where did the system fail? It's because you connected too many dots and you gave too many people access to information. Well, we've got to stop that." And so the pendulum swings back the other way.

The problem is -- then the reality is, and a lot of people probably don't want to hear this, if there is somebody determined to commit a criminal act, if there was a summer intern in my office determined to get into my office, which is a SCIF, and snatch from my desktop a top secret document and give it to Mike Isikoff, he will probably be able to figure out a way to do that and break through all the barriers that exist. And we don't necessarily need to think about changing national security policy in reaction to one criminal event. I think that

that person needs to be dealt with in the criminal justice system.

MR. ISIKOFF: And then will have to avoid criminal prosecution by Neil. Anyway, on that point -- apparently we are out of time. I want to thank our panelists for a great discussion, to be continued.

(Applause)

* * * * *