PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

Workshop Regarding Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act

July 9, 2013

The workshop 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
Elizabeth Collins Cook

PANEL I

Legal/Constitutional Perspective

Steven Bradbury, formerly DOJ Office of Legal Counsel
Jameel Jaffer, ACLU
Kate Martin, Center for National Security Studies
Hon. James Robertson, Ret., formerly District Court and Foreign Intelligence Surveillance Court
Kenneth Wainstein, formerly DOJ National Security Division/White House Homeland Security Advisor

PANEL II

Role of Technology

Steven Bellovin, Columbia University Computer Science Department

Marc Rotenberg, Electronic Privacy Information Center

Ashkan Soltani, Independent Researcher and Consultant

Daniel Weitzner, MIT Computer Science and Artificial Intelligence Lab

PANEL III

Policy Perspective

James Baker, Formerly DOJ Office of Intelligence and Policy Review

Michael Davidson, Formerly Senate Legal Counsel

Sharon Bradford Franklin, The Constitution Project

Elizabeth Goitein, Brennan Center for Justice

Greg Nojeim, Center for Democracy and Technology

Nathan Sales, George Mason School of Law

PROCEEDINGS

MR. MEDINE: Good morning, and welcome to the third public meeting held by the Privacy and Civil Liberties Oversight Board.

I want to first introduce my fellow board members Rachel Brand, Pat Wald, Beth Cook and Jim Dempsey.

PCLOB, as we are often known, is an independent bipartisan agency within the Executive Branch. We were recommended by the 9/11 Commission and created by Congress.

The board's primary missions are to review and analyze actions by the Executive Branch 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 laws, regulation and policies related to protect the nation from terrorism.

Essentially PCLOB is both an advisory and it has an advisory and oversight role with respect

to our country's counterterrorism efforts.

I wanted to thank our many panelists throughout the day for agreeing to participate in this workshop and share their views about these important programs with the board.

I also wanted to thank Sue Reingold, the board's chief administrative officer and Diane Janosek, our chief legal officer for their tireless efforts in making this event possible.

Our focus today will be two federal counterterrorism programs, the Section 215 program under the USA PATRIOT Act and the Section 702 program under the FISA Amendments Act.

The purpose of the workshop is to foster a public discussion of legal, constitutional and policy issues relating to these programs. PCLOB has agreed to provide the President and Congress a public report on these two programs, along with any recommendations it may have.

A few ground rules for today's workshop, we expect that the discussion will be based on unclassified or declassified information.

However, some of the discussion will inevitably touch on leaked classified documents or media reports of classified information.

In order to promote a robust discussion speakers may choose to reference these classified documents or information but they should keep in mind that in some cases these documents still remain classified, therefore while discussing them speakers in a position to do so are urged to avoid confirming the validity of the documents or information.

There will be three panels today. The first will focus on legal issues, the second on technical aspects, and the third on policy.

After the first panel we will be taking a lunch break. Two board members will moderate each panel and will pose questions and additional board members may have follow-up questions.

Panelists are urged to keep their responses brief to permit the greatest possible exchange of views.

At the end of the day there will be some

time for members of the audience to make statements about these two programs.

This workshop is being recorded and a transcript will be posted on what we hope will be PCLOB's website active this evening, and as well as on regulations.gov.

Those who wish to submit written comments about these issues are welcome to do so, and comments may be submitted at regulations.gov or by mail until August 1st.

I want to start by level setting the discussion. My description that follows of the two programs is based on information that's been publicly disclosed by the federal government. It should not be interpreted as saying new about these programs. It's merely a summary of the unclassified remarks by federal government officials.

PCLOB has not come to any conclusions regarding the accuracy or completeness of this information or the two programs' legal justification.

There are a couple of things in common between the two programs. Both are designed, among other things, to identify terrorists and if possible prevent terrorist plots. Both require orders from the Foreign Intelligence Surveillance Court, but the criteria for such orders may differ for each program.

In both it's possible that even with the best intentions the government may end up collecting or accessing information beyond what was authorized leading to questions about how such information should be handled.

And of course both programs have been the subject of leaks by Mr. Snowden.

In terms of the specific programs, the first is based on Section 215 of the USA PATRIOT Act, which was reauthorized by Congress in 2011. Sometimes this is referred to as the 215 Business Records Collection Program.

One of the things the government collects under 215 is telephone metadata pursuant to court order authorized by the Foreign Intelligence

Surveillance Act under a provision that allows the government to obtain business records for intelligence and counterterrorism purposes.

The government's argued that the collection of this information must be broad in scope because more narrow collection would limit the government's ability to screen for a identify terrorism-related communications.

The metadata that's been collected describes telephone calls such as the telephone number making the call, the telephone number dialed, the date and time the call was made and the length of the call.

The government takes the position that these are considered business records of the telephone companies.

This program does not collect the contents of any communications, nor the identity of the persons involved with the communication. Intelligence community representatives have stated that cell phone location information is not collected, such as GPS or cell tower information.

In approving the program, the FISA Court has issued two orders. One order, which is the type of order that was leaked, is an order to the telephone providers directing them to turn information over to the government.

It's been asserted that the other order spells out the limitations what the government can do with the information after it's been collected, who has access to it and for what purpose it can be accessed and how long it can be retained.

Court orders must be issued every 90 days for the program to continue.

Concerns have been raised that once large quantities of metadata about telephone calls have been collected it could be subjected to sophisticated analysis to drive information that could not otherwise be determined.

This type of analysis is not permitted under this program. Instead the metadata can only be queried when there is a reasonable suspicion that a particular telephone number is associated with specified foreign terrorist organizations.

Even then the only purpose for which the data can be queried is to identify contacts.

In other words, the input and output of this program is limited to metadata. In practice only a small portion of the data that's collected is actually ever reviewed because the vast majority of data is never going to be responsive to terrorism-related queries.

For example, in 2012 fewer than 300 identifiers were approved for searching this data.

The rationale for this program is that because all the metadata is collected because if you want to find the needle in the haystack you need to have the haystack.

Follow-up investigations that result from the analysis of metadata such as electronic surveillance of particular U.S. telephone numbers requires a court order based on probable cause.

I'm turning now to the second program under Section 702. It involves the government's collection of foreign intelligence information from electronic communication service providers

under court supervision pursuant to Section 702 of the Foreign Intelligence Surveillance Act. It's been referred to as PRISM, which is a misnomer. PRISM does not refer to a data collection program, it's instead the name of a government database.

Under Section 702, which was reauthorized by Congress in December 2012, information is obtained with FISA Court approval with the knowledge of the provider, and based on a written directive from the Attorney General and the Director of National Intelligence to acquire foreign intelligence information.

The law permits the government to target a non-U.S. person, that is somebody who is not a citizen or a permanent resident alien, located outside the United States for foreign intelligence purposes without obtaining a specific warrant for each target.

The law prohibits targeting somebody outside of the United States in order to obtain information about somebody in the United States. In other words, Section 702 prohibits reverse

targeting of U.S. persons.

The law also does not permit intentionally targeting any U.S. citizen or other U.S. person, or intentionally target any person known to be in the United States.

In order to obtain FISA Court approval there must be first an identification of the foreign intelligence purposes for the collection, such as for prevention of terrorism, hostile cyber activities or nuclear proliferation, and procedures for ensuring individuals targeted for collection are reasonably believed to be U.S. persons located outside of the United States.

There must be also approval of the government's procedures for what it will do with the information about a U.S. person or someone in the United States if it gets that information through this collection.

Court approved minimization procedures, which have also been the subject of a leak, determine what can be kept and what can be disseminated to other government agencies.

Dissemination of information about U.S. persons is expressly prohibited unless the information is necessary to understand foreign intelligence, assess its importance, is evidence of a crime, or indicates an imminent threat of death or serious bodily harm.

The intelligence community asserts the communications collected under this program have provided insight into terrorist networks and plans, including information on terrorist organizations strategic planning efforts, contributing to impeding the proliferation of weapons of mass destruction and related technologies and successful efforts to mitigate cyber threats.

We will turn now to our first panel which will focus on legal and constitutional perspectives on the two programs. Board members Rachel Brand and Pat Wald will moderate the panel.

MS. BRAND: All right, thank you, David. Good morning, everyone, thank you for coming.

I'm Rachel Brand, one of the members of

the board. My colleague Patricia Wald and I are moderating the first panel which is focusing on the legality of the two types of surveillance that David described. The policy implications of those types of surveillance will be discussed at a later panel.

We have a panel of five distinguished experts to give us their views on these issues. I'll introduce them in a moment. Each of them will have up to five minutes to give opening remarks.

Our general counsel Diane Janosek is in the front row with cards, red, green, yellow, so for your benefit on the panel.

Then each panelist will have up to two minutes to give responsive remarks, reflections on what the other panelists have said. Pat and I will then ask a series of questions to the panel, and for the last 15 minutes our colleagues on the board will have a chance to ask questions as well.

So our panelists are, in alphabetical order, Steve Bradbury, who is a partner at a law

firm here in D.C. and was the head of the Office of Legal Counsel at the Justice Department from 2005 to 2009.

Jameel Jaffer is the Deputy Legal Director with the ACLU and is currently involved in a constitutional challenge in court to one of the programs we're talking about today.

Kate Martin is the Director of the Center for National Security Studies.

James Robertson is a former U.S. District Judge and also served on the Foreign Intelligence Surveillance Court.

And Ken Wainstein at the end is a partner at Cadwalader, Wickersham and Taft and served previously as the Homeland Security Advisor as the Head of the National Security Division at the Justice Department and as a U.S. Attorney here in Washington.

So Steve, we'll start with you.

MR. BRADBURY: Thanks, Rachel. I appreciate the opportunity to participate today.

I'm going to focus my opening remarks on

the telephone metadata program. As the government has stated, and David summarized, this program is supported by a Section 215 business records order, which must be reviewed and reapproved by the federal judges who sit on the FISA Court every 90 days.

And I understand that fourteen different federal judges have approved this order since 2006.

The metadata acquired consists of the transactional information that phone companies retain for billing purposes. It includes only data fields showing which phone numbers called which numbers and the time and duration of the calls.

This order does not give the government access to any information about the content of calls or any other subscriber information, and it doesn't enable the government to listen to anyone's phone calls.

Access to the data is limited under the terms of the court order. Contrary to some news

reports, there's no data mining or random sifting of the data permitted.

The database may only be accessed through queries of individual phone numbers and only when the government has reasonable suspicion that the number is associated with a foreign terrorist organization.

If it appears to be a U.S. number the suspicion cannot be based solely on activities protected by the First Amendment. Any query of the database requires approval from a small circle of designated NSA officers.

A query will simply return a list of any numbers the suspicious number has called and any numbers that have called it, and when those calls occurred. That's all.

The database includes metadata going back five years to enable an analysis of historical connections.

Of course any connections that are found to numbers inside the United States will be of most interest because the analysis may suggest the

presence of a terrorist cell in the U.S.

Based in part on that information the FBI may seek a separate FISA order for surveillance of a U.S. number but that surveillance would have to be supported by individualized probable cause.

The NSA's Deputy Director, as David mentioned, has testified that in all of 2012 there were fewer than 300 queries of the database, and only a tiny fraction of the data has ever been reviewed by analysts.

The database is kept segregated and is not accessed for any other purpose. And NSA requires the government -- and FISA, excuse me, requires the government to follow procedures overseen by the court to minimize any unnecessary dissemination of U.S. numbers generated from the queries.

In addition to court approval, the 215 order is also subject to oversight by the Executive Branch and Congress. FISA mandates periodic audits by inspectors general and reporting to the intelligence and judiciary

committees of Congress.

When Section 215 was reauthorized in 2011 I understand the leaders of Congress and members of these committees were briefed on this program, and all members of Congress were offered the opportunity for a similar briefing.

Now let me address the statutory and constitutional standards. Section 215 permits the acquisition of business records that are, quote, relevant to an authorized investigation.

Here the telephone metadata is relevant to counterterrorism investigations because the use of the database is essential to conduct the link analysis of terrorist phone numbers that I've described. And this type of analysis is a critical building block in these investigations.

In order to connect the dots we need the broadest set of telephone metadata we can assemble, and that's what this program enables.

The legal standard of relevance in Section 215 is the same standard used in other contexts. It does not require a separate showing

that every individual record in the database is relevant to the investigation.

The standard is satisfied if the use of the database as a whole is relevant. It's important to remember that the Fourth Amendment does not require a search warrant or other individualized court order in this context.

A government request for business records is not a search within the meaning of the Fourth Amendment. Government agencies have authority under many federal statutes to issue administrative subpoenas without court approval for documents that are relevant to an authorized inquiry.

In addition, grand juries have broad authority to subpoena records potentially relevant to whether a crime has occurred, and grand jury subpoenas also don't require court approval.

In addition, the Fourth Amendment does not require a warrant when the government seeks purely transactional information or metadata, as distinct from the content of communications.

This information is voluntarily made available to the phone company to complete the call and for billing purposes. And courts have therefore said there's no reasonable expectation that it's private.

I would stress however that Section 215 is more restrictive than the constitution demands because it requires the approval of a federal judge.

And while the 215 order for metadata is extraordinary in terms of the amount of data acquired. It's also extraordinarily protective in terms of the strict limitations placed on accessing the data.

For these reasons I think the program is entirely lawful and conducted in a manner that appropriately respects the privacy and civil liberties of Americans. Thank you.

MS. BRAND: Thank you, Steve. Jameel.

MR. JAFFER: Thanks for the invitation to participate.

Since these programs were disclosed much

of the public debate has focused on issues of policy, and I think that's understandable. No government has ever trained this kind of surveillance power upon its own citizens.

Until quite recently none had the technological capacity to do that. We need to think carefully about how the exploitation of new technology could affect liberties that generations of Americans have fought to protect.

What I'd like to underscore today is that the recently disclosed surveillance programs aren't just unwise, they're unconstitutional as well.

And I'm going to focus principally on the 215 program with the hope that we'll be able to return to 702 later on.

Under the 215 program the NSA collects metadata about every phone call made or received by a resident of the United States.

Some news reports indicate that the NSA is collecting Internet metadata as well, making a note of every website an American visits and every

email he or she receives.

The program is a massive dragnet, one that raises many of the concerns associated with general warrants, that is many of the concerns that led to the adoption of the Fourth Amendment in the first place.

You might say that these Section 215 orders are general warrants for a digital age. The President and the DNI has emphasized that the government is collecting metadata, not content. But the suggestion that metadata collection is somehow beyond the reach of the Constitution is wrong.

For Fourth Amendment purposes the crucial question isn't whether the government is collecting metadata or content, but whether it is invading reasonable expectations of privacy. And here it clearly is.

The Supreme Court's recent decision in Jones is instructive. In that case a unanimous court held that long-term surveillance of an individual's location constituted a search under

the Fourth Amendment.

The justices reached that conclusion for different reasons, but at least five justices were of the view that the surveillance infringed a reasonable expectation of privacy.

Justice Sotomayor observed that tracking an individual's movements over an extended period allows the government to generate, quote, a precise comprehensive record that reflects a wealth of detail about her familial, political, professional, religious and sexual associations.

The same can be said of the tracking now taking place under Section 215. Call records can reveal personal relationships, medical issue, and political and religious affiliations. Internet metadata may be even more revealing, allowing the government to learn which websites a persons visited, precisely which article she read, whom she corresponds with, and who those people correspond with.

The long-term surveillance of metadata constitutes a search for the same reasons that the

long-term surveillance of location was found to constitute a search in Jones.

In fact, the surveillance that was found unconstitutional in Jones was narrower and shallower than the surveillance now taking place under Section 215.

The location tracking in Jones was meant to further a specific criminal investigation into a specific crime and the government collected information about one person's location over a period of less than a month.

What the government has implemented under Section 215 is an indiscriminate program that has already swept up the communications of millions of people over a period of seven years.

Some have argued that Section 215, the program under Section 215 is lawful under Smith v. Maryland, which upheld the installation of a pen register in a criminal investigation.

But the pen register in Smith was very primitive. It tracked the numbers being dialed but it didn't indicate which calls were completed,

let alone the duration of the calls, and the surveillance was directed at a single criminal suspect over a period of less than two days. The police weren't casting a net over the whole country.

Another argument that's been offered in defense of the metadata program is that though the NSA collects an immense amount of information, it examines only a tiny fraction of it.

But the Fourth Amendment is triggered by collection of information, not simply by the querying of it. The same is true of the First Amendment because the chilling effect of government surveillance stems from the collection of information, not merely the analysis of it.

The Constitution isn't indifferent to the government's accumulation of vast quantities of sensitive information about American's lives, neither should the board be.

Indeed it's worth remembering in this context that other countries have aspired to total awareness of their citizens' associations,

movements and beliefs. The experiences of those countries should serve as a caution to us, not as a road map.

Thank you again for inviting me to participate, and I look forward to the board's questions.

MS. BRAND: Thank you. Kate.

MS. MARTIN: Thank you also for inviting me and giving me this opportunity to participate today.

I want to take this opportunity to raise some overarching concerns which I hope the board will address before making specific recommendations about necessary changes to either Section 702 or 215, and begin by quoting Senator Sam Ervin, who in 1974 as the author of the Privacy Act noted that the more the government knows about us, the more power it has over us. When the government knows all of our secrets we stand naked before official power. The Bill of Rights then becomes just so many words.

I think it is not debatable that secrecy

increases the danger that the government will overreach, nor is it debatable that foreign intelligence activities depend to some degree on secrecy and that a democracy must continually work to figure out ways to provide for the national defense, while respecting civil liberties and preserving constitutional governments.

The increase in technological surveillance capabilities, global connectedness and the reliance on electronic communications in daily life has made doing this more complex and even more important.

I want to ask however whether or not the expansion of secret government surveillance and secret legal authorities, especially in the last twelve years requires us to ask whether we are witnessing the serious erosion of our constitutional system of checks and balances, and the rise of a system of secret law decreed by courts, carried out in secret, enabling the creation of massive secret government databases of American's personal and political lives.

As you know quite well, the system of checks and balances relies upon, first, the existence of a Congress which engages in and is influenced by a public debate.

It relies upon the existence of courts which hear two sides to a question and know their opinions are subject to appeal and subject to public critique.

And finally, an Executive Branch who will be called to account should they ignore or violate the law.

And fundamentally all of this depends upon the existence of an informed and engaged press and public.

So why does it matter? I think it matters fundamentally for two reasons. First is that the system is set up in order to prevent the government from breaking the law and to ensure that if it does so that will become known and the Executive Branch will be held to account for doing so.

Secondly, the system is meant to prevent,

as Jameel outlined, the government from using its surveillance capabilities to target its political opponents, to chill political dissent, and to limit the political debate and options in this country.

This is not a theoretical concern. Of course in my lifetime it has happened many times already in this country.

Perhaps later on I could detail what I find to be the shocking revelation of the history of these programs, beginning in 2001 and resulting in where we are today, where we only learned through unauthorized leaks that there is at least one secret opinion authorizing the massive collection of telephony metadata.

We still don't know what the secret law is about the collection of massive amounts of Internet metadata. Although we know that presumably this administration has stopped that, we have no idea whether or not there is law that would permit that to resume.

I think that the question that we need to

ask is whether or not the system of checks and balance needs to be reaffirmed so that it acts as a safeguard against these two harms.

There is, I think the history of the debates on these issues over the past few years demonstrate that the debate has been incomplete. It has been informed by inaccurate information at best supplied by the government, if not deliberately.

Finally I just want to note that I've worked on these FISA issues for almost a quarter of a century and I think that probably of the many civil liberties voices that have been raised in objection to these programs, I am maybe one of the least likely to be labeled an alarmist.

MS. BRAND: Thank you. I know you have more you wanted to get to, and David may have mentioned this too, but any of the panelists and anyone in the public can submit written comments to the board, so if you have a fuller statement that you'd like to submit, you're welcome to do that.

Judge Robertson.

MR. ROBERTSON: Thank you. I should probably first state that I am a member, I am now and have been a member of the Liberty and Security Committee of the Constitution Project, which wrote a report in September of 2012 expressing some alarm about these programs. And I signed that report and stand by it, but that's not primarily what I want to talk about today.

I did sit on the FISA Court for a few years. I asked to be appointed to the FISA Court, frankly to see what it was up to. And I came away from it deeply impressed by the careful, scrupulous, even fastidious work that the Justice Department people, and the NSA, and FBI agents involved with it did.

The FISA Court was not a rubber stamp. The fact, the numbers that are quoted about how many reports, how many warrants get approved do not tell you how many were sent back for more work before they were approved.

So I know at firsthand, and I wish I

could assure the American people that the FISA process has integrity and that the idea of targeting Americans with surveillance is anathema to the judges of the FISA Court, which they call the FISC.

But I have a couple of related points to make. First, the FISA process is ex parte, which means it's one sided, and that's not a good thing.

And secondly, under the FISA Amendment Act, the FISA Court now approves programmatic surveillance, and that I submit and will discuss for a few minutes, I do not consider to be a judicial function.

Now judges are learned in the law and all that, but anybody who has been a judge will tell you that a judge needs to hear both sides of a case before deciding.

It's quite common, in fact it's the norm to read one side's brief or hear one side's argument and think, hmm, that sounds right, until we read the other side.

Judging is choosing between adversaries. I read the other day that one of my former FISA Court colleagues resisted the suggestion that the FISA approval process accommodated the executive, or maybe the word was cooperated. Not so, the judge replied. The judge said the process was adjudicating.

I very respectfully take issue with that use of the word adjudicating. The ex parte FISA process hears only one side and what the FISA process does is not adjudication, it is approval.

Which brings me to my second and I think closely related point. The FISA approval process works just fine when it deals with individual applications for surveillance warrants because approving search warrants and wiretap orders and trap and trace orders and foreign intelligence surveillance warrants one at a time is familiar ground for judges.

And not only that, but at some point a search warrant or wiretap order, if it leads on to a prosecution or some other consequence is usually

reviewable by another court.

But what happened about the revelations in late 2005 about NSA circumventing the FISA process was that Congress passed the FISA Amendments Act of 2008 and introduced a new role for the FISC, which was to approve surveillance programs.

That change, in my view, turned the FISA Court into something like an administrative agency which makes and approves rules for others to follow.

Again, that's not the bailiwick of judges. Judges don't make policy. They review policy determinations for compliance with statutory law but they do so in the context once again of adversary process.

Now the great paradox of this intelligence surveillance process of course is the undeniable need for security. Secrecy, especially to protect what the national security community calls sources and methods.

That is why the Supreme Court had to

refuse to hear Clapper versus Amnesty International. The plaintiffs could not prove that their communications were likely to be monitored so they had no standing. That is a classic catch-22 of Supreme Court jurisprudence.

But I submit that this process needs an adversary, if it's not the ACLU or Amnesty International, perhaps the PCLOB itself could have some role as kind of an institutional adversary to challenge and take the other side of anything that is presented to the FISA Court.

Thank you.

MS. BRAND: Thank you, Judge. Ken.

MR. WAINSTEIN: Okay, good morning, everybody. I'd like to thank the board for inviting me here to speak on these very important issues.

I'd like to focus my remarks today on the FISA Amendments Act and the authority in Section 702.

MS. BRAND: Ken, can you pull the mic over to you.

MR. WAINSTEIN: I'm sorry. As I said, I'd like to focus my remarks today on the FISA Amendments Act and the Section 702 authority that David has described earlier.

The recent disclosures regarding the PRISM Program have raised questions in some quarters about the appropriateness and legality of the government's collection of Internet communications traffic, with some expressing surprise that collection of that type and that scale is taking place.

A review of the text of the FISA Amendments Act and the historical record reveals however that that Internet collection appears to be exactly what was contemplated when Congress passed that statute in 2008.

I'd like to take a moment to remind ourselves about the FAA, the FISA Amendments Act and the reason it came into being in the first place. In 1978 Congress undertook to create a process by which electronic surveillance of foreign powers or their agents must first be

approved by the FISA Court.

In doing so however Congress recognized it had to balance the need for a judicial review process for domestic surveillance against the government's need to freely conduct surveillance overseas where constitutional protections do not apply.

It sought to accomplish this objective by imposing in the FISA statute a court approval requirement on surveillances directed against persons within the U.S. and leaving the intelligence community free to surveil overseas targets without the undue burden of court process.

With the change in technology over the years since FISA was passed however that foreign domestic distinction started to break down. And the government found itself expending significant manpower in generating FISA Court applications for surveillances against persons outside the United States, the very category of surveillances that Congress specifically intended to exclude when it

imposed the FISA Court approval process requirement in 1978.

As this problem got worse, particularly after the 9/11 attacks, the government found itself increasingly unable to cover its surveillance needs.

Congress, to its credit, took up this issue in the spring of 2007 and over the next fifteen months or so numerous government officials, including Steve Bradbury, myself and others, spent countless hours testifying and meeting with members and staff up on the hill, and after thorough analysis and deliberations Congress ultimately provided relief in the form of the FISA Amendments Act, which passed in the summer of 2008.

Section 702 of the FAA created a new process, a new process by which categories of foreign surveillance targets can be approved for surveillance.

Under this process, the Attorney General and the DNI provide the FISA Court annual

certifications identifying the target categories and certifying that all statutory requirements for surveillance of those targets have been met.

The government in turn designs targeting procedures which are the operational steps that it takes to determine whether each individual surveillance target is outside the United States, as well as minimization procedures that David described, that limit the handling and dissemination of any information relating to U.S. persons.

The government then submits the certifications, as well as the targeting and minimization procedures for review by the FISA Court and the FISA Court confirms whether all statutorily required steps have been taken in compliance with FISA and the Fourth Amendment.

Now this process succeeds in bringing the operation of FISA back in line with its original intent. It still provides that any surveillance targeting a U.S. person here or abroad, or targeting any person believed to be inside the

United States must be conducted pursuant to an individualized FISA Court order.

However, it allows the government to conduct surveillance of foreign targets overseas without the need to secure individualized court approval. And it does so while at the same time giving the FISA Court an important role in ensuring that this authority is used only against those non-U.S. persons who are reasonably believed to be located outside the U.S.

In addition, the FAA tasks various levels of government with conducting significant and meaningful oversight over this authority.

The authority procedures and oversight prescribed by the FAA have been in place since 2008 and just last year they were reauthorized.

Prior to its reauthorization the intelligence committees of both houses were briefed on the classified details of its implementation, and that same briefing was made available to all members.

As this history demonstrates the FAA was

a carefully calibrated piece of legislation that addressed an urgent operational need while at the same time maintaining the privacy protections that the original FISA statute afforded to domestic communications.

With the recent public disclosures about the PRISM Program we are now seeing the statute in action. Not surprisingly we're seeing exactly what was contemplated when Congress carefully considered and passed the FAA, which is a program that focuses on the surveillance of foreign national security targets, which is where the Executive Branch has its greatest latitude, that is conducted well within the bounds of the Fourth Amendment, that is carried out with the knowledge and engagement of all three branches of government and that is monitored with multiple levels of oversight.

And that is exactly what Congress and the American people asked for in the legislative process that resulted in the passage of the FAA.

I appreciate the opportunity to address

these issues here today and I look forward to any questions that the board may have.

MS. WALD: Thank you. We're now going to enter into the second phase of our program and that is, each person on the panel gets two minutes to respond to any of the comments or to make their own comments upon what other panelists have said. So we'll get the going, Steve.

MR. BRADBURY: Thank you, Judge Wald. Just real quick responding to a few points that Jameel made first.

Jameel said that he thought no other country conducts surveillance like the NSA. I don't think anybody here should leave today assuming that statement is correct.

In terms of the 215 telephone metadata collection, he described it as a dragnet. I think of a dragnet as a collection of mass amounts of content communications, not metadata. I think there's a critical difference between content and metadata, and I think the Constitution recognizes that.

He talked about the Jones case which is the GPS tracking device that's put on a particular car for a particular individual. Well that case involved, as he described it, tracking of an individual, the government doggedly following around and tracking a particular individual.

Here in the collection of the metadata there's no targeting or tracking of an individual until a suspicious number is put into the database.

And the targeting under the 702 order is only focused on non-U.S. persons believed to be outside the U.S.

He described the Smith versus Maryland case as simply a case involving a primitive device and focused on an individual. Well, this case has been applied by the lower courts more broadly and also the fact that it was focused on an individual there I think is more constitutionally significant than a general collection of metadata.

I want to talk for just a minute about some of the comments that Kate and Judge Robertson

made about secrecy and the rise of secret law and also the role of the court with programmatic orders, etcetera.

I think it's important to understand the constitutional background. As Ken alluded, before 1978 surveillance for foreign intelligence purposes was conducted by the president without court approval. And the courts have consistently said that the president has authority to undertake such surveillance without court approval where the target is a foreign intelligence threat.

And FISA -- that led to abuses, but FISA was created as a compromise between the branches to enable that kind of surveillance but to involve Article III courts in the review and approval, and Congress in the oversight, creating the intelligence oversight committee.

MS. WALD: Steve, I'm going to have to be very tough. You've covered an enormous amount and I'm sure --

MR. BRADBURY: Thank you.

MS. WALD: You can pick up in the

individual questions, which will come about later. Thank you. Jameel.

MR. JAFFER: So let me just start by expressing a degree of frustration about something that Mr. Wainstein said.

So when we were before the Supreme Court in Amnesty v Clapper last year, the government repeatedly said, and they said this in the lower courts as well, they repeatedly said that the assertion that the NSA was engaged in large scale surveillance of Americans' international communications under Section 702 was speculative and even paranoid.

And now the program has been disclosed and everybody can see that the NSA is engaged in exactly that. And the intelligence community, and I would include Mr. Wainstein in that category, the intelligence community's position now is that, well, this is what was contemplated by the statute. Everybody knows that this is what the statute was all about.

And you know, there's a certain

frustration I feel in this sort of moving target. You know, a year ago it was speculative and paranoid and now there's nothing to see here.

And it would trouble me less if it weren't part of a pattern in which the Executive Branch officials and members of the larger intelligence community have repeatedly misled the public about the scope of these surveillance laws and the safeguards that are in place or aren't in place to protect individual's privacy.

And on a related topic I think it's just very important, Mr. Bradbury points out quite rightly that under 702 the government can target only foreign nationals outside the United States but nobody should take that to mean that Americans' communications aren't being collected.

In the course of collecting the communications of people outside the United States the NSA collects Americans' communications. And not just their international communications, but their domestic communications as well.

That too, that assertion I just made was

something characterized by the government in Amnesty v. Clapper as speculative and paranoid but the minimization procedures that have been disclosed over the last few weeks I think make clear that that's exactly what's taking place.

MS. WALD: Kate.

MS. MARTIN: So I just want to reiterate that I think Ken illustrated the importance of the history in looking at these programs. I would disagree with his, and Steve's as well, description of that history.

I think that as Jameel mentioned, the important question here is not under what circumstances can the NSA collect and use communications by foreigners overseas.

The important question that we've always tried to focus on is under what circumstances is the NSA going to collect and use in secret information about Americans usually gathered inside the United States, including both metadata, which is extremely revealing of their associations and private life, and the content of their

communications, especially communications with people located overseas.

To repeatedly focus on or to state that the purpose of this surveillance is about foreigners overseas I think is confusing at best about the real issues that face the American people.

I just, I think the other issue that's underlying here is that it's not only a question of collection of course but it's a question of how the government uses the information. Many of those regulations are secret about how the NSA or the FBI is allowed to use them.

To the extent that there are public regulations they're extremely complex to figure out which set of regulations applies to which set of information, and that fundamentally I think they don't address the problem that the government is in a position perhaps to use information about Americans against Americans. And that's the issue that needs to be addressed.

MS. WALD: Jim.

MR. ROBERTSON: Perhaps two quick points. It is certainly true that a government request for business records is not a search, but I think we all need to pay attention to what Jameel said about this subject and about the Jones case, because modern technology enables analysis of metadata that was not possible before.

It reminds me of something that Ben Bradlee is supposed to have said about Woodward and Bernstein. He said if you give those guys enough steel wool they will knit a stove.

Secondly, as to Ken Wainstein's point that we got exactly what Congress asked for. That's true, but the brouhaha after the Snowden leaks, and this meeting indeed establishes what I think is true that we need to have a more wide open debate about this in our society and thankfully we're beginning to have the debate, and this meeting is part of it.

MS. WALD: Ken.

MR. WAINSTEIN: Thank you. I'd like to start off by responding to Jameel's suggestion

that I or others misled him in any way about the collection of U.S. person communications. That contention's flat wrong.

I spent fourteen, fifteen months with Steve and others up on Capitol Hill explaining the intricacies of the procedure that ended up being adopted, or a formula which ended up being adopted in the FISA Amendments Act.

We answered every conceivable question on the record and in meetings, in forums like this with privacy groups about the implications of this collection, and it was abundantly clear to everybody, and we said numerous times that this will be focusing on foreign targets overseas collecting their communications, whether those communications were overseas or also if the happen to come into the United States.

So what he's getting at is the concept of incidental collection. While you're targeting a foreign person, a non-U.S. person overseas, you'll get that person if he and she is talking to somebody in an overseas country. You'll also get

that communication if he or she calls somebody in the United States.

That's authorized collection and the collection of that U.S. person's communication is acceptable. That's what happens in any form of authorized collection.

If you look at Title III, which is the criminal rule that allows criminal wiretaps, the same thing happens. If I'm a criminal suspect a court authorizes a Title III wiretap on me, the government's also going to get the communications between me and the pizza delivery man when I call to get pizza, not only with other criminal colleagues.

So that incidental collection is a reality of any kind of surveillance and it's something that was fully vetted and made clear to the American people.

And then the second point I'd very quickly make, which is, you know, Kate talked about the collection and the use of this information in secret and the concern about how

this information is used.

I think one thing that's not touched on sufficiently is the value of oversight. You can take a look at the FAA in itself it prescribed four or five or six different types of oversight. And all these programs are carefully overseen by the FISA Court, by Congress and importantly within the Executive Branch itself and that oversight is very important and meaningful in terms of preventing abuses. Thank you.

MS. BRAND: Okay, thank you all. Pat and I will now ask some questions of the panel. We sort of agreed in a sidebar here that since we have a bit of time, I think we started a little early, we can be a little bit more flexible with the length of your responses to these questions, but let's try to keep it not beyond three minutes maybe. But we don't need to be so strict about it.

My first question deals with the relevance standard in Section 215. I'm particularly interested in all of your views about

that. So each of us will throw a question open to all of you so you can answer in turn, if you want. If you want to pass on the question, that's fine too.

Section 215 authorizes an order for tangible things that are relevant to an ongoing FISA investigation. And I have several sort of sub-questions related to that.

One is whether relevance can attach as the government seems to be asserting to the entire set of data or whether relevance needs to attach to any particular record that's collected.

And relatedly whether Congress, which one of those things Congress understood itself to be passing when it enacted Section 215, the kind of haystack approach or the relevance attaching to a particular record.

And then relatedly, and some of those of you with criminal backgrounds, I'd be especially interested how that compares to the way relevance is understood in the criminal context or even in the civil litigating context. Is this

understanding of relevance broader? Should it be broader?

So Steve, if you want to start with that.

MR. BRADBURY: Thanks, Rachel. Well, I began to touch on that I think in my opening remarks.

And of course individual members of Congress might say, well, I didn't have in mind this specific concept when I voted for something that says relevant.

But I think in adopting the word relevant Congress embraced a broader context in which that word is used embraced frequently and commonly in other situations, administrative subpoenas, for example, civil investigative demand by agencies that regulate industries can be extremely broad in concept of relevance.

Civil litigation, a lot of folks who are involved in civil litigation understand that a party in litigation gets a broad right. For example, it could encompass an entire database of information where particular items of data in that

database may be useful in the litigation and the parties work out an arrangement that maintains that database so that it can be searched for potentially useful documents. That's under a concept of relevance.

Grand juries have an extremely broad concept of relevance when they can go after any materials that are potentially relevant.

For example, after the Boston bombing where if there was a concern about follow-on attacks or collaborators, a grand jury could subpoena without court approval all airline manifests of flights in and out, passengers flying in and out of Boston in a particular period of time because one of those people on one of those flights might have been relevant. Communications similarly.

So I think the concept of what's relevant to an investigation is naturally understood to be broad in lots of contexts and I think it's reasonable that that's what was incorporated in the statute when Congress adopted it.

MR. JAFFER: Well, I agree with some of that, that relevance is, you know, a relatively broad standard, but there are haystacks and there are haystacks.

And if you just think about the examples that Mr. Bradbury just provided, for example, this hypothetical situation where a grand jury subpoenas the flight manifests in and out of Boston for a particular period of time, I mean that is not anywhere near the scope of the program we're talking about here.

And I think, you know, I can say with confidence, and I'm sure that everybody on this panel will agree with me, that there is no subpoena out there, there's no case out there in which any court has approved on a relevance standard surveillance on this scale.

This is, this takes us across a new frontier, maybe several new frontiers. This is orders of magnitude broader than any surveillance that has ever been approved under a civil or a criminal subpoena.

MS. BRAND: Can I just ask a quick follow-up to that since this panel is focused on the legality of the alleged current programs. Where would you draw the line then if this haystack is too broad but if your argument is not that each individual record collected needs to itself be relevant, what line do I exercise with the FISC engage in?

MR. JAFFER: Well, I don't think that it's possible to set out a line with any more clarity than to refer to relevance.

The surprising thing here is not that the court is applying a relevance standard, but that it isn't, that in spite of the statute's clear language that requires it to apply the same standard that applies with respect to ordinary subpoenas, the court has approved the government to collect everything. It has allowed the government to collect everything.

And you know, I think it's fair enough to say that relevance doesn't require the kind of specificity that probable cause does.

But everybody agrees that relevance is supposed to be a limit, and I think it's quite obvious that relevance isn't doing that work with respect to this kind of order.

MS. MARTIN: On the question of what did Congress and the American people understand with regard to the use of the word relevance, I think it's pretty clear that until this past month the American people had no idea that Section 215 relevance was being used to collect all of telephone metadata on Americans' phone calls, and I assume that it was also being used to collect all of the Internet metadata.

And I think the mere fact that, not only did we not know that, but our assumption during the debates on the FISA Amendments Act was that that was not happening, that that had been part of President Bush's warrantless program, it had been revealed and that it stopped.

I think a further indication of that is that in the bible, which I commend to you, on this statute written by Mr. Chris and Mr. Wilson, their

description of Section 215 orders during the relevant time period describes a very limited number of orders.

And if you were to read that description you would never suspect that the government was using 215 orders to collect millions or billions of records on Americans.

And finally in response to the question, Rachel, about well, what should be the standard? Of course 215 is about all different kinds of records. Some of them are more revealing than others. Communications metadata, both telephone and Internet I think are among the most revealing kinds of records covered by 215.

One possibility is to go back to what was in the law before 2001 and require a showing that the collection of communications metadata is connected to a specific suspect, a specific incident, a specific plan. That requirement was deleted.

And finally on the analogy to the criminal context, I strongly object to that

analogy. In the criminal subpoena context there are two key factors that are not present here.

One is that at least after the subpoena is served and sometimes during the service of the subpoena, it's public, and that leads to all kinds of restraints on its use, objections to use, etcetera.

And secondly, there is the possibility of true adversarial adjudication in the way that Judge Robertson talked about it in a criminal subpoena. That does not exist under Section 215 and will not exist even if you allow the recipient of the 215 order to go to the FISA Court, because the recipient of the 215 order is not the party that has the interest in the order. The persons whose information is being sought are the persons who need to have that right to show up in court.

MS. BRAND: My question about the criminal context wasn't so much whether it's a completely apt analogy but whether the relevance standard is the same.

I mean do you have a view on that,

whether the word relevant or relevance in 215 and the concept of relevance in the criminal context or in a civil litigating context are the same?

MS. MARTIN: You know, I don't know, but I don't think it's a relevant question, with all due respect. With all due respect.

MR. ROBERTSON: Well, I think your relevance question is a great question and I would love to know whether the FISA Court ever has considered the question when it reviewed the program.

Relevance is usually raised, it usually comes into question in a legal proceeding if there's an objection, but there's nobody there to object.

MR. WAINSTEIN: I'd just like to I guess make two quick points. One, add to something that Steve mentioned about you know, the statements that we've heard from members or former members of Congress saying, you know, gee, I didn't intend when I voted to 215 that it would apply in this way.

You know, that's just, just to make it clear, that's not unique to this situation that former or current members of Congress might now be voicing some concern that the way a statute is applied is not exactly as they conceived of it before passage of that statute.

You saw that with the authorization for use of military force back in 2001. I've seen it throughout my career with, for example, statutes like the Racketeering Influence Corrupt Organization Act, RICO, which was initially passed and many members thought it was going to be focused on primarily, if not exclusively, on traditional organized crime.

And then it has now been applied to a much broader swath of criminal activity, with many people saying, gee, I didn't think when we passed that statute that that's the way it was going to be applied. So just to make it clear, this is not an anomaly, this is a fairly common phenomenon.

And then I guess the second point I'd want to make is as to Kate's point. She argues

that the criminal grand jury subpoena is different and you can have more comfort in the government's use of those subpoenas and their interpretation of relevance for purposes of using one because these subpoenas will see the light of day ultimately.

And that's true for some cases, no question. Those cases where a grand jury subpoena is issued and that grand jury process ripens into an indictment which then goes to trial and the evidence is tested in court, then there's a good chance those subpoenas are going to be turned over in discovery and then tested in a suppression hearing or at trial.

But that's not always the case. There are a lot of grand jury subpoenas that I've issued over the years that never see the light of day because that sequence of events doesn't happen.

So just to make clear, that's not sort of a perfectly distinguishing feature that would break down the analogy between the grand jury subpoena and 215 which Steve made. Thanks.

MS. WALD: Okay. I'd like to delve a

little bit into the constitutionality of some of the facets of constitutional analysis of one or both programs, which will give you a chance to elaborate on some things that you may not have been able to catch up on the earlier segments.

We already talked a little bit about U.S. v Jones and whether some of the opinions of the Supreme Court justices, and in fact the majority opinion of the D.C. Circuit, which preceded the Supreme Court which suggested that in fact when you have an extensive surveillance of location in that case, but in a sense kind of metadata over a long period of time, it reveals enough of a person's personal life so that it may indeed constitute a search requiring Fourth Amendment compliance.

But there are a couple of other aspects and constitutionality that have been brought up, if you want to touch on them.

One is, I think this was raised by Senator Feinstein in some of the hearings, and that is whether or not there are less intrusive

alternatives.

In other words, it was brought up specifically with regard to 215 that do you have to seize, does the government have to, in the alleged program, seize the data or require that it have the data? Would it be less intrusive if it queried the data which was existing in the hands of the communications providers?

And in fact, the Executive Order 12333 which governs intelligence conduct activities generally, speaks of requiring the least intrusive collection technique feasible.

Whether or not it specifically applies to 215, we can debate that, but the general principle why isn't it sufficient that they query the communications companies which have the data, rather than requiring that they get all the data.

And indeed there's possible constitutional question about, and I think Kate may have raised this, if the alleged program that's under 215 is okay on telephone metadata then are there any inherent limits in 215?

I mean are there other kinds of metadata, the fact of bank records, the fact of various other kinds of records, are there inherent limits there?

Now what I have left out but I'm going to save it for my next question is the whole FISA Court area and what might possibly, following up on Jim's analysis, could anything be done? Is it better that we not have the government, we not have the court getting into programmatic analysis at all? If not, where are our protections going to be?

But that's the question for another day. In this case I'm giving a lot of grist for your mill.

Steve.

MR. BRADBURY: Thanks. Is that last question for another day or the next question?

MS. WALD: No, the FISA question.

MR. BRADBURY: I have a lot to say about that so I hope you do ask that.

MS. WALD: Well, I'll ask it now but in

that case everybody gets six minutes.

MR. BRADBURY: Well, on the Jones case I already talked about that.

But on your question, Judge Wald, about the database and would it be less intrusive if the telephone companies just maintained the database and what can we get with a business records order, I don't think it's a question of intrusiveness.

I don't think it would less intrusive. It would be far less efficient, far more costly, and perhaps less effective. You'd have to have multiple databases at the different telephone companies.

And they don't for business purposes retain this data for as long as the government needs it. This is just business record data they retain for billing purposes. They don't have a separate national security reason for keeping it.

So we'd have to create a database. They don't have all the servers and everything. So the government is going to have to create the database, which evidently under this alternative

would be housed with the private company, have to pay for it.

And of course the government would still have to control the querying because you're not going to tell the telephone company what queries you're going to do to the database. That's national security investigatory information. They don't need to know that.

And so it's far more efficient. The government already has facilities in place and it can segregate them. It can ensure that all of the protections are honored and that the data is not being accessed for other reasons, etcetera. So it's really an efficiency question.

In terms of --

MS. WALD: Just one slight follow-up question, a subordinate question. Is that, are some of those criteria you talked about, in your view more sort of convenience kind of things or are they necessity because when we're talking about constitutional analysis are they necessary to the feasibility or purpose for which the

program is related.

I mean the cost and that kind of thing sound a lot like convenience factors.

MR. BRADBURY: Well, I do think there are very real practical and feasibility requirements. I don't think the Constitution would see a difference between the data being housed with the government or the data being housed elsewhere but the government controlling it and controlling access and ensuring it's preserved, etcetera.

But 215 is focused on business records so you have to be talking about the kind of data or database information that a business is maintaining for its own business purposes.

So that may be very different with respect to the email that people have alluded to, email metadata under 215. Telephone companies maintain these call detail records for billing purposes and it may be very different in other contexts.

So I don't think you can just easily say, oh, well they must be using this for other things

too. These are business records that have to be in existence in a separate business, for separate business purpose.

Shall I leave the FISA Court questions for later?

MS. WALD: Let's do everything but FISA and then come back and do FISA.

MS. BRAND: Let's do constitutional now and then save FISA for another round.

MS WALD: Well, that is part of FISA.

MR. JAFFER: So just to point out the obvious, I think that the least restrictive means question is an important question and a question that the board should be asking.

But it assumes that the government has some overriding national security interest to get access to the information in the first place, that this information is somehow crucial to protecting the national security.

And that is something that I think many people have been pressing the intelligence community to corroborate, but thus far nothing

convincing has been said to establish that this information is actually crucial.

I understand that at one point the government pointed to the Zazi case. The Zazi case turns out not to have turned on that kind of information at all.

If there is some case out there to which this information was in fact crucial, I don't think the government has pointed to it yet.

But, you know, to go back to the question. If we assume that the information is in fact crucial then I think it's crucial to ask the question about the least restrictive means of getting the information.

And on that question I do have a problem with this centralized database, the creation of this centralized database in the hands of the NSA. And here I'll take the opportunity just to agree with something that Mr. Wainstein said earlier which is that authorities created for one purpose, it's not uncommon at all to find out later that they were used for some other purpose.

That happens all the time, and the same thing is likely to happen with this database. Even if it's true right now that the government queries it very rarely, that the queries are quite narrow, and that only 300 queries have been made thus far, even if all of that is true, and even if all of that satisfies you about the privacy safeguards that are in place right now, you don't know what those privacy safeguards are going to look like three years from now or five years from now.

If there is another significant terrorist attack you can imagine the pressure that members of Congress will come under to change the parameters or the intelligence community will come under to change the parameters that govern access to the database.

And that massive database of American's most sensitive information will be forever available to the intelligence community to access under whatever standards prevail at that particular point in time.

So that's just to say that there are problems that arise from the existence of this kind of centralized database.

MS. MARTIN: So I think the truth of the matter is, as you know, that the Supreme Court hasn't answered these questions, that if you start from the understanding that in order for the government to seize or obtain information inside the United States it needs to meet Fourth Amendment requirements, then you end up in one place.

If of course there are many situations in which the Fourth Amendment has been held not to apply to government seizures of information. I think that as Jameel says the ability for the government to obtain information and create massive databases raises serious constitutional issues not yet addressed by the court.

They're not just Fourth Amendment issues, they are also First Amendment issues about the impact that that has on people's exercise of their First Amendment rights.

I think the other constitutionally significant fact is that the seizures are being done in secret. And I know that some of us who worked on the 1994 amendments to FISA which allowed secret searches of American's homes and offices, but in a particularized way with a particularized warrant objected though to that authority because it allowed secret searches of American's homes and offices which would never be revealed to the people whose homes and offices had been searched.

That 1994 amendment was enacted before the Supreme Court held in the criminal context that notice of a search was constitutionally required and not just required as a matter of the criminal law.

So one of the questions is the applicability of that basic understanding to this kind of search and seizure.

And I think on the question of less intrusive alternatives that Jameel is correct, but the initial question is what is the purpose? Less

intrusive than what?

There is no doubt that if the government is able to create as large a database as possible and use as sophisticated analytics as possible that it will be able to generate information that will be useful from time to time in combating terorism. There is no doubt about that. And in fact, we've seen that in other countries. I don't think that's the question.

I think it's a much more complex question. I think it requires looking at the actual threats that the United States poses, including the scope of those threats, looking at the different ways to meet those threats and looking at the different alternatives that exist other than creating a database that's always available to query.

MR. ROBERTSON: I don't have I think a very useful view on least restrictive alternatives or on permanent databases versus accessing the databases that are in the hands of the vendors.

But I have to tell you that what keeps

running through my mind as this conversation is going on is that this is not only a First Amendment problem and a Fourth Amendment problem, but NRA members, a Second Amendment problem. It is exactly the argument you'll get from the NRA about permanent records of gun ownership. Think about that.

MS. MARTIN: Which are not permitted of course.

MR. WAINSTEIN: I'm not going to bite on the Second Amendment issue. I'll leave that one for another day and another panel.

But I do want, you know, Jameel expressed some agreement with me, and we can't allow too much agreement between Jameel and me so I'm going to have to put a stop to that.

But he did, he made the point that, yes, you put legislation in place and it adapts to the situation and it adapts to the needs at that time. That's the way legislation is supposed to be imposed and that's why you have courts to make sure that any adaptations remain true to the

original intent of the original legislation.

But I guess what I find concerning is the notion that if you have a strong but lawful and appropriate investigative tool in place now, that you should think twice about maintaining it because of some speculative concern that down the road it could be misused.

I think that's a recipe for disaster. I think if we were to take that approach we'll end up walking right back into another 9/11. I don't think that's exactly what was suggesting, but that is a concern you see in some of the opinions out there in the real world.

I think what instead we need to do is exactly what I believe we learned over the last decade, which is the value of oversight. And oversight, as a government employee, I'll tell you it drove me crazy because I spent half my life running up to Congress answering questions, talking to the FISA Court about their various concerns and questions. And I would have much preferred to stay in my office and work. And many

of my former colleagues who are here today probably feel the same way.

But we learned the importance of that oversight and making sure that these things, these legislative tools stayed true to the legislation, true to the Constitution. But also because it helped to ensure the confidence of the American people when they knew that that oversight was effective and strong they had confidence in those tools.

So instead of taking the approach of scaling back on the strength of appropriate investigative tools now out of some speculative concern of misuse in the future, just make sure you build in the safeguards and the oversight that will prevent that kind of misuse.

MS. BRAND: Thank you. I'm going to go back to the statute again, and I apologize if this seems like a quiz, but I want to get the benefit of your views, to the extent that you can provide them.

So if you look at section -- my question

is whether Section 215 can be interpreted to allow the government to get ongoing production of not yet created business records?

So the document that purports to be a leaked 215 order would authorize, would require the company to provide on a daily basis records at a future date. So they haven't yet been created.

And the language of Section 215 authorizes that production of any tangible things, etcetera, even though this doesn't use the term business records, everyone understands this to be a business records provision.

Later in the section there's a proviso that it can only require the production of a tangible thing if such a thing can be obtained with a subpoena duces tecum, etcetera, grand jury subpoena. So I'd like your thoughts on that.

And relatedly there is two sections earlier in FISA, there's a pen trap provision, right, which also is based on a relevance standard. Pen traps, as everyone knows, are inherently sort of ongoing and real time, unlike a

business records subpoena.

In light of the existence of that provision and the limitations of the language in 215, do you think that if this leaked order is actually correct, the language of 215 permits that?

MR. BRADBURY: Yes, I think it does. I don't think the statute in talking about tangible items distinguishes when the tangible item is created.

I think there are a lot of production orders under a relevance standard that require ongoing production of relevant materials. That's common in litigation. It can be common in administrative investigation.

The items are created and are records by the time they're turned over, and the order is focused on a known existing category of records that are constantly being refreshed. But they are tangible, they are in existence. They are business records when they're obtained under the order. So I don't think that's a distinction the

statute requires or points to.

In terms of pen registers, trap and trace devices, that's a different technology. That's for when communications are occurring you're picking up the addressing information, the calling party number, etcetera. So those pen registers would be somewhere out in the network or on the switches, etcetera, in real time collecting all of the calling party number type information when calls are being placed.

And this is a business records order because it's actually with the telephone company it's much more efficient to go to their existing databases where they maintain this, the information you're looking for, for billing purposes.

Can I just say one quick thing? Jameel has useed the word surveillance in describing this 215 order. This is not surveillance. Surveillance is a defined term under FISA. That includes getting the content of communications usually when they're being transmitted across a

wire, for example.

This is not content, this is just metadata. It is not surveillance and it's not accurate to use the word surveillance. Thanks.

MR. JAFFER: I think that people can decide for themselves whether it's surveillance or not, in the same way they can decide for themselves whether or it's torture or not. You know, the statutes can define these things but the terms also have ordinary usage.

You know, I have a different view of how the statute can be read. I don't think that the statute was meant to allow the government to require the production of records on an ongoing basis.

If you take grand jury subpoenas as the relevant comparison, I don't think it's typical for grand jury subpoenas to require ongoing production in that way.

And if you look at the legislative history of the statute there is no hint in the legislative history that anybody considered the

possibility that this statute could be used for the purposes it's now being used for.

In fact, there was this testimony that then Attorney General John Ashcroft gave to Congress I think way back in 2004. It must have been 2004. And he was asked about the outer limits of the Section 215 authority, and at one point somebody asked, you know, could it even be used to require the production of DNA? And he said yes, I suppose it could. And that was sort of the outer limit.

But nobody ever suggested, nobody even asked the question, you know, could it be used to require ongoing production of any of these things you just said it could be used to compel the production of. Nobody even contemplated that possibility.

So you know, I don't think that the statute can be read that way. I don't think that members of Congress who are advocates of this particular provision thought it would be read that way.

And Representative Sensenbrenner, who is often thought of as the grandfather or the father of this provision has spoken out over the last few weeks saying that it had never occurred to him that it would be used in this way.

So I think that there's really very, very little to support the proposition that the statute is now being used for the purposes it was designed for.

MS. MARTIN: It seems pretty clear that the government has argued that Section 215 can be read this way and that the FISA Judge has agreed with that argument.

And I would, in order to evaluate and respond to that argument, I think it should be disclosed and then we can have a discussion about whether or not that interpretation by the government and the FISA Court is a reasonable or a correct one, especially given the existence of overlapping authorities under FISA for pen trap collection.

MR. ROBERTSON: I'll pass to Ken.

MR. WAINSTEIN: I'll just second what Steve said.

MS. WALD: Okay, back to FISA. This is a three part question. Maybe we'll open with Jim and then everybody will get a chance, but since he covered this in his opening remarks.

My initial question is whether or not judicial, effective judicial review is necessary to the constitutionality of a program or a statute. That's a general overview question, as one of the ingredients.

But Jim, you felt that the court really had no legitimate role in passing on programmatic issues, as opposed to the individual applications.

And so to you, I'm directing the question, what would you put in their place? If you took that particular kind of review away from the FISA Court would you be happy with just leaving it with congressional oversight and internal governmental, or what would you do?

And the third question to all of you,

including Jim, it's been suggested and in some of the comments today too, that maybe you could beef up the FISA Court by having some kind of an ex parte, whether you call it amicus, ex parte, somebody representing the interests of the people involved who don't even know that they're the subject of a FISA Court proceeding, how that would work.

But one other, the other one would be on appeals. I mean technically the only people that can appeal a FISA order of this type is the government, if it doesn't get what it wants, or the holder of the records, although many of them complain that they feel that they are hindered because they don't even have access to the secret targeted, original targeting record, so that all they're getting are tasking orders. And so they don't know. They don't feel that they're equipped to do that, even if it was in their interest to do it.

But even more specifically the question has been raised in Congress about, and Kate raises

it again, is there some way that we can find out what the FISA Court does, because the majority of its opinions are secret.

I think in the last congressional reauthorization last December there was a request made and sort of a promise given that they would see, the government would see whether or not some form of redacted order, some form of redacted orders or opinions could be given, but as yet that hasn't happened.

The question of whether there's some form of declassification which would give us the benefit of what the legal analysis is, especially when you are dealing with a program of great magnitude such as the 215, alleged 215 program appears to be.

Okay, take it away.

MR. ROBERTSON: Well, that's about a quint part question I think.

MS. WALD: I sneaked it in.

MR. ROBERTSON: But let me take the last part of it first. I was frankly stunned when I

read the other day that Eric Lichtblau story --

Sorry. I was stunned when I read Eric Lichtblau's story about the common law that's being developed within the FISA Court because I frankly have no familiarity with that. And everybody needs to understand that it was eight years ago that I was on the FISA Court.

But in my experience there weren't any opinions. You approved a warrant application or you didn't, period.

I think there was one famous opinion that was reviewed and reversed by the court of review back in 1902. But a body of law and a body of precedent growing up within FISA is not within my experience. And I don't know what the answer to that question is, how we get hold of it.

I'm more comfortable dealing with your question about should there be some sort of an institutional amicus or opponent that deals with FISA issues.

And I think I would like to say the answer is yes. My problem is I don't know what it

would be or exactly how it would work.

I wasn't kidding when I suggested that perhaps some tweaking of the statute establishing the PCLOB might make the PCLOB that institution. But you're not going to ask for that and I don't know who it would be.

There is, for example, within the defense department a group of people who are dedicated to the defense of detainees at Guantanamo. They are defense lawyers defending detainees that are being prosecuted by the other part of the defense department.

So it is, there is some precedent for it. Whether there would be some institutional office adverse to the office that brings these applications to FISA or not, I don't know but it's conceivable.

I'm going to pass on your question of the big constitutionality. I don't think the FISA Court itself, I'm not even sure they have the jurisdiction to pass on the constitutionality of the statute that they're carrying out. But I'm

not aware of any constitutional challenge to the FISA statute that's ever been brought before the FISA Court itself. It's got to be handled I think by Article III courts.

I don't know if that answers all of your questions.

MS. WALD: Well, it goes part way. Thank you.

MR. ROBERTSON: Part way.

MS. WALD: The rest of the panel, anybody that wants to take a whack at any part of the quartite question.

MR. BRADBURY: Sure, I'll take a whack. In terms of whether judicial review is required by the Constitution, well to the extent the Fourth Amendment in a particular situation requires a warrant supported by particularized probable cause approved by a judge, then yes, judicial review is necessary.

And of course in the classic warrant context it usually is ex parte. The government comes in with an application with an affidavit and

a judge signs a warrant without an opinion often, typically.

And the FISA Court is analogous to that model. And there are a few very small number of opinions but as Judge Robertson suggested, most of the time it's an elaborate application, it goes back and forth, and then it's finally approved by the court with the judge's signature. There may be memos internally at the court analyzing issues.

I do think that Bob Litt, the general counsel of the DNI said in a congressional hearing the other day that they're scrambling, and I imagine they are, to declassify as many applications and prepare white papers and explain legal analysis to the extent consistent with national security. And I think they're doing that.

In terms of replacing the court involvement, I think that again we need to understand the constitutional background is that foreign intelligence surveillance until 1978 occurred without court involvement.

It was a unilateral action of the Executive Branch that led to lots of abuses and something the authority being used focused on domestic targets.

FISA was a big compromise between the branches to bring courts in, and to the extent feasible and consistent with national security, to involve a court, like a warrant type situation in approving surveillance, types of surveillance that used to happen without any court approval.

And then to create the intelligence committees on Congress for so Congress could be briefed in, in secure facilities, etcetera.

And that's, it is a very unusual animal and I agree with Judge Robertson that it raises some significant questions, for example, with programmatic approvals under 702.

But prior to 702, the FISA Court was overwhelmed with individualized orders focused on foreign targets. It was just the court didn't understand why it was spending so much time worrying about non-U.S. persons' privacy outside

the United States.

So the 702 process was intended to make it easier where it's just focused on foreign targets to collect those communications in and out of the United States to those targets.

So it's workable. I think it's a great story that Congress passed this legislation. And when Congress did pass it and consider it, all members of Congress were given the opportunity to be briefed on all the classified details of these programs and all the members of the intelligence committees were briefed.

Finally on the amicus participation, I'm not sure that's feasible because the amicus would have to know the classified details of the particular surveillance request and what's up.

I mean the court is witting of all, of lots of detailed classified information supporting the probable cause determination or the reasonable suspicion determination and the context of the surveillance. The amicus couldn't, there's not a feasible way for --

MS. WALD: Even with a security clearance? I mean for instance in the detainee analogy that somebody raised, I mean the government has a defense layer, as it were, and they do have security clearance, I don't know, that allow them to --

MR. BRADBURY: That's right. But number one, the defense lawyer is only given access to what the government is going -- is what's relevant to that particular prosecution.

And the government of course always has the choice not to prosecute if the disclosure of some particular information to defense counsel is too worrisome.

In this context we're talking about doing surveillance of the most sensitive threats based on the most sensitive national security information, and the Executive Branch is only making it available to the court and to the congressional committees because it's required to by statute.

And it's so sensitive that you'd need to

have an amicus that's really a permanent. It would probably have to be an officer of the government, whether of the court or of the Executive Branch that would be fully participating in the process and cleared into the same things that the court receives.

MS. BRAND: Just to inject one other idea into your comments perhaps, and this has sort of been alluded to, but the federal public defender's office is part of the judiciary essentially, employees of the judiciary hired to oppose the government and I wondered if something like, a model like that would be feasible?

MS. WALD: How about some other panel members on anything they want.

MR. JAFFER: So I think in the usual case before the FISA Court it would be good to have somebody with access to classified information who could play an adversarial role within the process that already takes place.

I'm not convinced that with respect to broader legal questions like is it consistent with

the Fourth Amendment for the government to collect all American's telephony metadata. I'm not convinced that that kind of question has to be decided behind closed doors.

I don't see why the court couldn't articulate that question publicly, notify the public that it was going to consider the legal implications of a proposal to collect all American's telephony metadata, and allow anyone who wanted to, to file an amicus brief.

I think that Mr. Bradbury starts from, I think it's clear, a different assumption than I do. His assumption is that everything that is classified and that has been classified is properly classified, and that is not my view.

My view is that a lot of these programs, well, some of the programs that have been disclosed over the last few weeks and the last few years should never have been secret in the first place. They should have been disclosed to the public, at least the general parameters of the program should have been disclosed to the public,

both because it's important that the political leaders who put these programs in place be held accountable, but also so that the judicial process can actually function in the way that it's supposed to in an adversarial fashion.

And then you know just to expand on something that Judge Robertson said earlier, you know if we're asking the question whether FISA, whether the oversight of the FISA Court is sufficient I think it's important to keep in mind that there are structural limitations on what the FISA Court can do.

So even apart from these questions about, you know, is it appropriate that the Chief Justice of the Supreme Court appoints all of the FISA C judges, even apart from questions like that there are structural limitations on what the FISA Court can do.

And some of those have to do with the court's jurisdiction. The court doesn't have the jurisdiction to consider First Amendment implications of the government's proposed

surveillance. It doesn't have the jurisdiction to consider the facial validity of a statute like the FISA Amendments Act. And the court itself has said that in one of the opinions that was made public a few years ago.

And the court doesn't have the authority to consider the constitutionality of the limits on its own jurisdiction.

One of the arguments we made in Amnesty v Clapper, which was our constitutional challenge to the FISA Amendments Act was that the role that the court was playing with respect to surveillance under Section 702 was different from tthe role that Article III courts are permitted to play under the Constitution.

They weren't considering individualized suspicion allegations. They weren't making determinations of probable cause. The government wasn't appearing before the court identifying proposed surveillance targets or proposed facilities to be targeted.

Instead the court was making these, and

is making these judgments about the appropriateness of the government's programmatic procedures relating to targeting and minimization. And that's something that no Article III court has ever done in the past and is quite foreign to the kinds of things that Article III judges are accustomed to doing.

That argument we made before, initially before a judge in the Southern District of New York, but it wasn't heard because our plaintiffs were found ultimately to lack standing.

But the point, the narrow point I'm trying to make is just that that is a question that the FISA Court doesn't even have the jurisdiction to consider. The fact that other courts aren't considering it, I think makes it all even more problematic.

MS. MARTIN: So I don't know the answer to your question, Judge, but I do think it's important to distinguish and probably limit the role of the FISA Court.

I think that it was created, as Judge

Robertson said, to issue warrants in the way that judges have always issued warrants.

The fact that it is now creating a body of common law is extraordinary, and I'm not sure that is an appropriate function of the court.

The fact that that body of common law is being created in secret of course compounds the problem of it being created ex parte.

And the fact that the administration, although I take that their promise to try to disclose more information is sincere, I wish that they would work on that before they described to the New York Times and the Wall Street Journal legal opinions which are still classified. We could use the legal opinions themselves.

But fundamentally I think we need some kind of system where a traditional Article III court, not the FISA Court, is looking at these questions that have to do with what does the law allow and what's constitutional.

And I just in that connection want to push back on the notion that somehow this might be

legal even without court involvement because it was done that way before 1978. I disagree with that.

But I think more importantly is that we mustn't forget that during the Bush Administration when the FISA statute was exclusive, it explicitly said you may not conduct this kind of surveillance except pursuant to a FISA Court order, and if you do so it is a crime.

The Bush Administration in secret violated those provisions and made up a series of flimsy legal arguments for doing so. But most of all, forgot to tell the American people that it was taking the new view that it was no longer bound by FISA. And we only found that out as a result of leaks to the press, which is not the way the system should work, you know.

And similarly, just because Mr. Wainstein keeps talking about the efficacy of oversight here. We have a situation during this administration where two members of the oversight committees have repeatedly raised questions about

what was happening. They have been repeatedly blocked from bringing those questions to the public. And now here we are as a result of an unauthorized leak.

MS. WALD: Okay, Kate. Ken, you get the last word, right of reply.

MR. WAINSTEIN: Okay, thank you very much, Judge. I'd like to address the amicus idea, the idea that there should possibly be some other party that would take the side of the person who's to be surveilled in a particular FISA application.

A couple of points to keep in mind. One is something that Steve mentioned a few moments ago. Keep in mind that the notion of a judge receiving and assessing an application for a search is not new.

As Steve said, this is exactly what we do in the criminal side. When I go to judges like I did with Judge Robertson to get a search warrant as a prosecutor, or to get a Title III wiretap warrant against somebody, that was done ex parte.

It was the prosecutor, maybe the agent and nobody on the other side, nobody representing the person whose house is to be searched or the person whose telephone calls were to be listened in to. And that's the paradigm and I think it's important to keep that in mind.

You might see, you might be able to sense a theme of mine, which is that this construct on the national security side for these investigative activities all is drawn from parallels and origins on the criminal side. So this idea of an ex parte consideration of warrants is not something that's out of the ordinary. In fact, that is the norm.

And the point of that of course is that we trust judges. We trust the judges to look, you know, scrutinize the showing, and in the case of a warrant to make sure that there's probable cause to support that warrant.

And I can tell you from experience that judges on the FISA Court, they are Article III judges they are, you know, contrary to what some people have suggested not at all in the

government's pocket. They are very independent and they put us through our paces to make sure that what we give them measures up to their standards and the standards in the law.

But keeping those two points in mind, the idea of some sort of counter-party is an intriguing one. I think Steve's right that there are a lot of practical issues with that in terms of the sensitivity of the information that the FISA Court judges see. They see the most sensitive information in the intelligence community.

But to the extent that that would help establish greater public confidence in the process, I think is something that the board and others should look at, whether it's practical or not, it's hard to say.

In addition, Kate mentioned the concern about the transparency. You know, same point there. To the extent that the government can be more transparent with its legal theories, or if the FISA Court, and I don't know whether it can

because I haven't seen any of these opinions, but if the FISA Court can disclose some sanitized version of these opinions, it's just good for public education, but it's good because these programs only work so long as we have the confidence in the American public that they're being conducted honestly and reasonably and consistent with the Statute.

MS. WALD: Thank you.

MS. BRAND: Thank you. My clock here says 11:17. We're scheduled to go to 11:30, I believe. Do the other members of the panel have questions?

MR. MEDINE: Yeah, I have a question about the 702 program. Steve and Kate have touched on it.

Under that program by definition the target is non-U.S. persons outside the United States, but of course inevitably some of those conversations are with U.S. persons in the United States.

My question is whether that raises a

Fourth Amendment issue by collecting and using that information involving U.S. persons, and if so, are the minimization procedures in place sufficient to meet Fourth Amendment concerns?

MR. BRADBURY: Well, I guess I'm going to go back a little bit to history again. There's been some discussion, Ken mentioned changing technology, you know prior to 1978 and when FISA was first enacted almost all international communications in and out of the United States were carried by satellite, not even covered by FISA.

Over time that migrated to fiber optic cables in and out of the U.S. Suddenly if you're conducting that surveillance on a wire in the U.S., even though it's international communication, suddenly it's covered by FISA, individualized orders required. And that was okay. It was workable.

But then 9/11 hit, huge problem. We suddenly needed to know about all suspicious communications from thousands of potential

terrorist dots outside of the United States. When are they communicating in or out of the U.S.

Of course that led to the President's special authority to conduct that surveillance. Very controversial, the disclosures, the debates.

Congress grappled with it, ultimately resolved on a statutory solution, 702, which again is targeted at non-U.S. persons reasonably believed to be outside the United States.

But it is particularly focused on communications in and out of the United States because just as it was right after 9/11 when the President gave that authorization, those are the most important communications you want to know about if you're talking about a foreign terrorist suspect communicating to somebody you don't know inside the United States, potential planning, etcetera.

And 702 enables court involvement, review, approval of procedures to ensure the targeting is focused outside the United States but I don't think the Fourth Amendment and the

particularized warrant requirement of the Fourth Amendment would apply to those communications if you're targeting a non-U.S. person reasonably believed to be outside the United States just because some of the communications happen to come in and out of the U.S. if you're not focused on a U.S. person whose privacy interests you're attempting to invade.

And whenever you do get into that sphere FISA specifically requires individualized surveillance orders that are very much like warrants, supported by probable cause.

Although I still wouldn't say they're warrants because it's not probable cause to believe a crime is being committed or has been committed. It's focused on use of a facility.

And it's also important to remember that 702 is not limited to terrorism and counterterrorism. What Congress authorized in 702 is any foreign intelligence gathering purpose, so it can be much broader. And it's not, it's actually much broader than the President's special

authorization in that regard.

MR. JAFFER: Well, the government conceded in Amnesty v Clapper that surveillance that takes place under 702 implicates the Fourth Amendment and requires the government to establish reasonableness. And in fact, they filed a summary judgement brief in the district court explaining their view that the statute was reasonable, in part because of the minimization procedures that you just referenced.

You know at the time we didn't have the minimization procedures so it was very difficult for us to answer that argument.

Now we do have the minimization procedures, and one thing that's clear from the minimization procedures is that the use of these words, incidental and inadvertent is highly misleading.

The collection of American's communications under this statute is not incidental or inadvertent. As Mr. Bradbury just said, those are the communications that the

government was most interested in. The minimization procedures allow the government to retain all of that information, if it's foreign intelligence information, forever. Even if it's not foreign intelligence information for up to five years.

The procedures allow the government to collect and retain and disseminate attorney, client communications. There are some are restrictions for communications between attorneys and clients who have been indicted in the United States, but that's a very narrow category compared to the larger category of attorney, client communications more generally.

So the statute was designed to allow the government to access American's communications. The procedures reflect that design. And the government has conceded that the Fourth Amendment is not irrelevant to the question of whether this statute is lawful or not.

So the I think you're asking the right question. My view is the answer to your question

is the minimization procedures are insufficient, insufficient to protect American's privacy.

MR. MEDINE: Steve you want a rebuttal?

MR. BRADBURY: Can I just say one quick thing? If I said this I misspoke. I did not mean to say the Fourth Amendment is irrelevant or does not apply.

I think what I said, what I meant to say is the warrant requirement in the Fourth Amendment wouldn't apply. It would still have to be reasonable under the Fourth Amendment, and that's a special analysis in the foreign intelligence context.

MS. MARTIN: Well, I would agree that the Fourth Amendment applies and I think there's a serious question about the applicability of the warrant requirement when the seizure is taking place in the United States, the seizure is deliberately intended to obtain the communications contents of Americans located in the United States.

And the argument that was made during

consideration of 702 is that the reason why you didn't need a warrant was that an American talking in the United States to somebody else doesn't know whether or not their conversation is being eavesdropped on because that other person could be the subject of a warrant and could be wiretapped.

But what you do know and what you, I think, have a right to know is that if you're communicating inside the United States with someone, the government's not collecting the contents unless it has a warrant on you or a warrant on the person you're talking to. And so that's not the case under 702.

Then the question becomes, well, what about the practicalities? How do we do this? And I would urge the board to look at proposals that have been talked about by ex-NSA officials which basically would set up a system where by the information might be acquired by the computers but before the government could access the communications of Americans, it would need to go back to the FISA Court and make a probable cause

showing and get a FISA warrant.

MR. ROBERTSON: That indeed is one of the recommendations of the Constitution Project report that I mentioned when I made my opening remarks.

This concept of minimization, minimization is one of the great classic euphemisms of our time. Nobody really knows exactly what it means and I think the board could profitably study that subject in great detail and for weeks.

MR. WAINSTEIN: I'd just like to clarify one point Kate mentioned and I might have the phrasing a little bit wrong, but you know, some of these surveillances under 702 could be intended to collect communications of person in the U.S.

Just to make clear, there's actually a specific provision in 702 that says you cannot do reverse targeting. I think, David, you mentioned that.

So that you cannot, the NSA cannot target somebody who's overseas for the purpose of collecting a communication within the United

States. What 702 does permit, and this is I think Kate and I are on the same page on this, is you can target somebody who's overseas, knowing that you're going to collect his or her communications with other people overseas, but also with communications that are inside the United States, which often, as Steve mentioned, are the most valuable or most concerning communications because they might indicate the existence of the plot.

But just you have to keep in mind that if you were to try to impose a warrant requirement, we discussed all this in the lead-up to 702. If you try to impose a warrant requirement of some kind to protect the communications of the U.S. person who might be communicating with someone who's rightly targeted overseas, then that same notion would apply to, presumably apply to our 12333 collection around the world.

You know, and FISA was drafted specifically to work around that collection to make sure that didn't get hindered by the FISA order requirement. And obviously the same thing

could to Title III. And so it would be a major paradigm shift in our collections.

MR. MEDINE: A quick response from Kate.

MS. MARTIN: I just want to, I think Ken and I would agree that the reverse targeting provision in 702 prevents the government from using 702 surveillance in order to obtain the communications of a specific known American.

But if the intent of the government is to target someone overseas in order to find out and obtain the communications of people that are in the United States who are talking to somebody overseas, that is the purpose of 702.

MS. BRAND: We're almost out of time for this panel but I know Beth has one question. I don't know if Jim has a question, but if we can --

MR. DEMPSEY: I'll just make a comment but go ahead.

MS. BRAND: Okay, then go ahead. If we could just make it very, very brief.

MS. COLLINS COOK: I was actually at the risk of assigning homework going to ask that you

all consider my question and if you are so moved provide information afterwards to keep us on track.

This is following on some of what we've been talking about, and Kate, you came close to what I was thinking about. But looking at what happened in 2006 with multi-point or roving surveillance, when there was some uncertainty as to how an authorization that was granted by the court would be implemented in a given case, a return requirement was imposed.

And my question is whether or not when you're dealing with these more programmatic or bulk authorizations whether it would be appropriate to impose a return requirement through a statutory provision. So whether it's for 702 or whether it would be for this, to use y'all's phrase, programmatic collection under 215 of business records.

So I would appreciate your thoughts on that and I will also pose this to panel three, so y'all should come back for panel three and

hopefully folks will have some opinions on that.

MR. MEDINE: And just to add to Beth's point, 702 provides for judicial review of directives and the question is can the judge's actually review specific targeting requests or only just the broad program as well? And if not, should they be able to under 702?

Jim.

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

I have an observation and I have some homework as well. My observation is up until the very end we really only heard one concrete recommendation for what might be changed, which was Judge Robertson's suggestion which a number of the witnesses engaged with about creating at least for some of the activities of the FISA Court some adversarialness to the process.

I'll just say that I really think it's incumbent upon the civil liberties community, of which I consider myself part I guess, but really incumbent upon the civil liberties community to

develop some concrete recommendations for moving forward here.

It might be that your bottom line is the 215 program is inappropriate and should be ended completely. But I think that whether it's 702 or 215, you really have to get more granular and more specific in terms of some concrete suggestions.

Now at the tail end we started to get to another one here which was this idea that's apparently reflected in the Constitution Project report about acquisition versus then a second search, a search, the particularized search. That's another concrete change.

I'll say one thing to Steve and to Ken. I think it's very important for people like you to engage in that process as well. And again, Ken started to at the end in terms of engaging with the idea about the adversarial process.

The way this was set up it was a little bit we have two critics of the programs and two defenders of the programs. I really think that there's a role for former government officials to

play. It can't be that everything is perfect. It can't be that no changes can be made, that no additional improvements or checks and balances or controls, etcetera can be made.

And a little bit I know you're put in this position of somebody says it's terrible and you've got to say it's great. I really think both the civil liberties community has to be more specific in its criticisms and its forward looking suggestions, and I think former government officials, including those who helped design these programs have, I think, a role to play in offering concrete suggestions for how to improve them.

And then my sort of follow-up, my homework assignment, I guess to take Beth's term, I would like to see more specific engagement on the question of minimization.

Judge Robertson is a hundred percent correct in terms of the misunderstanding at least, or the use of that term in a way that it becomes a mantra and no one really has dug in on that. There is a document online, whether it's valid or

not, whether it's still right or not, I think there's a document online that, assuming that minimization procedures looked like what is in that document, what's the reaction to them? How do they play out here? Is it good, is it bad, is it indifferent?

Secondly, I think there's some follow-up to be done on the legislative history of Section 215. Everybody talks about relevance. Relevance didn't come into the statute until 2005. In 2001 the statute said the documents are sought for an authorized investigation. Relevance came in 2005.

And I think it's worth thinking about what was the possible intent of Congress in shifting from sought for an investigation to specific and articulable facts giving reason to believe that they are relevant to an investigation. Did that have any impact? Should it be viewed as having an impact?

And then on the Zazi case I would like to see some, whatever there is on the public record

in terms of Jameel had mentioned that. I'd like to see somebody dig in a little bit and spell that out for us.

MS. BRAND: Thank you. Thank you, Jim. We're out of the time, unfortunately. But thank you to all the panelists for being here.

As I mentioned before, anyone on the panel or in the audience is welcome to submit written comments. Diane Janosek or Sue Reingold can give you the details on how to do that. Thank you.

MR. MEDINE: And thanks. We're going to take an hour break for lunch and we'll resume at 12:30.

(Off the record)

CERTIFICATION

I, LYNNE LIVINGSTON, A Notary Public of the State of Maryland, Baltimore County, do hereby certify that this is a verbatim transcription of the proceedings; that this transcript is a correct and accurate record of the proceedings, to the best of my knowledge, ability and belief.

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 _____ 2013.

_____

Lynne Livingston

Notary Public

My Commission Expires December 10th, 2014