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 terrorism. 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 used 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 the 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 surveiled 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)

MR. MEDINE: Good afternoon. We're going to begin the second session of our program today and this is the section that will focus on technology issues.

Jim Dempsey and I will be co-moderating this. And I'll turn it to Jim to make introductions and kick things off.

MR. DEMPSEY: So good afternoon again

everybody, and thanks to our afternoon panelists as well for giving their time to us on this important set of issues.

Our panelists for the afternoon are four of the leading experts, and sort of one of the questions or one of the challenges facing the PCLOB, which is bridging the gap between technology and policy.

So we have Steve Bellovin, currently a professor in the computer science department at Columbia University, many, many years at Bell Labs, one of the country's leading experts on computer security issues, as well as other issues at the intersection of technology and policy.

Secondly, is Marc Rotenberg, long time president and head of the Electronic Privacy Information Center, and again a nationally and internationally recognized expert on privacy issues.

Ashkan Soltani is an independent researcher on privacy and security issues, among other things was a consultant to the Wall Street

Journal on its extensive series of articles on Internet privacy issues.

And finally, Danny Weitzner, currently at the computer science and artificial lab at MIT, former White House science and technology policy advisor, co-founder of the Center for Democracy and Technology, and again, a long time participant in these debates.

So again we will adhere to the rules we established this morning, five minute opening remarks from each of the panelists, followed by a two minute response by the panelists to comments made by their fellow panelists and then questions by the Chairman David Medine and myself.

And as with this morning and as with members of the public, the record of this proceeding will remain open until August 1.

Several of the speakers on the second panel have already submitted either final or draft comments, which we're grateful for, but they will have, like everybody else, until August 1 to, as they say on Capitol Hill, revise and extend.

So Steve, please.

MR. BELLOVIN: Thanks, Jim. And let me add a brief disclaimer, I wear many hats in this town. Today the only one I'm wearing is as a private citizen, nothing else.

And what I'm going to be saying is based on my draft remarks. You have copies of them but for anyone else, they're already on my web page. You can find it easily with your favorite search engines.

But these are draft remarks, draft comments. I need to just make sure I've got the facts right, let alone my analysis in writing. So take it with a grain of salt, this is still a draft.

So I'm a computer scientist, not a lawyer, but it means when I look at a system, I look at it from a technical perspective. And when I see a system the first two questions I ask are, why was it built that way and what else can I do with it?

And you can say that that's my training

as a computer scientist, alternatively that's why I became a computer scientist because that's in my personality. Gee, shiny, pretty, what can I make it do?

As a privacy scholar and technologist, I also know that one of the things that's the biggest problem in privacy is not the primary uses of data collected for a legitimate reason but the secondary uses that are often found later on for some particular database. And that's another part of the attitude I took towards this.

And so when I look at this large database of phone records and presumably Internet metadata as well, my first question is, why does somebody need to build such a large database of phone company records when the phone company has these records?

I could come up with three possible answers. One is retention. Perhaps the phone companies do not retain the data for as long as is necessary. The EU has a data retention law for about two years covering a wide variety of

communications metadata. But that in itself is controversial.

In the U.S. one reason why it will be controversial is we don't have workshops and hearings as much on what private companies are allowed to do with their data, unlike in Europe.

Having a large telephone company maintain data for longer might be worse for privacy. I don't know. But it certainly is an issue. A data retention law is not an automatic answer to a privacy question.

A second possible answer that occurred to me is the efficiency of search, and in particular the indices. If you have a large amount of data it's often organized to make it efficient to answer the kinds of queries you need to answer for your business purposes.

Arguably the phone companies do not have the right indices for the kinds of queries that the intelligence community wants to do and needs to do. And that's perfectly reasonable for the phone company not to. They don't have the same

questions.

It's a little harder to say what should be done about that other than a copy. Asking a phone company, could you build this index for me is revealing of the kinds of questions an intelligence agent, analyst might want to ask and that could easily, very plausibly be seen as a serious security issue.

The third answer, and the one to me that I think poses the most difficult legal and policy questions is machine learning, data mining, call it what you will.

If you don't know what it is just think of the phrase you've all seen in the press, heard on the radio. I've heard several NPR stories in the last year on big data. That's what this is, big data.

What can you do with it? What can you learn from it? It's a powerful technique but it's also one very susceptible to abuse. Machine learning finds things out by correlation, not causality. It can find out very, very surprising

things.

The best example I can give you, go back and read last year's New York Times Magazine article on Target and the kinds of analyses they were able to do with their customer base.

But the thing that makes it most relevant, relevant, yes, that's an interesting word here, isn't it? Machine learning often requires a very large collection of data that defines normal, precisely so you can say this is abnormal because it's different than normal.

This means that by extension everything is relevant, which makes for an interesting reading of the law. It's not necessarily wrong from a technical perspective.

I don't know what it means to do a Fourth Amendment search which requires particularity when it's data that's already there. We need to have a legal understanding of what relevance and particularity mean in the context of data mining.

We're going to have to go short because I'm running very short on time. Metadata, you can

consult my written comments. Metadata, I look at it from a technical perspective, a legal perspective, third party doctrine, something I'm giving to somebody else.

Can I look at this from a technical perspective and say this piece of the technical data is going to somebody else? It turns out that it requires a very detailed technical analysis in order to understand that. It cannot be done easily.

There's a lot of invisible things that can change the answer, and it's ridiculous to have an expectation of privacy that depend on that.

How do we enforce the search limits that the court has supposedly imposed? Can we do it by technical mechanisms? Can we do it by auditing? Do we do it on the server side or on the client side? Both have problems.

Finally, there's the role of the system administrator. In a recently declassified NSA publication noted that system administrators, because they have all privileges, are among the

very biggest security risks. This was once a classified statement. I don't know why since any system administrator knows it, and I've been doing that for almost fifty years.

But looking at the technical, organizational roles of the system administrator is a very important thing that the board needs to look at to understand the real security of the system against the privacy against insider misuse.

MR. DEMPSEY: Steven, thank you. Marc.

MR. ROTENBERG: Thank you very much. I want to begin by saying following Steve's comments that I am not now a computer scientist. I was a computer scientist and decided to go to law school to help address the lawyer shortage in Washington, D.C., and you know, I've contributed my time to solving that problem.

In this statement that I've submitted I outlined some of the steps that EPIC has taken to date and made some recommendations to the oversight board.

I do want to say that over the years at

EPIC I've had the opportunity to work with many great computer scientists and technical experts. And the one thing that they have taught me is a healthy skepticism of technical solutions to what are ultimately social or policy problems, which is a point that I'll come back to.

In brief, let me first describe the steps that we have taken. This may be of interest to the oversight board. As many of you know, we filed a mandamus petition with the Supreme Court this week challenging the legal authority under which the Verizon order was issued by the Foreign Intelligence Surveillance Court.

This order was based on Section 215 of the PATRIOT Act and it requires the telecommunications firm to provide on an ongoing basis all of the call detail records, that's the phrase in the order, also described as telephone metadata, for all Verizon customers on an ongoing basis.

We looked very closely at that statute. We read an enormous amount of commentary. We

simply concluded that the court did not have the legal authority to issue that order.

We believe that the Supreme Court was the only court that we could bring this claim to, and that's a very important part of the analysis I think.

Even as we talk about changes in the law, we have to answer the question under current law, is this surveillance activity lawful?

The second thing that EPIC has done is to begin the formal petition process to the NSA Director, General Alexander.

The National Security Agency, like all federal agencies, is subject to the Administrative Procedures Act and when it engages in a substantial change in agency practice, it actually has an obligation to notify the public of its determination.

Now of course there are certain rules, almost unique rules that apply to the NSA, and we understand that. But that doesn't get the agency out from under its fundamental responsibility to

be accountable to the public.

And as we did with the Department of Homeland Security when they made the decision to deploy the airport body scanners for primary screening and that challenge was ultimately successful in the D.C. Circuit, we think on a similar basis the National Security Agency should give the public the opportunity to comment on this domestic surveillance program.

We have also asked the Federal Communications Commission to determine whether Verizon may have violated Section 222 of the Communications Act when it turned over the customer records to the National Security Agency. The FCC plays a critical role in safeguarding the privacy interests of American telephone consumers.

And finally, we've pursued a series of Freedom of Information Act requests for some of the key legal documents that have been thus far kept secret.

If you have suggestions for more things that we should be doing please send an email

marc@epic.org. We're very interested.

In brief, let me summarize the key points of my written statement. The first point that I'd like to make, as I did already, is that we think the legal authority was exceeded in the Section 215 activity. It's set out in the petition in considerable detail, summarized in our statement.

The second point as to metadata is that this information is far more detailed and far more revealing of person activity than typically the underlying content in a communication.

And in this sense current law, U.S. law in particular, is almost upside down with respect to the privacy interest. As many of you know, our laws have evolved following a paradigm which basically distinguishes between the content of a message, what's in the envelope, and the header information contained on the exterior of the envelope. And we've carried that forward with the contents of a telephone communication, as opposed to the CPNI, the call detail information.

But that analysis, you know, which might

have worked forty years ago when Smith versus Maryland was decided, is almost unrelated to current circumstance because in a digital word, as opposed to an analog word, it's the digital data, it's the transactional data that enables the linking, the chaining, the profiling, the matching, the assessing, the ranking, the rating.

All the analytic techniques that are deployed to assess personal information are most useful as against transactional data.

Underlying communications actually requires interpretation and assessment, and it's a slower process.

So the second point is that the metadata which has been said as something of less privacy interest than the content, in fact the opposite is true. And I think that is the view widely held in the scientific community.

The third point to make is that this type of data, unlike underlying content, generates additional uses.

I've said in the past that data chases

applications, which is to say that once you have information collected and stored in a database, you will not surprisingly find new uses for it. In fact, it would be surprising if you didn't find new uses.

Now you can through law attempt to restrict and legislate the way in which the data that you've collected may be used. But over time almost certainly those boundary points will be pushed further and further as more applications for the data are found.

And I think the conclusion to draw from this point is that a threshold is crossed once the data is gathered because it is at that moment that you've created the opportunity for future applications.

Whether you choose at that moment in time to permit those applications is a safeguard you can put in place, but there is no guarantee that that safeguard will remain over time.

The final point that I'll make, coming back to my original comment is that it's very

tempting to imagine that there are technological solutions to privacy problems. And I will say our organization EPIC has been on the front line since our founding to promote technologies to protect privacy.

We were started over the freedom to use encryption. We've supported de-identification, anonymization, techniques of minimization. All of these methods are very important, but there is no question that at the end of the day the most effective safeguards are the legal safeguards.

And I just wanted to close by sharing with you a quote from President Jerome Wiesner, former president of MIT, was the first science advisor to President Kennedy.

He was asked to testify before the U.S. Congress in the early days of the hearings on the Privacy Act. And he was asked this question, are there technological solutions to the problems of privacy. And he said, there are those who hope new technology can redress these invasions of privacy that information technology now makes

possible, but I don't share this hope. To be sure, it is possible and desirable to provide technical safeguards against unauthorized access. It is even conceivable that computers could be programmed, this is forty years ago by the way, it is even conceivable that computers could be programmed to have their memories fade with time and to eliminate specific identity. Such safeguards are highly desirable, but the basic safeguards cannot be provided by new inventions. They must be provided by the legislative and legal systems of this country.

We must face the need to provide adequate guarantees for individual privacy. Thank you.

MR. DEMPSEY: Ashkan.

MR. SOLTANI: Thanks for having me. And I want to just echo, before I start, just echo Marc's points, that I agree wholeheartedly that the metadata is actually more sensitive at times than the content, and the retention of this information exposes, even with policy safeguards, just the existence of this information collected

at points it normally wouldn't be collected, exposes us to great risk from breach, from misuse, similar to the ways where hanging a piano over my head might be legal but it exposes me to being crushed by that piano at some point.

So I'm going to talk today about just kind of four points, and I've written these in comments, in draft comments on my blog, which you guys can refer to and I'll submit them by the 1st. I'm expecting that there's probably more revelations that are going to be made and I'd like to incorporate those before I submit.

So the points I want to make is, one, that traditional ideas about geography and borders don't really translate onto the Internet.

And that, two, that most of our modern activities take place in part through some digital medium. They create data trails about our activities.

In fact, the NSA itself remarked that in 2002, they remarked that only 1 percent of the 290 gigabytes of traffic, of Internet traffic at that

time was outside of their reach at the time. That's in any 2002, right.

And two other points, that computer systems don't inherently understand law. They don't understand borders. You know, they don't have the same kind of limitations that we do or understanding that we do.

And that they work under the guidance of their operators. And these operators are empowered under a legal authority which I feel like might be confused or lack understanding of the technical capabilities.

One is, for example, the point Marc made that the metadata has more capabilities, or big data has more capabilities than one would naturally logically infer. But just other understandings of how the technology operates.

And so I'd like to expand on that a bit. And the one other point of clarification from this morning's kind of discussion was that there's been a couple of different kind of very clever push backs and a couple of different revelations

we've made.

But the metadata collection wasn't just business records. It wasn't just the NSA going to AA&T and saying, show us your call records that you collected historically.

There was at multiple times equipment that the NSA had implanted at key Internet exchanges and key junctions at service providers in order to themselves create this metadata and collect it.

And we want to be mindful of that in particular because it's a very different issue than just going to Verizon and saying, hey, give us call records. This is generating call records, generating IP metadata.

And the process by which that's generated is problematic because, as I said, computers don't understand law. They don't understand the difference between, say -- they do understand the difference, but it's a very small distinction between an IP header and the email content itself, right, and the same equipment is often very easily

able to capture that same data if it wanted to. And we have some understanding that they were actually collecting email content from the wire.

So I'm going to start just to expand on the first point, which is on a quote that former NSA Director Hayden himself made in an interview recently where he said, let's keep in mind that global telecom infrastructure, geography doesn't mean what it used to mean. Things of a place may not be in a place, and things in a place may not be of a place. The Internet actually lacks geography.

And so this is his statement. It's kind of telling, the person who kind of spearheaded these projects himself doesn't believe that there's an inherent geography to the Internet.

And we kind of need to push on this a bit because, in fact, we want to understand that the NSA is collecting information about kind of any geography and then using, or taking technical measures to limit the amount of information they use on Americans.

And to do this, it's kind of unreliable. I describe a couple ways where this breaks down in my comments around things like users using VPNs, users switching email addresses, who uses, you know.

For example, the NSA maintains a database of identifiers on U.S. citizens which in itself is information about Americans, not anonymous information, but for example, phone numbers, MAC addresses, Internet IP addresses, those kinds of things to identify who's an American. And so that's actually information about Americans.

And oftentimes these things can, to the degree that they're right, they're problematic, and to the degree they're wrong, oftentimes it's problematic because they'll be inadvertently collecting information.

The other thing that kind of complicates things is that the systems that are in place, you know, using these identifiers, using these selectors, right, to discern content can often be implemented improperly, right.

So in fact, we know that through contact chaining targets of interest could be anyone that has an affiliation or interactions with someone else of interest, right. So I could be potentially be a target of interest by my communication with someone of interest.

But you'll find that most of the modern Internet systems that we use today, things like Skype, P-apps like Skype or Spotify, I don't know if you guys use Spotify to listen to music. These are P to P apps, right. They connect with anyone on the Internet for the purpose of providing the service.

So if I and a member of Al-Qaeda like the same Britney Spears's song, right, does that actually put me as a target, right? Does that put me as a target under this contact chaining?

And so the system would probably say yes because I have, you know, some sort of communication with that target, some sort of data sharing with that target. But we want to be mindful that these systems are limited in the way

they understand geography.

And then finally I want to make the point, I make this in my comments as well, that I feel like most of the, you know, we might look to Congress and look to policy makers at what, you know, they've had repeated opportunities to shut down and push back on these programs and they haven't.

And we might infer that to mean that they think these programs are justified or think that they are effective or they're worth the tradeoff.

But one other explanation I want to kind of propose is that, again, people don't understand the technical implications and the raw elements that go into these systems.

So that in fact, the policy makers don't actually understand the technical capabilities of these underlying infrastructures and what data they ingest and what they're capable of.

And because of that lack of understanding that it seems generally okay, right. The geeks have the key to the castle where they'll give you

an explanation that of course the system won't collect information. But in fact, if you looked under the hood, you'd realize that there is actually quite a bit of domestic surveillance going on, quite a lot of inadvertent data collected, quite a lot of misuse from both a policy and a technical perspective. And I think that lack of understanding might explain why there hasn't been kind of tighter controls.

MR. DEMPSEY: Okay, thank you, Ashkan. Danny.

MR. WEITZNER: Thanks very much. Thanks to all of you for having me and congratulations to us on having you here.

I think that we all know that as this round of privacy discussions kicked off, the President said we need a national conversation and I think you guys are it, and that's great. Hopefully there's more, too.

But you have my written remarks. I want to just highlight three points from those remarks. I want to touch on a little bit of a

what I see as the functional goals of a system with sound oversight, some of the technical challenges of getting to that kind of system, and a new technical approach that we've been developing at MIT as part of a larger family of research that's going on around the computer science world.

I see really two functional goals in thinking about how a combination of law and technology can shape the system that we're talking about. And we've concentrated, you've asked us to concentrate on the 215 and 702 programs.

I will say that I think it's important, as Ashkan has suggested, to see these programs in a larger context. They draw on data from a much larger set of systems out there, and I think the ability to draw boundaries in those systems is not nearly as easily as changing section numbers in a statute. So I think it's useful to look in a broader context.

But I want to suggest that there are two goals that we ought to pay special attention to.

First of all, I do think that we should be thinking about how to enable, within the bounds of law and under the rule of law, the process of what Bob Litt has recently called finding a needle in a haystack without undue privacy risk. That's goal number one.

And goal number two, I think given that kind of intensive information analytic environment, to create an environment, as Ken Wainstein said, where there's genuine public confidence in the operation of these programs based on oversight that's effective and a meaningful sense of transparency.

I do think that if we look over the last month it's been the lack of public transparency in these programs and the continued revelations about more data and more data and more information and more information that's come out about these programs that has caused people to feel more and more uneasy.

I think it's caused American allies around the world to feel more and more uneasy. I

think it causes citizens to feel uneasy. I think it causes companies to feel uneasy.

And so I think that having a real sense of transparency here is quite important. And I would suggest to you that it's important to think about transparency in two dimensions here.

The first panel spent a lot of time talking about the reasonable transparency for rules and the rule making processes associated with these programs. But I think the second kind of transparency that this panel can address perhaps in a more focused way is transparency of the actual data usage. How are we going to know what's actually going on in these systems?

Let me talk for just a minute about what I see is the technical challenge of having that kind of transparency. Within certain bounds I think it's safe to assume that the government is going to have more and more and more data.

I think the constitutional process, the legislative process will determine how much more, but it's going to be more, and that's just because

of the trends in the world that we live in.

So I see the challenge, again picking up on Bob Litt's, he's been very eloquent these days, Bob Litt's statement, he's very up front recently in a public statement said that we, the intelligence community, collects all the data because if you want to find a needle in a haystack, you have to have the haystack.

Steve addressed some of this question about whether you actually need all the haystack all the time, but I think we can see the development of government programs, the NCTC programs as an example, are moving towards having all the data in one place.

And then the challenge, the oversight challenge for organizations such as the PCLOB, for the internal oversight functions for the courts, for the Congress and ultimately for the public is how to have a sense of confidence that all that data that's held where again the claim is only a tiny bit of it is used, that in fact those rules are being adhered to.

What I think it's very important to recognize about these rules is that these are rules that really are governing the usage of information, not the access to or collection of information.

Again, in the larger privacy policy debate I think we can see more and more a recognition that many of the privacy challenges we have are going to have to be addressed by usage limitations, not simply by collection limitations because to a large extent all the data of interest has been collected and is sitting somewhere.

Very briefly, I would say that if you look at the computational techniques available to address these kinds of challenges, in computer science we're quite good at access control. We're quite good at controlling who has what access to what data at any given moment. We can encrypt it. We can put it behind firewalls. We can do all kinds of things. And Steve is one of the world's experts on all of those sorts of techniques.

But what we're not actually as good at

until recently is the ability to examine a system and determine how the information in a system is actually used and whether its uses are in accordance with whatever the appropriate rules are.

Several years ago my research group at MIT took on the challenge of trying to think about whether there's a way to actually characterize information usage rules in a formal computational sense and whether you can then apply those rules or you can ask whether those rules have been adhered to in any given information system.

We've developed a number of research prototypes that enable us to detect violations of rules such as nondiscrimination rules, law enforcement information sharing rules, and then some non-privacy rules such as copyright law.

And you have in my written remarks a description of this research. And by the way, there's now a very active community of researchers around the country and around the world who are working on systems like this.

I guess if I could stress one thing about these systems and the state of their development, I think we know a fair amount about how to design these systems.

We know much less about how to deploy them at large scale. And I don't think we will know anything about how to deploy them in large scale until we actually start doing that. And that won't happen until the entities that hold information are actually told that they have to be accountable to these usage rules.

What we have now I think, and I think we can take --

MR. DEMPSEY: If you could, can we hold it right there.

Mr. Weitzner: Yes.

MR. DEMPSEY: I was a little generous on the five minutes on the first round and instead of having a full two minute round where everybody feels obliged to say anything, let me simply ask, is there anybody who feels compelled to say something at this moment before we get to

questions?

Marc.

MR. ROTENBERG: Thanks, Jim. Well, I actually wanted to follow-up on some of the points that Danny just made because I'm very troubled by his description and his proposal.

He seems to be arguing that there's really no need, purpose, or likelihood of success for collection limitation rules.

So I mean let me stipulate that for a moment, but ask you these questions, if that's true, A, what is the legal authority under which U.S. agencies are currently allowed to collect all this data? In other words, what's the basis?

I used to think of that as a search requiring some legal standard, even a low one. Do you think there is such a legal standard that operates as a limit on collection?

And secondly, if you don't, if you don't think there are any legal standards that prevent collection, is there any boundary point?

In other words, if the Verizon order, the

NSA were to go to FISC and say we want all credit card information, all telephone information, all web searches, everything you possibly have and then we will sort out the usage conditions, do you have any problem with that?

MR. WEITZNER: So let me make sure that no one misunderstands, I am in no way suggesting that we should eliminate all collection limitations.

What I am suggesting is that our current legal standards appear to allow the collection of very large amounts of information. And I said very directly that I think it is for the legislative process and ultimately for constitutional determinations to sort out how broad that is.

But my belief is that agencies have reasons to have large amounts of information. And again, I don't know whether it's large or very large.

I also think that it's quite challenging, based on some of the comments Steve made, to

understand where those limits will be. We need those limits, but what I would suggest is that some of the protections that we have traditionally sought from collection limitations, which I would submit have mostly been practical limitations, that it's hard. It used to be hard to store data, it used to be hard to analyze a lot of data, those practical limitations have fallen away.

And I believe we need to replace them in many cases with very clear usage rules to prevent against the misuse of data.

I don't think it's an either or question in any way, Marc, but I think it's equally mistaken to assume that you can solve this problem with collection limits.

MR. SOLTANI: Just a quick comment on that. I think I would agree with both sides here in the sense that I'm a fan of usage or audit-type, basically transparency, technical transparency mechanisms, right.

For an agency that's, you know, whose bread and butter is kind of data mining and data

analysis, they should be able to analyze what the effectiveness and the usage of their information is, right, that's a no brainer.

They could tell us what percentage of the information throughout a trail was relevant to an investigation.

However I want to push back on the use of technology as a placebo or fix, or sorry, a panacea of policy limitations, right, because all that does, all the use of things like encryption, or firewalls, or access control rules, all that does is make it more expensive to get at the data, but rarely does it make it impossible.

We've found that with enough resources and enough effort almost every security advancement, there's been some vulnerability found, it just takes --

MR. DEMPSEY: Although I mean we can talk about the abuse scenario. Honestly, I would rather focus on the non-abusive uses.

MR. SOLTANI: Absolutely. But let me give you, so let's say there's a database that's

encrypted or it has access limitations that has the subject of a potentially suspected terrorist and it's our only lead for it.

We know that data exists in a database but it also contains, you know, millions of records of individuals, innocent individuals, Americans.

So not in an abuse scenario but in a scenario where we know that data exists somewhere, we have technical limitations, but do you think we would not as a nation or as a country overcome those technical limitations if the data exists?

MR. DEMPSEY: All right, that's a different.

Steve, do you want to add anything quickly here?

MR. BELLOVIN: I'll pass for now.

MR. DEMPSEY: Okay. For my first question let me ask the following, which is geography. A couple of you mentioned geography and that the Internet lacks geography, quoting General Alexander or whoever.

We have a law, 702, which is based upon the geography of people, persons. And let's assume for now that persons means an individual. So an individual only exists in one place at a time, and we have a system that's based upon assessing where that individual is, and if they are outside of the United States and not believed to be a U.S. person, then they can be subject to collection under 702.

Now my question is, what are the best and what are the worst indicators of whether a person is outside the United States? Steve.

MR. BELLOVIN: So there are several technologies that are commonly used. The most common one is something called IP geolocation. There are databases saying where different IP addresses are, Internet protocol addresses.

If you look at this, this is used by gambling sites, by major league baseball to see if you're in the blackout area and so on.

MR. DEMPSEY: And by the way, don't forget the possibility of nontechnological means

in terms of your --

MR. BELLOVIN: Yes, absolutely. It's an imperfect technology, is probably about 85 percent accurate, certainly more accurate when we talk about the country level rather than the city level.

MR. DEMPSEY: Which one are you talking about now?

MR. BELLOVIN: This IP geolocation. The NSA actually has a patent on a somewhat more advanced technique which uses round trip time from geographically known points. Speed of light is a limit. I don't know if they're actually using it, but there is a U.S. patent that they were granted on this.

The problem is that data doesn't respect national boundaries and as we see more and more data moving to the, quote, cloud, unquote, if you're operating one of these large data warehouses in the Internet someplace, you want to disburse geographically for reliability, redundancy, another northeast blackout or another

California blackout won't take it out, one of the migration's going to happen quite transparently and nobody is controlling where a lot of this stuff goes. So the geography of the data makes for a very, very poor analogue --

MR. DEMPSEY: Again, we have a law here. We have a law here that ignores the geography of the data and focuses on the geography of the person, and I'm trying to ask -- Ashkan.

Finish up, Steve, and then go to Ashkan.

MR. BELLOVIN: There are approaches, they're not perfect, especially a lot of the technical mechanisms that business travelers especially use when they're traveling virtual private networks makes them appear in the U.S. who are not in the U.S. depending on what their country of origin is.

It's not a particularly useful paradigm today. And there's a lot of stuff that's out there which is not easily attributable to a particular person because of twitter handles and the solution of massive databases has its own

privacy risks.

MR. DEMPSEY: Ashkan, and then I'll go back to Marc.

MR. SOLTANI: I want to echo Steve's comment. There's actually the third largest ISP in New Zealand, they have a feature where their IP addresses become borderless. They can appear to come from the UK or come to the U.S. so they can have access to things like Hulu or BBC, right.

So these are like commonly used. VPN tools are commonly used and they basically render IP-based geolocations somewhat ineffective. IP geolocation will tell you the source of the network equipment but it won't tell you the location of the individual.

But one thing I want to point out is email addresses don't have the same property. So an email address doesn't inherently have a nationality that you can infer from the email address, right, so perhaps you can look at the country code or maybe the nationality of the name. But there's nothing actually inherent to the email

address.

And in fact, we've learned that most email, so most email between cloud providers, right, so when you go to Gmail and you send an email, even though you see a lock icon in your browser, when Gmail delivers that email to someone else, it's transmitted through Gmail servers in the cloud, as Steve described in Cleartext, right, and so anyone with equipment at large Internet exchanges can monitor that and scoop that information up, metadata or content.

And the question is at what point then or how do they determine whether it's a U.S. citizen or not? And we understand there's some indication to show that they have database of U.S. citizens. There's other indication to show that there is other data appended to it, right.

And at that point you're actually looking at the data. You're actually, so if 702 is a collection limit, you've collected and looked and processed the data, at which point then you decide, well, it might be American.

And the problem with that is it kind of, it's kind of after the fact, right, you've already looked and processed that data.

And then we know under section, what is it, Section 5 that if you actually encounter any illegal activity in that process you're then able to hand it over to other law enforcement agencies for processing, right, under Section 5. So it renders this problem of email identity somewhat borderless and somewhat ineffective to try to differentiate.

MR. DEMPSEY: Marc next, Danny and then I'll come to you. Marc was next.

MR. ROTENBERG: Let me see if I can give you a somewhat more precise answer shaking the cobwebs of my computer science background.

Now for locating the device the typical cell phone can be located based on three techniques. One is the cell service triangulation. The second is the GPS, which the devices typically include. And the third is the Wifi access to the local router.

But you're talking about the identity of the individual, you're actually talking about the individual using the device at a moment in time. And that's actually a problem in isomorphic mapping.

In other words, you need a big table of all U.S. citizens and then you need a unique link to the user of the device at that moment in time. Because, by the way, the person who's holding John Smith's device may not necessarily be John Smith. So you actually have to authenticate the user to the device and then determine if that person has the status that allows them to be a U.S. citizen for 702 purposes.

Now I actually suspect that the NSA has given considerable thought to that problem because they need to address that challenge in satisfying their 702 requirements.

I also know something about this because I participated several years ago in a workshop on something that was called eDNA. And the theory of eDNA, and this was not long after 9/11 was that it

would be possible to uniquely link every activity on the Internet, every key stroke to an identifiable user. It actually solves the isomorphic mapping problem because you know exactly who did what when, right? It's perfect if you're trying to design something like total information awareness.

But here's the problem with this calculus, and I think it's why we've gone too far down this road of distinguishing between U.S. citizens and non-U.S. citizens. Our Fourth Amendment actually doesn't draw that distinction.

Our Fourth Amendment, and almost all privacy laws but for the FISA, regulate the conduct of the police in undertaking law enforcement activity. We certainly recognize the need for the conduct, but it's the police conduct that we're regulating.

What FISA introduced was the notion that in the collection of foreign intelligence we needed to safeguard the privacy interests of U.S. citizens, and in that introduction attempted to

build a barrier against the overreach on the U.S. side, which was very sensible.

MR. DEMPSEY: Marc, if we could, back to the question of geography. Again, the law focuses on persons reasonably believed to be outside the United States. That's the first filter, let's call it.

And what I'm asking is in terms of how that assessment is made, is this person or device, let's assume, because you don't care so much about the identity of the person, you care about the location of the person, reasonably believed to be outside the United States.

My question is, can somebody give me, give us a list of what are the most reliable factors, answering just that question, and then what are the least reliable factors in answering that question.

I'm going to go Danny and then I'll yield to David because we've got to move on.

But to me, personally, it would be helpful to have some kind of way to go back to NSA

and say, how are you making this determination, what are you looking at, what is technologically more reliable and technologically less reliable? So you don't get then to the second question, which is, oops, we got it, turns out it's a person inside the United States, or oops, we got it, it turns out to be a citizen. How do you first make this judgement of geography? Danny.

MR. WEITZNER: I want to suggest that perhaps the more reliable, less reliable list may not be the best way to do it.

What I would say about more and less reliable is the more contact you have with some target, the more reliable your determination should become.

And I think that in these uncertain cases, let's take Steve's 85 percent accuracy as a given, and I think we can get, there's known, there are known reliability levers for different IP address blocks. We can get you that sort of information. The NSA obviously knows it.

But I think the real question is, does

any intelligence agency as they develop more information about a target, do they act on it? Do they realize, oh, actually it's now more likely that this is a U.S. person so we better start treating them that way?

Or, so the question is, do we have a way of establishing that dynamic threshold? That is the way that any web service, any Internet service functions is it learns over time about who it's dealing with. And I think it's reasonable to expect that intelligence agencies should deploy that kind of technique also and be accountable to it.

So I'm a little nervous about these bright line rules because I think the hard cases are going to be the ones that change over time, and the question is when does that change get recognized?

MR. SOLTANI: And just real quick, because of the point that I made in my -- the other assumption is that there isn't a reliable method, right, that as Steve said and others have

said, the Internet is without geography and that you need additional information to prove one way or the other. Sometimes that requires looking at the content.

And there's a perverse incentive here, as we found in the minimization guidelines and the targeting guidelines whereby the standard is, the information is basically guilty until proven innocent, right. So unless you can reliably prove that it's a U.S. citizen, you are able to hold it and analyze it and for later analysis. This is encrypted data. This is data that we don't have clear understanding of.

And so these two things together that the Internet is inherently without geography and there's not a reliable way and the standard is hold the data until you can reliably prove that it's not U.S., I think causes a --

MR. DEMPSEY: Let's move on. We could go on this forever.

MR. MEDINE: Yeah, I want to pull back to about 5000 feet. One of the board's

responsibilities is to oversee programs and see if they strike the right balance between privacy and civil liberties.

We've heard from panelists about there are privacy and civil liberties issues with regard to collection, use, access and disclosure of information.

I guess my question for each of you is, if you could guide us in how we should approach these problems, where can technology address those concerns? Where does law, where do we have to rely on law to address those concerns, or how does technology and law interact together so that we could address those concerns as a framework for thinking about these issues going forward?

MR. BELLOVIN: Technology at best can implement a policy. If I'm designing a system I have to know what, you know, what are the specs, what are the things I'm trying to do?

And I get, depending on the problem, I can come closer or not so close from a technical perspective.

The flip side to that is audit. How do you verify that people are staying within the rules?

I'll take a somewhat different non-national security system, electronic medical records in hospitals. Anybody who's looked at these realizes that you can't require really strong authenticate need to know because someone's going to walk into the emergency room. So all of these systems have so-called break the glass access. In case of emergency, break the glass, look at the data.

But there's going to be an audit process after the fact to say was this a reasonable thing for this doctor, this nurse, whatever, to have done at that a time? And that's a deterrent. It's also a way to catch and punish people who are ignoring the rules.

But what comes first is the policy. After that I can design a technology and it will, it has to include an audit function.

MR. ROTENBERG: Well, I didn't mean to

suggest by my earlier comments that technical solutions aren't appropriate. Obviously they're necessary, and audit logs are key.

My point is simply that I don't think that's an ultimate solution, and I think you do need legal safeguards. And to that issue, you know, I listened to the panel this morning, which I thought was absolutely fascinating. All of the speakers I thought had very interesting things to say.

But I was particularly struck by Mr. Wainstein's comments regarding how the FISA process is similar to the traditional Title III wiretap process. He said, you know, we have ex parte access. We don't tell our targets when we're trying to get information about them in the course of an investigation. And of course in that respect he was absolutely right.

But what struck me also, you know having studied the oversight mechanisms for both of these frameworks for electronic surveillance in the United States, is how many other things are in

place for traditional Title III wiretaps, law enforcement investigations.

So it's true, you don't notify the target and you wouldn't, but what do you do? Well, you know, the courts are have to report on an annual basis the number of wiretaps that were authorized, how long they took place, what the outcome was, what the cost was, what percentage of non-incriminating information was gathered.

And all of that data, by the way, is made available to the public, not any investigation-specific information, but an enormous amount of information is made available to the public about the scope, use, purpose, and effectiveness of those traditional wiretaps.

With respect to FISA, we have almost none of that information. We have a letter that says roughly in 2012 there were 1,784 applications submitted, one was withdrawn and 1,783 were modified or approved, or actually approved or approved subject to modification, because they're ultimately virtually all approved.

So the key point I'm trying to make with regard to the legal safeguards is I think there are necessary and appropriate ways to pursue the collection of data and to safeguard the nation. No one is disputing that. But I think there are many more ways of establishing meaningful oversight within the FISA that really we haven't scratched the surface of.

MR. MEDINE: Ashkan, law versus technology.

MR. SOLTANI: Yes, so I think there are some technical ways to do this but you would need essentially kind of an intelligence agency to monitor the intelligence agency.

So you would need a set of technically capable kind of actors, you know, they could be under PCLOB, they could be under some other agency, that are building tools, building audit mechanisms, building security mechanisms to measure exactly what the agency is doing and the effectiveness.

This could be simply things like, you

know, the number of email addresses, IP addresses, U.S. persons, gigabytes, whatever is collected, how that information relates to investigations, how effective it's been. And provide kind of a good, in-depth kind of, you know, red teaming the NSA essentially, right, having someone from the outside that's independent of the NSA audit them and provide intel to you guys to tell you whether they're doing their job, rather than you relying on them. And this could be technical.

But this isn't things like what Danny and Steven have described as the NSA implementing their own audit logs, right, because I think that's -- they will perhaps not classify an email address as an individual, whereas you guys might feel that is an individual. So you would probably want an independent team doing this, I think.

MR. MEDINE: Taking that a step further, is there also an argument that some of these programs should be subject to testing and analysis before they're rolled out on a larger scale?

I mean typically in technology you test

something and then see if it works and then you build it out, as opposed to waiting after the fact and seeing if it ended up working. Is there a lesson there?

MR. SOLTANI: Absolutely. And fed back to the judges and the policy makers approving these programs, right.

So as you give a FISA order for something like this, do you know the actual number of individuals affected, the number of records, the amount of records collected from this, how much was over-collected, how effective this was?

That is, there's no feedback mechanism to the FISC or to Congress as to how well. You just kind of trust the NSA to say, yeah, this recommendation, this is working great, these algorithms are on it. And I don't think you guys have a way to say, actually, you know to call BS on that.

MR. MEDINE: Danny, any thoughts on law and technology?

MR. WEITZNER: So I think that along the

lines that Ashkan is suggesting, I think we have 21st century intelligence analytic capabilities and 20th century accountability and enforcement methods, and we have to get the privacy enforcement methods up to date.

I don't think it requires creating a whole other intelligence agency and you probably were just being flip in saying that.

I do think it requires a much more intensive approach to auditing and it requires a way of looking at the results of those audits in a fashion that can have a certain amount of public transparency, certainly access for independent entities.

Maybe there's a role for the PCLOB in doing but there'd probably have to be more than just five of you to do it.

So I think we should raise our expectations of the ability to detect anomalies and detect misuses in the way these agencies operate.

I'm a little leery of blending together

the question of intelligence effectiveness and privacy rules. I find it to be -- so, yes, I think certainly if agencies are going to spend lots of money on new data analytic systems they should make sure they're effective and they shouldn't waste their money.

But just because a system is effective doesn't mean it passes our privacy test. I think we should make sure to keep those two questions on separate tracks.

But there is really a lot that can be done in having better accountability, but it comes back also to Steve's original point, the rules really have to be clear and not dependent on technical accidents such as whether a particular IP address might be geolocatable or not.

MR. DEMPSEY: Steve, did you comment on this question or did you have anything?

MR. BELLOVIN: Well, I started by saying that policy has to come first, and that's the law.

MR. DEMPSEY: Okay. One quick follow-up for Marc and then one general question.

Marc, you mentioned, you said we've barely scratched, I think you said we've barely scratched the surface on approving the FISA project, there's a lot more to be done there.

Either off the top of your head could you tick off a couple of items or submit them for the record please, but anything off the top of your head that you want to tick off.

MR. ROTENBERG: I think we could improve public reporting through the availability of more statistical information that doesn't compromise any particular program or activity of the agency but would give the public a better picture of how these programs are used over time.

I mean we found, for example, with respect to the wiretap data, it's very useful to see trends. It's very useful to understand, for example, why narcotics investigations today are the primary reason we have wiretapping, and bookmaking was in the 60s and 70s, or regions of the country.

And I think it leads to a more informed

public debate because people who think these are necessary tools have the data to support their points. We're not arguing in the dark.

MR. DEMPSEY: Thanks. And anything further you could submit along those lines would be very helpful to us, or other witnesses, or other members of the public.

Content versus non-content. I have to say personally I'm not yet convinced the statement, Marc, that you made that the non-content is as revealing as or more revealing than the content.

Two reasons. Often of course when the government collects the content they collect the associated non-content as well.

But even on sort of the big data basis, I mean I get it that, you know, I call the cancer testing clinic, and then ten minutes later I call the oncology department, and ten minutes later I call the insurance company, and then I call the drug store, and then I call the oncology clinic, you know, every week for three months. So you

infer that I have cancer.

Well, I may have called and said my mother is 90 years old, she has cancer, what can we do about it? Or my child is six years old, she has cancer, I'm going to be bringing her in every day.

Now it would be far better, far more revealing it seems to me to have that content than the unreliable inference.

And I think there's a privacy flaw in the, there is no distinction, because I actually think you fall into the argument that the content is so powerful you actually end up making the government's argument as to why they need it.

I think there's a different argument to be made, which is actually the metadata can be highly misleading and you conclude that I have cancer when in fact it's a relative that has cancer.

MR. WEITZNER: Could I speak in favor of Marc's proposition, which is that I would just amend it slightly to say that metadata at scale is

at least as revealing as content. A single piece of metadata or even a single set of metadata about you can very well be misinterpreted.

A few years ago two students of mine did as a final class project a paper that they called, Gaydar. They looked at the MIT social network on Facebook and were able to infer relatively accurately who in that 25,000 person social network was gay and who was straight, based on the strength of the friendship relationships, based on a link analysis.

So that was information that was actually not available for the vast majority of the members of the social network either publicly or privately. You couldn't get it with a warrant but you could infer it by looking at the metadata.

MR. DEMPSEY: Good point. Marc.

MR. ROTENBERG: I mean I agree with Danny who is agreeing with you that at the micro level inferences can be wrong, but at the macro level the amount of useful information you can glean from the metadata is far more valuable than the

underlying content.

And the simple way to understand this is the dramatic paradigm shift from an analog world to a digital world. Analog information doesn't lend itself to analysis.

To analyze analog information you need to transform it into a digital representation, which by the way, is what's happening with a lot of telecommunications, because a lot of voice traffic is now being digitized and transformed so that it can be analyzed as a digital representation.

But once in digital format you have unbounded opportunity to examine, compare, rank, analyze.

And I have to say coming from a bit of a computer science background, I mean it's fascinating. It's absolutely fascinating what you can learn that you didn't even think you would look for at the outset.

I would be surprised if people at the National Security Agency aren't uncovering things they didn't anticipate that they would find.

But you also made a critical point, Jim, and I agree with this. I think it's the hard policy problem. It is the value of the digital data to the NSA that's driving these programs.

It is also the risk to privacy that I think has raised the need to update our privacy laws to reflect the underlying interest, the actual interest in digital data.

If I can make one final point. I know I've talked on a bit but I really don't want to lose this one. We're thinking a lot about the communications realm and the linking of identities through investigations, which is an appropriate investigative technique, but you should also be aware that these large data sets are used to profile individuals, including American travelers entering the United States, to assign a threat index to the likelihood that they may commit some act that poses a risk to the country.

So by taking all of that data, looking at prior acts, you can assign a score across a large data set and allocate your resources. That is

another way in which large data is being used.

MR. DEMPSEY: But if the data is so powerful, isn't that a good thing?

MR. MEDINE: And let me just follow-up on that. That's really the converse of what your argument is, is if the goal here of these programs is to find terrorists that the data is very good at that and shouldn't we be using it, and doesn't that support the government's argument that we need to amass all of this data to be as effective as possible in identifying --

MR. WEITZNER: But we're missing, we missed some steps, because we have answers I think in consumer privacy law, as you know, David, laws like the Fair Credit Reporting Act that are good at managing very large scale analysis of data in a way that attempts to be fair to individuals, so that when determinations that could be harmful to them, like you're not allowed into the country, or you don't get a loan, are made, that there's a feedback process, that people have a right to respond and correct the data.

I think that there are obviously, you know, there have been calls for that. It seems like there's been some progress in DHS in doing that, but I don't think that we've gone far enough.

When there are real adverse consequences for individuals, people should have the right to be able to respond and correct the record, not to be able to hide from what's true, but to make sure that in fact the inferences are accurate.

MR. BELLOVIN: And let me just clarify a little bit what Marc just said, it's not digital data that's helpful, it's structured data.

Anyone who's done one of these voice menu systems on the phone knows just how bad computers can be in processing unstructured, just voice, especially unstructured conversations.

Structured data, this is the calling number, this is the called number, is extremely valuable. You can process it very efficiently at scale, gather vast amounts of data. It's much harder to hide. You can do it retrospectively

rather than prospectively.

I want to wiretap, I have to go in advance because the phone company is not recording all of my target's phone calls, but they are keeping call detail records. You can go do this retrospectively.

The intelligence community has known for more than seventy years that just the metadata is an exceedingly valuable technique, and it's gotten more so with modern data processing and data handling.

Content is great but it's much harder to get, especially harder to deal with --

MR. WEITZNER: Can I just express one note of caution? I don't think that we should necessarily make asumptions in an unclassified environment about what the capabilities are to analyze very large volumes of digital voice data. I don't know, but I don't think we should necessarily assume what the limitations are.

Because there's certainly been a lot of advances in voice recognition and in processing

very large streams of digital data of this sort.

MR. SOLTANI: I agree with Danny. And I'd rather propose a different perspective, which is rather than saying content is gold and metadata is maybe less, or trying to come up with a formula where a thousand pieces of metadata equal one piece of content, we should kind of view this as information.

And information has kind of confidence levels, right. So you have certain amounts, like certain ability that information is accurate. Oftentimes you'll find content itself, right, content itself will be unreliable. There will be lies, or code words, or misleading statements in the content itself, right.

So, and if there's not a gold standard of the truth, there's the information reveals certain characteristics about you, about the individual and that information has some level of confidence.

And so oftentimes you'll find that a statement like, you know, I like puppies is a very

high confidence interval that I've made, right, or you could try to infer that based on my, you know, previous pet activity or previous browsing activity of puppies.

And you have some levels of confidence, as Jim said, sometimes they're wrong, but as you tune systems you often find that in a large data environment you start kind of improving these algorithms and with enough information you can make these inferences.

And the question of whether this is effective or not is definitely one question, right. We've found in some cases this stuff is effective or can be effective, right.

There've been examples of calling patterns. Getting a nation's calling patterns will reveal, you know, who might be in a drug ring based on just the fact that people make inbound calls, right.

So there is effectiveness to that stuff, but it doesn't alleviate the policy question, which is that, or I'm sorry, the privacy question

or the privacy interest, which is that, does this information reveal sensitive, does metadata reveal sensitive information? And to some degrees it does.

MR. DEMPSEY: Just one quick observation and I want to go to other members of the panel if they have anything.

You know we talk about machine learning and the feedback process and sort of system learning, and again, thinking about the role of judges, traditionally the judge issues the search warrant, he gets a return. But if the search turned up nothing, it's not like it was a bad search or a bad warrant.

So in a way we're talking about, as Judge Robertson said, changing the role of judges in a way with these programmatic approvals.

Also with this question of what's coming back. There might be something to be done there to say, well, it's not that it was a bad search, but we're just not going to do it again.

MR. SOLTANI: Right. If in your example

if historically you do a thousand of those and you do intrusive searches and you kind of expend a ton of resources and they don't come back as hits, at some point the judge might kind of say, hey, this is kind of a waste of time, let's not expend resources on this. We don't have that accountability in this program, right.

MR. DEMPSEY: Do the other members of the panel, I am willing to yield if you do, if something has occurred to you since.

MS. WALD: I've got one.

MR. DEMPSEY: Okay, good. So let's go on down, Judge.

MS. WALD: You talked a lot about, several of you about the accountability and enforcement mechanisms being 20th century, whereas our technology is leaping ahead in the 21st century.

This morning's panel we talked a little bit about possibilities on a legal end. I mean people talked about maybe having not an ex parte thing before the FISA, but something that the

other side is represented by.

Now my not being a technological person at all, but my impression is that right now the accountability mechanisms are all, well pretty much all internal within the agencies. I mean they self-report when something goes wrong. They do have to report already to some degree, depending, back to the FISA Court in certain situations.

But, you know, even then they kind of decide, and I'm not saying no question of good faith, but they have the initial option of deciding, you know, when they will report, what they will report.

Now do you think there are any, we talked about like in the FISA Court on the legal end having somebody presenting the other legal side.

Are there any outside of the agency itself kind of accountability mechanisms, other than the one you mentioned about having the FISA Court say, come back to me and tell me how that program is working out, hoping the FISA Court is

more knowledgeable than I would have been in that situation, that would help to enhance your notion of accountability?

MR. WEITZNER: Could I suggest, Judge Wald, that one, I don't actually have an answer about what outside institutions might be put in place, but I think that having structured, well understood audit returns could help a court, could help an authorizing judge evaluate the authority that that judge has given to a given agency in a given situation.

You know, I think that the problem we have is it seems like on the one hand sometimes there's a very large volume of data, there's millions of elements of telephone metadata and then we hear only 300 of them were used.

And I think that seems to present, or Jim's example looking at geolocation, maybe if we follow Steve's numbers, one in five, or one out of six times you misidentify the location of a person.

Well, do we have to just accept that as a

given for all programs and should judges act accordingly, or could a judge say, well this time you were accurate five out of six times, I want to see it better. Come back, you know, fix your program, come back with 90 percent accuracy.

You know, these are in many cases challenges that could be met and we can identify the underlying policy goals, the underlying harms we're trying to prevent.

So I guess I think that, again, from a technical perspective we should expect better analysis of the data that's returned so the judges can make judicial and policy determinations.

MS. WALD: But just to follow-up on that, as you know the judges, the FISA judges are picked from the pool of U.S. District Court judges. My impression, I knew many of them, is that they didn't come with a great deal of technical knowledge or with computer science knowledge. I mean they do their very best. I think they probably do a good job, but they are not technical people.

And when you get a massive operation and they say, X with the selector or something went wrong and as a result we got X number of things that we shouldn't have gotten, blah, blah, blah, blah. I guess what I'm saying is, do they need or is it possible that FISA judges need maybe a technical law clerk, I don't know, somebody who's outside of the system who can relate to them?

MR. WEITZNER: Certainly. I think absolutely having technical expertise to evaluate --

MS. WALD: Or not outside the agency to evaluate the data that comes back on returns.

MR. WEITZNER: But I think it's ultimately up to policy makers.

MS. WALD: Yes, I agree.

MR. WEITZNER: To set that expectation, to say that we actually care about this U.S. persons question and we want to see accuracy increase. It seems to me a judge, a court with technical resources could implement that determination.

MR. DEMPSEY: Steve and then Beth. Steve just to follow-up on this answer.

MR. BELLOVIN: Yes. I'm not going to answer who should do the auditing because you don't want me designing your organizational structure. Trust me on that.

But I can give you a few questions that need to be asked. The first question, is it actually effective? Are you actually finding targets? If it's not finding targets, what's the point in the system?

Second, how accurate were the preconditions? The analog through probable cause saying this is a program that we think will be good enough or this is why we think this individual is or is not American. How accurate was that judgment on later investigation? How well is it actually working? Are you really finding the people you want to find? What are the risks to privacy, both from intrinsic risks, from later reanalysis, from misbehavior?

These are the questions to ask in the

audit. How often are people actually following the rules? Rules that are too strict tend to get evaded, and those are no good either. There's just pro forma adherence to it. So this is the kind of question.

But yeah, you want to feed that process both internal and external. I hope they've done internal.

There's one NSA whistle blower, I forget his name, who blew the whistle on some project. He said it was not working, it was privacy violating, but most of all it wasn't working and we're spending a billion dollars on it. What's the point of doing that? Assuming his claims are correct, and I do not know.

MR. DEMPSEY: Marc had a follow-up on that one.

MR. ROTENBERG: Just very briefly, Judge, I recommended earlier enhanced public reporting.

I think the question also should be considered whether the statutory scope of the court should be limited. It has enlarged over

time to a significant degree. It was actually in 2003 that the number of FISC orders exceeded the number of Title III warrants approved in the United States. And that trend has continued.

And the final point which I thought Judge Robertson made very eloquently on the earlier panel today is that the judicial process works best of course from an adversarial proceeding.

And so even to have a technical expert, you know, maybe that's helpful, but I think you really do need to hear both sides of the claim to make a meaningful determination. Otherwise you transform the judge into someone who's basically an agency manager, and that doesn't seem to be the appropriate role for the court.

MR. DEMPSEY: Ashkan, if you could --

MR. SOLTANI: Actually just a quick --

MR. DEMPSEY: Okay.

MR. SOLTANI: There are external actors or external entities, right. These are the companies. A lot of these programs couldn't actually be possible without the assistance of the

companies, right.

And the companies are currently under gag to report the number of people that are affected. We've seen some expansion of that recently. But you could actually try to get more information from the companies to actually describe, you know, what information is revealed, not specific to targets of course, but kind of trend reports, in the same way we have transparency reports by a few companies. You could actually have the agencies that are working with these companies.

And these, but these companies are actually dying to tell us, right. They're dying, their brand and reputation are going down the drain. So they're dying to reveal that in fact it's not as bad as it is, or that the NSA is over-collecting, right. And that's a nice little external hook you could latch onto.

MS. COLLINS-COOK: So thank you guys. This has been extremely helpful from my perspective.

Danny, I wanted to follow up on one thing

that you had mentioned which was the gap between the development of the capacity to do more substantive and more effective auditing and the inability to deploy it on larger scales.

And I just wanted to confirm what I got out of that is that there are potential operational risks.

For example, if you were to attempt to deploy some of these more substantive audits on existing systems or in existing databases, or is it possible to simultaneously task some of the programs y'all are developing without risking the operational efficiency of ongoing programs?

MR. WEITZNER: So I think that it is possible to. These systems all generate logs. They have logs coming out, you know, logs and logs. So it's possible to parallelize the analysis of the logs from the ongoing operation of the system. I don't think that one needs to burden the other.

Very often we've seen situations in which analysts, it's actually helpful for analysts to

have real time assessment of the policy impact of a query they're proposing or a conclusion they're reaching. Can I use that conclusion for a certain purpose or not?

You know, that's where it's important that we have adequate computational efficiency to get that answer in the time that the analyst needs to make a decision. But I don't think that there's a reason to worry that one burdens the other.

I do think it is the case that, and my guess is the agencies would say, well, they're going to have to spend money on it, and that's true.

MS. BRAND: Beth started the practice of giving homework in the last panel, so I know we're just about out of time here so I don't want to make all of you go down the line and answer, but I actually was focused on the same comment, Danny, that Beth just mentioned.

You said something like, we're not very good at figuring out how information is used and

whether it's consistent with the rules and we've started to learn how to design the systems but haven't figured out how to deploy them on a large scale.

So you know, you presumably are not privy to whatever the NSA is doing to audit its own systems and so there's sort of the front end restrictions, such as who can access it and what the supervisory levels of authority are there, and then after the fact whatever the audit trail is and, you know, that's not public necessarily.

But it occurred to me that in the current context with Snowden, his leaks are viewed to be a national security risk because the things that he's leaking are more structural in nature. But you could also imagine a situation where somebody in a position like his wanted to leak things that would violate peoples' privacy, so the underlying data instead of the structural documents.

And so perhaps in your written statements you can address this. Is there a way to design a system that would kind of issue a red alert if

somebody is accessing data in a way that seems to indicate that they are going to use it for that kind of purpose, as opposed to violating an internal rule that might not immediately violate someone's privacy?

That's not a very well-formed question but --

MR. SOLTANI: Hospitals have the same complaints. So hospitals, you know, it's a commonly known thing that people will leak when a superstar comes in and they'll leak it to the press. So there are existing systems in place that will do anomaly detection for access.

So why are you, if your region is here, why are you accessing data on people? So it would be much harder in a global, kind of in a global operation, but.

MR. ROTENBERG: I just wanted to end with a cautionary note here. You know when we talk about audit logs in the 21st century this is not simply the problem of a person accessing a data set from a computer terminal. What we realize

increasingly is the amount of information that a person can pull down from a system off of a server and walk out with in something that's, you know, smaller than a credit card is really remarkable, right?

And I think this belief that through carefully tailored audit logs we can ensure legal compliance and prevent misuse has already been demonstrated many times not to be a reliable operating principle. So we --

MR. WEITZNER: Could I just very quickly though differentiate between operational security risks, which are real, and obviously Snowden and Bradley Manning have demonstrated that there are very real operational risks, and they can entail privacy intrusions, as we saw with the WikiLeaks situation to great harm.

But I would distinguish that from policy compliance problems where in fact the assumption is that an institution, or at least large parts of an institution is prepared to be accountable to a set of rules, but because we don't have fine

grained enough, precise enough audit mechanisms, we allow a lot of fuzziness. We allow fuzziness about who is a U.S. person or not because we can't determine it. We allow fuzziness about what's a terrorism investigation use and what isn't.

We can get much more precise and close these gaps. I agree with Marc that there are, the rogue insider problem is not one that can be solved with the kind of information accountability that we're proposing.

I would suggest that it can be solved by detecting, as Ashkan suggested, anomalous activity by someone who's supposed to be infrastructure analyst but is instead doing something else.

But I think, Marc, you're right to distinguish the two, but I don't think that the difficulty of doing one means that the other is not useful.

MR. BELLOVIN: Here's a quote from Bradley Manning, attributed to Bradley Manning in the WikiLeaks case, weak servers, weak logging, weak physical security, weak counterintelligence,

inattentive signal analysis, a perfect storm.

He was able to get away with downloading all those documents because no one was paying attention. The stuff wasn't being logged or no one was paying attention. Yeah, someone downloading 250,000 documents that should have tripped a flag, if there were enough audits and if people were paying attention.

And that's about, that's an anomaly and that's about the best you can do there.

MR. DEMPSEY: With that, I think we will bring this to close right at the top of the hour. Thank you all very much.

MR. MEDINE: And we're going to take a 15 minute break and then we'll pick up with the third panel. Thank you.

(Off the record)

MR. MEDINE: So welcome to our third panel on policy issues, and I'll turn it to Beth Cook to introduce the panel.

MS. COLLINS COOK: So thank you all for joining us for this third panel of the day, that

certainly for me, and I hope for my colleagues and for all of you, has been very informative and very thought provoking.

So we turn now to the third panel, where we are joined by six very distinguished experts in this field.

And from left to right we have with us Jim Baker, who is a former Department of Justice official and lecturer at law at Harvard Law School.

To his left we have Mike Davidson, who served as both minority counsel and then general counsel for the Senate Select Committe on Intelligence.

We then have Sharon Bradford Franklin, who is senior counsel with The Constitution Project.

Then Liza Goitein, who is the codirector of the Brennan Center for Justice's Liberty and National Security Program.

Greg Nojeim, who is the director of the Project on Freedom, Security and Technology at the

Center for Democracy and Technology.

And Nathan Sales, who is a law professor at George Mason and former Justice Department and Department of Homeland Security official.

So we're going to structure our panel just a little bit differently than the first two panels. We're going to start with a question.

And the question, and we will allow each of the pnaelists five minutes to respond and then a two minute secondary response, is the following, we begin by asking whether based on the publically available information you have any recommendations for change to the programs or whether you believe the programs appropriately balance the potentially competing interests?

And Jim, going alphabetically, I would invite you to start.

MR. BAKER: Well, thank you. Thank you very much for the invitation to speak before the board. I appreciate this opportunity.

And I just would say at the outset I'm speaking just for myself today, not on behalf of

any current or former employer, employers.

And so with respect to thinking about these issues, I mean I guess if I could just for a moment take it up a higher level to sort of make sure that we're thinking about these problems in the right way.

And I guess one of the disadvantages of going last is that a lot of people have said a lot of things and you guys have talked a lot about a lot of things today. But I also get to sort of react and reflect a little bit on what has been said.

And so at the outset, you know, I'm sitting in the back and watching what was going on and thinking about your banner here and thinking about the name of the panel and so on, and it was striking to me that really at the end of this session, I think some of the fundamental, some parts of the name of this board, there is still not agreement on and there was not agreement about today. And I think that complicates your task.

So for example, what does privacy mean?

I think you saw several different versions or several different visions of that during the discussions today. I don't think there is wide agreement on what that means today. And I think that's one of the issues that we're confronting.

And let me back up. There may be wide agreement that there is at least some significant disagreement, let me put it that way.

The same is true with respect to the term civil liberties. What exactly does that mean? It ties right into what is privacy and how do people think about this and how do we think about this in the current era in terms of the types and the variety of communication facilities and devices that people use on a regular basis.

And then how do we think about that with respect to the changes and the growth in the government's ability to conduct surveillance and to store and analyze and understand data.

Another thing that was striking to me obviously with respect to the name is oversight and what does that mean and how do we think about

that?

And reflecting upon these programs that we're talking about today, I guess my question is, how much more oversight do you want? Because you've got all three branches of government involved in these particular activities we're talking about. You've got the President, you've got Congress, you've got the courts, you've got lawyers all over the place running around doing oversight. And so the question is, you know, how much more really do you want?

And that, then I was thinking about, well, okay, so what's going on here? What's really at issue? And so a couple of different things.

One is that either people, the people who are critics of these programs either don't like the design that exists today, the design that's come up, that was passed by Congress, signed by the President and put into place, put into practice, implemented by the court, either you don't like the design or you don't like the people

that are implementing the design. It's one of the two. I don't know what else there would be.

So that is a significant problem. And it's a significant problem that reflects, I think even a deeper issue that you have to try to think about, and I'm not sure how you're going to deal with this.

I'm not sure that I have, I certainly don't have the answer, but it's this, at the end of the day if all three branches are involved there remains some fundamental distrust of the government and the structures that the government has put into place and the people who are implementing these things.

I mean I think that is what is underneath a lot of the critique and criticism. And I don't know how you deal with that. So that's point number one, I guess just in terms of reflection.

In addition, in terms of before I talk about solution, I do want to just mention briefly that these issues are even more challenging than we've talked about today. And I'll just briefly

state we have the cyber threat that we have to deal with.

All of the things we've been talking about today with respect to terrorism exists even to a more significant degree with cyber because of the volume of communications involved, because of the variety of the different types of communications involved, and because of the velocity of the communications.

All of those make all the issues regarding the collection and the analysis of metadata and content even more difficult.

So with that said, in terms of trying to think about structural changes and refinements in the law and what you can do to move forward, I don't think that anybody is going to have a perfect solution to you, to describe to you today.

You can, I think, do some things at the margins to try to improve these statutes, but you know, I'm just really not sure what you can do to have more oversight of these activities that impact privacy and civil liberties. I think it's

just a very tough nut to crack.

Having said that, let me just make a comment. One of the things that I recommend that you think about is to try to simplify the range of laws that apply in this area.

What we have right now, and others have made this observation, what we have right now is a very complex patchwork of statutes that overlap with each other.

And I can tick them off. It's not only FISA, it's Title III --

MS. COLLINS COOK: Actually before you go through the full list, we have six panelists so we're unfortunately going to have to be a little bit stricter on this panel than the last panel. Simplicity.

MR. BAKER: Okay. Simplicity.

And think broadly about the laws that are applied to the surveillance of content and metadata.

MS. COLLINS COOK: Thank you.

MR. DAVIDSON: Is that a color coded --

MS. COLLINS COOK: It is indeed. We have a very helpful green --

MR. DAVIDSON: There are not numbers?

MS. COLLINS COOK: There are no numbers.

MR. DAVIDSON: No numbers?

MS. COLLINS COOK: No numbers

MR. DAVIDSON: Red means stop.

If I could address perhaps a variant of the question that you asked and address it in these opening comments, not the specifics about what might be done with these programs but the conditions upon which they are discussed in several important places, one being the judicial, branch, the second being in the Congress, and then particularly looking forward to the next set of sunset debates, and the third more generally in the public.

With respect to the judicial branch there's of course been a discussion that's gone on since, well at least since 2008 about greater public information about the major decisions of the FISA Court, its reasoning as it approached

various segments of FISA.

And nominees have come before Senate committees and have pledged to proceed on. And that's been going on since 2008, and maybe we're on the verge of a breakthrough.

But without even looking to the past as to what the court has done, bear in mine that in the public information about business records it now appears publicly that those orders are 90 day orders.

And so there's some cycle going on before the FISA Court, which would mean that in days, or at least within months there will be an occasion for the FISA Court's consideration of the extent of any such orders, the legal basis for them.

And then with respect to the development of the program under the FISA Amendments Act, Section 702 of FISA, that's an annual cycle. The statute doesn't limit the government to any particular one year order or how it packages what it does, but it does say that those authorizations are for no more than a year.

And each time the FISA Court considers the government's submissions to authorize another year's collection, it has the statutory obligations that it has at the outset.

Central to those is to consider the compliance that the government system of targeting and minimization and other aspects of the statute have with both the terms of the statute and with the Fourth Amendment.

The statute reiterates the expectation and the requirement that the court will consider the Fourth Amendment in approving or not approving its annual authorizations.

And so within weeks or months, but certainly within the year, there will be an occasion before the FISA Court to consider the basic elements of the authorization that's allowed under section 702.

I think that this board, given its charter and its stature, can play a very important role in helping to improve that process so that there is a greater confidence that the FISA Court

in fact is dealing with the basic issues that have been discussed earlier today, and are being discussed in the larger society, and that there are models out there.

So that in 2002, when the FISA Court of Review considered legal issues relating to the wall between intelligence and criminal investigations, the Court of Review had a process in which outside groups came in, filed amicus briefs, and the court in its disposition of the matter addressed issues that had been raised there.

And in 2008, when the Court of Review had an appeal from the Protect America Act, which had a resemblance to, but it's far from identical to the system created by the FISA Amendments in 2008, it issued a public opinion. It redacted portions of it, but the public opinion dealt with substantial legal issues.

So finding a way for people outside the system to bring before the FISA Court important legal issues and for the FISA Court to then

communicate to the public at large is something that's been experienced.

Now the modeling of it could very well be different and it would take an initiative, I would believe, by the Department of Justice.

And I do believe that the board in its communications with the Executive Branch could help to make the case that we're now at a point in which there should be that form of public discussion.

And perhaps it could go to the extent of helping to identify the questions that should be considered on a public record.

Now the intelligence community is going to have some choices to make. It is loathe, and understandably loathe, when there have been improper disclosures to acknowledge the validity of those disclosures.

But there's also a reality out there. In fact, there appears to be public information about matters that are at the heart of the annual approval, of the targeting procedures of the

government, and the minimization procedures of the government.

And some way can certainly be found to now call for a process in which those are discussed against the requirements of the statute, which are both statutory and the call for an annual consideration of Fourth Amendment compliance.

MR. MEDINE: Let me just make also, in the interest of time and moving on, I think --

MR. DAVIDSON: You can interpret that as red?

MR. MEDINE: That's our timekeeper. So if you have additional comments you can make them in a later round.

MR. DAVIDSON: Sure.

MR. MEDINE: We appreciate that. Sharon.

MS. BRADFORD FRANKLIN: Thank you very much for the opportunity to appear here today, and I have already filed a lengthier statement on behalf of The Constitution Project so I will be more brief in my comments.

The short answer to your question is yes, we do believe that there are changes that should be made. And I just want to make two quick points before I get to summarizing what some of those recommendations are.

First, with regard to the PCLOB's role in assessing counterterrorism programs and whether the safeguards for privacy and civil liberties are appropriate, part of that role obviously, and the discussion at this morning's panel was whether existing programs comply with existing law including the Constitution.

And that is a very important assessment and we have already filed in our prepared comments our views on some likely legal violations there.

But beyond that, the PCLOB's statute talks about assessing whether the protections are, quote, appropriate, and, quote, adequate.

The board is not limited to making recommendations for compliance with the Constitution and existing law. And so I would urge you to be forward-leaning in the

recommendations that you do make.

There will be plenty of voices within the government pushing for strong powers in counterterrorism. And we know now from the recent disclosures that the administration, whatever administration it is, is likely to interpret existing law aggressively to the maximum extent that they believe they can justify under the words of existing statutes.

So I urge you to really take seriously the role to push for adequate and appropriate safeguards in law to make sure that we're protecting both our security and our civil liberties.

Second, the PCLOB's statute explicitly provides a role for informing the public, including holding forums like today, and in making sure that you're of course including the reports to Congress are available to the public to the greatest extent possible.

And I think that this transparency role is really a critical one the PCLOB can play, in

addition to making specific recommendations for a forum. And there's been a fair amount of discussion about that in the earlier panels, but I would urge you to take that role seriously, the place where you really can make significant change in pushing for a full disclosure.

The administration so far has been trying to release some more information in response to the leaks, but I don't get the sense that we're getting a full picture.

They are perhaps, you know, understandably picking the facts to release that they think will support their case. And you are authorized to get a full picture and to hopefully push for more of a full picture to the public.

So I'll try to be somewhat brief in summarizing the recommendations. We did outline some in fair detail in our written comments.

And I just want to emphasize that a lot of, most of the recommendations that are included in our comments are actually ones that come from The Constitution Project's Liberty and Security

Committee, which is a bipartisan committee, well before any of these disclosures.

These were things that our committee felt were necessary to better protect privacy and civil liberties, just looking at the statutes before we knew more details about how they are being used. And they fall into a couple of categories.

First, tightening the standards for when the government should be able to collect information in the first place. Second, regulating very strictly what uses can be made of the information once it is collected. And third, again, on transparency.

As far as tightening the standards, it's very important that we have strict rules to require a sufficient connection to terrorism before this information is collected.

The sheer fact that it is useful to the government for counterterrorism cannot possibly comply with Fourth Amendment standards and it's not the kind of society that we live in. Usefulness is not enough. We need to make sure

that there's a connection to terrorism.

And frankly, this should help the efficiency of the programs too. We want the surveillance to be conducted on the, quote, bad guys and the people we have reason to believe that they are a connection to terrorism.

In the context of Section 215, although we do not believe that the existing law does authorize the bulk collection of the telephone metadata that has been reported, although I haven't seen the underlying order, we would urge that at this point Congress should, you should recommend that Congress amend the Act to clarify that that's not permitted under 215 or any other authority, and specifically recommend tightening the standard for issuing an order under Section 215 to require a showing to a judge of specific and articulable facts demonstrating that the material sought pertains to a suspected agent of a foreign power or a person in contact with or directly linked to such an agent. So restoring some of the earlier standards.

In the context of Section 702, we have similar recommendations to restore the requirement that foreign intelligence be the primary purpose of the surveillance, and also to require the government to make a greater showing to the FISA Court of the actual foreign intelligence purpose, and more of a showing that it is not likely that it will be intercepting large quantities of communications of U.S. persons.

We've heard a fair amount of discussion this morning about justifying collection where an American is on the other end, I'll try to be quick here, when we know it is targeted at a foreigner. But we need to make sure that the word incidental has more of its common, everyday meaning in that targeting.

Then there should also be strict limits on data once it is collected. We had reference, Judge Robertson mentioned a recommendation that we made for post-collection warrants in the context of 702. I'd be happy to discuss that more in the questioning, if you are going to seek information

on a specific U.S. person in an existing database.

And finally, we have a series of specific recommendations on transparency, including releasing significant opinions of the FISA Court and more details on the extent of interceptions of U.S. person information that have gone on in the past.

And I appreciate the opportunity. Thank you.

MR. MEDINE: Thank you.

MS. GOITEIN: Thank you very much for the opportunity to participate.

On this panel, as you said, our task is to leave aside the question of the program's legality and focus on whether they strike the right balance between our security and our liberties. And I believe that the known threat to liberty from these programs exceeds any known benefit.

Now in my line of work I often get accused of invoking phantoms of lost liberty, as John Ashcroft once said. So let me start by

saying that I recognize that this is a remarkably free country. The vast majority of Americans go about their lives and speak their minds without fear of persecution.

But that has not always been the case at periods in this country's history. Throughout much of the cold war our law enforcement agencies and our intelligence agencies spied on Americans, not solely for the purpose of preserving security, but sometimes for the purpose of impeding social justice movements or harassing political enemies. Innocent Americans had their careers and sometimes their lives ruined.

When these abuses came to light in the 1970s, Congress and executive agencies implemented a range of laws and policies that establish a kind of golden rule. And that rule was law enforcement and intelligence agencies may not collect information on Americans unless they have some level of individualized, fact-based suspicion that the person is involved in some kind of wrongdoing or is an agent of a foreign power.

Now the exact level of suspicion would depend on the kind of information the government wanted to get and how. This golden rule served us well for decades.

The 9/11 Commission found fault with a lot of government practices, but it never said we need to collect more information about Americans with less reason for suspicion.

Nonetheless, since 9/11 we have seen a steady and rapid erosion of the level of suspicion that is required for our law enforcement and intelligence agencies to collect on Americans.

The FISA Amendments Act, national security letters, FBI assessments, electronic border searches, these are all instances in which the required level of suspicion has been lowered, in some cases to zero.

The programs we're talking about today fall squarely within this category. Section 215 already weakened preexisting law by allowing the acquisition of tangible things with a very low showing of relevance.

We've now learned that the government and the FISA Court have interpreted relevance largely out of existence, so there's no individualized showing required to get information, American's information.

That means it's up to the Executive Branch to police itself when it comes to actually using that information.

Section 702 of the FISA Amendments Act on its face doesn't require any individualized suspicion. Now it targets foreigners overseas nominally, but what we've learned is that the government Section 702 programs tolerate a massive amount of so-called incidental and inadvertent collection of American's information.

Again, this incidentally acquired information is nominally master deleted, but that relies on self-policing. And also, if you look at the targeting and minimization procedures, they tell a much more complex story in which there are many loopholes for keeping and sharing this kind of information.

When you get rid of the requirement of individualized suspicion for collecting on Americans, you reopen the door to the kinds of surveillance abuses we saw in the 40s, 50s, 60s and 70s.

And when you free government officials from the requirement of some sort of factual predicate for investigation, you open the door for them to fall back on conscious or subconscious prejudices, whether racial, or religious, or ethnic, or political.

Now if there were evidence that these programs were uniquely effective, then we might be willing to risk these downsides, but the burden should be very high in terms of the proof we require. And to date, all the government has told us is these programs have helped to disrupt terrorist plots.

That's not even the relevant question. The question is, have these programs thwarted real significant terrorist attacks that could not have been prevented using more narrower methods or more

narrow methods?

So I'm very much hoping that the PCLOB will insist on getting the information necessary to make that assessment. And if it turns out that these programs are useful and if it turns out that they comply with the Fourth Amendment, then as a society we'll have a very difficult choice to make.

Until then, we are weighing a known and serious risk to liberty against an unknown and unproven benefit.

MR. NOJEIM: Hi, I'm Greg Nojeim. I'm with the Center for Democracy and Technology. As it happens one of the PCLOB members is also employed by CDT. We have walled off our work from each other and don't discuss PCLOB issues.

I think we've strayed a long way away from the world that was envisioned in our Constitution where you don't have to worry about government surveillance unless there's evidence that you're up to no good. My gosh, we've moved so far away from that.

When it comes to these two programs I don't think that they adequately protect privacy, and I will focus with respect to the Section 702 program primarily on transparency, where I think PCLOB can play a huge role. And with respect to the 215 program --

MR. MEDINE: Move the mic closer to you.

MR. NOJEIM: With respect to the 215 program, I think that one is illegal and that the PCLOB should make a recommendation that it be discontinued.

On 702, there are some critical questions about FISA Amendments Act surveillance that have never been answered that we would urge you to take up in your report, or to encourage government officials to answer.

The first is whether the FAA can be and is being used to do bulk surveillance. That means surveillance of a large quantity, a large proportion of the communications between Americans and people who are abroad.

Because you can target anyone you

reasonably believe to be abroad, just how much of that surveillance is going on?

Second, the Washington Post reported that when it comes to targeting that a 51 percent likelihood of foreignness was good enough. Well, it's not good enough for me and I don't think it's good enough for the American people. That's a coin flip level of certainty.

I would think that there would be, and the procedures that have been leaked suggest that there is, more attention to foreignness than that. But I think PCLOB could play an important role in clearing up the 51 percent number.

I also think that when you look at the purpose for which the surveillance can be conducted in the 702 program, it's very broad. And I would think that all of the surveillance that's authorized under that program is not being conducted because it wouldn't be useful.

For example, it appears that because collecting foreign intelligence information is all the purpose that you have to have, that that would

cover, for example, collecting up all the email of people that have protested outside a U.S. base in Germany. I don't think that the government is ordering U.S. providers to turn over all the information because I don't think it's really what the government is looking for.

What I think is needed for 702, in addition to more transparency, is more FISA Court involvement, not less, where the FISA Court actually authorizes the surveillance, not just guidelines.

And I think that the PCLOB should give consideration to the purpose of the FISA surveillance and whether it could be limited to 18 U.S.C.(e), I'm sorry, I don't have the exact statutory citation here. But just the first part of the definition of foreign intelligence surveillance, which would make it much more limited.

With respect to Section 215, I think that that surveillance is unlawful. It's overbroad. It can't be the case that everyone's telephone

records are relevant to an investigation because if that's true, then everyone's records of any type are relevant to an investigation because they fit into a mosaic and could be used to engage in more learning about what might be actually relevant.

I think the most important change to Section 215 is the one that Sharon outlined to require that there be a tie to an agent of a foreign power, specific and articulable facts giving reasonable grounds to believe that the information sought pertains to an agent of a foreign power or a person in contact with such a person.

I think also the PCLOB should make it clear, I think this is already clear in the statute but apparently not to the NSA, that Section 215 is not about prospective surveillance, it's about records already in existence.

Perhaps an exclusive means provision should be added to the pen trap statute to make that entirely clear.

There should be clarity about the particularity that's required and more work on transparency with respect to the surveillance.

Finally, I will just say this, I don't think that FISC oversight is serving us adequately at this point.

It seems to have been the case that one judge of the FISC issued the orders that determined that this information about all phone calls were relevant, and that when those orders were issued, the other judges on the court didn't even know. I mean that is not a system that I think has the oversight that Congress intended.

There ought to be explicit authority to consider all constitutional claims, and I think the idea of an ombudsperson is a very good one, and I'd like to discussed that later.

MS. COLLINS COOK: Thank you.

MR. SALES: Thank you to the members of the board and my fellow panelists for asking me to participate in this important and interesting conversation.

I'd like to take a step back and look at the big picture concerning surveillance. It seems that the programs that have been leaked to the press are examples more or less of what we might call programmatic surveillance. Greg called it bulk data collection.

Programmatic surveillance is something that's familiar to a lot of intelligence personnel, but those of us who are lawyers probably haven't encountered it all that much.

We're more familiar with individualized surveillance where cops think that Tony Soprano is up to no good, they therefore ask a court for permission to wiretap him to come up with evidence that they can use to prove his guilt.

You move, with individualized surveillance you move from suspicion, to an individual, to evidence.

Programmatic surveillance is in a sense the exact opposite of that. We don't have a particular target in mind. In fact, the whole point of the surveillance is to develop enough

information so that we can find the bad guys.

So programmatic surveillance therefore relies on bulk data collection and screening it through various algorithms or analytical processes to identify pieces of information, individual data points that might be important.

Programmatic surveillance, I think what I'd like to talk about is its potential benefits and how to do it in a way that respects privacy values, and rule of law, and civil liberties values as well.

The benefits are fairly straightforward. Programmatic surveillance is an important tool for identifying unknown associates of known terrorists. The process is called, as you know, link analysis.

We know that Mohamed Atta is up to no good, let's find out who is in his social network because they may also be up to no good, and we can use that to trigger further investigation.

There's a report from 2002 indicating that a rudimentary form of link analysis actually

would have enabled investigators to identify all 19 of the 9/11 hijackers. Still, we start with two hijackers who were known to have attended a terrorist meeting in Malaysia. Let's look at their passenger reservation data from their various airlines travels and find out what we can learn.

Well, it turns out that a number of people had used the same frequent flier number as these two terrorists. It also turns out that other people had used the same addresses and credit cards as these terrorists.

Building out from the initial two suspects, it was possible to put together a fairly detailed portrait of their social network leading us to all 19 of the 9/11 hijackers.

So programmatic surveillance has the potential to yield some important national security gains, not merely hypothetical ones, but actual concrete national security gains.

The question for me is, how do we do it in a way that is consistent with our rule of law,

values, and with our commitment to privacy and civil liberties.

I want to propose a series of principles that I think can help guide our judgment as to whether any particular program, including these programs, live up to our values in addition to protecting us from national security threats.

There's two basic sets of principles that I personally would like to see reflected. The first set has to do with the formation, the architectural considerations. When building a system of programmatic surveillance, how should we design it?

And the second set of considerations concerns operational features. What sorts of safeguards should we build into the system so that when it operates it does so in a privacy and civil liberties friendly way?

As far as formation goes, one of the most important principles to me is anti-unilateralism. The Executive Branch shouldn't be doing programmatic surveillance on its own. It should

rather have to obtain authorization, legal authorization from Congress, perhaps also from the judiciary. There have been examples of the judiciary signing off on and approving in bulk programmatic surveillance programs.

I also favor maximum transparency and public debate. The public should be informed of the government's plans as much as is possible with operational security, so that an informed deliberation in the public can take place and so Congress's deliberations can thereby be informed.

I also want clear legal authorization for programmatic surveillance. I think it's important for Congress not to hide elephants in mouse holes.

If we're going to have a system that authorizes bulk data collection, it should be approved transparently and expressly, rather than something that's simply hidden in the penumbral emanations of various other statutory provisions.

I also think it is important to prevent mission creep. These are important tools to be used to protect against existential threats and

mass murderers. I don't think we should be using these sorts of tools to go after tax cheats. I want a firewall that prevents those sort of tools from bleeding over into routine ordinary investigations where a lot less is at stake.

As far as the operational principles are concerned, the basic idea here I think is to substitute for restrictions on the collection of data, restrictions on the use of data.

As the government acquires more and more information on the front end, it becomes more and more important to substitute on the tail end restrictions on who can access it, what can be done with it and so on.

I see I'm nearly out of time so let me just finish this thought very briefly. There's a couple different type of checks you could have in mind, external checks, judicial oversight, ex-ante approval before you conduct surveillance or access the data, ex post oversight audits and reviews of surveillance that has taken place in the past.

Internal checks are also an important

part of the conversation, inspectors general, the PCLOB itself, and other forms of internal Executive Branch oversight can help prevent the sorts of abuses we saw in the 70s and that nobody wants to go back to. Thank you.

MS. COLLINS COOK: Thank you all. And we will now ask you to, if you have some thoughts, two minutes each.

And one thing I did want to mention, and building on something that Jim had said earlier was that we're really looking for solutions here. We're very much looking for recommendations, we're looking for concrete and specific ideas that can be discussed, that can be assessed, that can be analyzed.

And you know, we spent a lot of time today on the framework of what we're talking about, and I hope that over the rest of the day that we can really start exploring some very specific options for how these programs might be done differently if necessary.

MR. BAKER: Okay. So let me focus on

that and try to get very, there's a lot of stuff to talk about. Let me focus on one thing in particular, transparency.

MS. COLLINS COOK: Yes.

MR. BAKER: Okay. So back to my earlier comment in terms of that may be one thing that would help enhance trust in government, okay.

So with the transparency of the FISA Court orders and FISA Court proceedings, so I've got just a couple of observations.

And just by way of background, I was in charge of representing the United States in front of the Foreign Intelligence Surveillance Court from 1998 till 2007. So I dealt a lot with the court in that time period.

Two things. One, this will be easier going forward than it will going back. So if Congress were to mandate in legislation that from here on some type of rulings by the FISA Court would have to be disclosed, then that's going to be easier because the judges, I think, will be able to write opinions knowing that that's the

case.

Going back I think there's two problems. One is the intertwining, I think this is why it's taking so long to declassify all this stuff is that the intertwining of classified facts with legal analysis as you go through makes it difficult to extract the two pieces in a way that will give the American public any real information, as opposed to just pages and pages of blacked out stuff, or text with a lot of blacked out stuff. So going forward I think will be easier than going back.

Secondly, you have to understand that not everything that the FISA Court does is reflected in some opinion, I think Judge Robertson was talking about this before, some opinion that's what like you're used to seeing in the normal judicial proceedings with other courts.

A lot of it is based on you submit an order, the court says, hmm, you want to do X, well, we think you should have minimization procedure Y to go along with that. The government

works that out, okay, fine. Then the next time you file it, you just have X plus Y is built into the package. There was never any opinion. There was never any ruling like that. It's just an order from the court and that's what you have.

So there's a lot of back and forth that is not going to be apparent in some kind of big judicial opinion like people think about.

MR. MEDINE: Just to clarify the recommendation, so would you envision on the going forward basis that where there are opinions that there essentially be an unclassified summary or syllabus of the decision and there be a classified, more detailed decision addressing the specific facts of the case or something that they need to be classified?

MR. BAKER: Basically, yes, because that way if the court is writing the summary, the court can say what it wants to say knowing whether it will become public. As opposed to somebody, I mean I'm sensitive to this, as opposed to somebody else writing some summary of some decision that

was written, and whether they get it right or not is another matter.

MS. COLLINS COOK: And Jim, on that point, I think one of the things we've struggled with is I think it's too strong to say it's a red herring, the declassification of previous opinions issued.

And one thing I would like your opinion on is whether or not it would be likely a more efficient course to simply direct a summary of past opinions, rather than to go through a declassification process of existing documents.

MR. BAKER: It would be more efficient, the question is would it be accurate and would people trust it. And would it accurately reflect what the judge's, or that particular judge who may not be on the court anymore, actually thought when he or she wrote that opinion. That's I think the trouble that you'll have.

So I'm not sure that that -- I'm not sure it's going to work in terms of summary.

You could, I mean I guess you could have

some type of analysis, I don't know, by OLC or something, where you mandate an analysis, comparison of the body of FISA Court law with the body of law that's out in the public. I don't know, you could think about things like that as well.

MR. DAVIDSON: Well, the government has experience in producing public documents based on underlying classified documents.

So in January of 2006, the Department of Justice took a portion of a May 2004 OLC opinion, a portion that then dealt with the January of 2006 concern, content collection under the President's surveillance program, and it produced a white paper.

That white paper was extraordinarily informative to the debate that then followed in Congress because it pointed to the fact that the government had been relying on the authorization for the use of military force for the content collection part of the President's surveillance program, and it elicited a considerable debate and

ultimately legislation on what it took to convey that there was some variant to collection under FISA, to what extent was FISA exclusive in the face of another statute.

So it has experience doing that. It has recently produced a white paper on drugs, on targeted killings. So it has done that.

And that also gets done in any litigation in which there may be classified information in which the government works with the court to produce an unclassified version.

It also need not just be a summary. There may be entire parts of a relatively small number of decisions that are in fact unclassified themselves.

And just do this to imagine it, if it is significant what the term relevance means. It wouldn't be surprising to find in a major decision or two how the government asked the court to draw from five different opinions of the United States Supreme Court in order to understand what relevance may mean in certain situations.

So just as another example, in the May 2004 OLC opinion, which was then made public in 2011, at least as to those parts that dealt with content analysis, there's enough of an indication there that relative to the question of reasonableness the Department of Justice looked to border search decisions of the Supreme Court, or other decisions of the Supreme Court about how much of some span of collected material needs to be on point in order for a government search to be a reasonable search.

So summaries are a possibility, but there are other mechanisms that are available in order to get the result of a broader public discussion. And I think I've used my two minutes.

MR. MEDINE: Yeah, why don't we move on to Sharon. Thank you.

MS. BRADFORD FRANKLIN: So two recommendations on how transparency can improve oversight.

One is by addressing the problem that many of us have been talking about in terms of

secret law. So in the morning panel Ken Wainstein made a comment that when members of Congress are expressing, you know, surprise at how a law's been interpreted, that's not what I thought I was voting for, that's just like any other law.

Well, the difference, unlike the RICO example he gave, RICO, there are published opinions on how RICO's being used. You can see what prosecutors are using that for.

Here it took a leak of a classified order for us to know how Section 215 was being interpreted. It shouldn't take a leak for us to know the legal interpretations that the Executive Branch and the FISA Court are applying.

Now that's different. There are certainly going to be classified information woven into those orders. I don't deny that in any way. But the actual understanding of what the law means should be public in the first place and that will facilitate a meaningful public debate over whether that's an appropriate use of the law in a legal authority.

The second is greater transparency for some of the auditing type practices that the second panel was talking about, to some extent that review again be classified. Maybe the FISC can play a greater role, this board can play a greater role, and Congress.

But in terms of reporting on the extent to which the minimization procedures are actually successful, to what extent are they limiting the collection of American's information, how much of that is being captured?

But to some extent we can have public disclosure there as well on statistics that are anonimized. There can be a much greater level of public reporting on that as well, and that as well can affect the public debate and have an informed consideration over what those authorities should mean.

MS. GOITEIN: Two quick responses to what other panelists have said and then some recommendations.

First Jim said that, you know, we have

all three branches in government engaging in oversight, what more could we want? I think it's important to point out that the oversight that we have right now is a kind of oversight-lite.

Oversight by congressional committees in skiffs looking at classified information does not work the same way that regular congressional oversight does because these are elected representatives who answer to their constituents and they answer to their donors.

And if those people aren't on the phone, you know, Jack Goldsmith said this himself in his book, Power and Constraint. The institutional incentives are not there for robust oversight in the intelligence committees. It's just not the same as regular oversight in an unclassified setting.

Similarly with the FISA Court, for all the reasons we've talked about, it does not operate in the way that a regular court operates. So this is a slightly different version of oversight than what we usually mean when we talk

about checks and balances.

On the point that programmatic oversight, sorry, programmatic surveillance to try to identify who the terrorists are necessarily means bulk collection, I think we don't want to conflate those things.

I agree that contact chaining can be a very important way to find out who known or suspected terrorists are talking to. You don't need my metadata to do that. You don't need Sharon's to do that. You work from the information you have and you branch outward.

All of the examples the government has given thus far, the Zazi example and any of the other specific examples of how it's used its authorities are examples that, from at least the information the government has made public, did not require bulk collect versus contact chaining outward.

Finally on specific recommendations, I'm talking fast, I agree with Sharon and Greg on how to amend Section 215. I agree with a lot of

what's been discussed about the FISA Court.

On Section 702, I think it was Ken Wainstein who said, well, it's not workable to get individualized orders, and then we had Steve Bradbury saying this is the way it's been since 1978.

FISA looked very different before 2007, and it required individualized orders in order to get any international communications involving Americans.

Now we heard today that that became unworkable because the FISA Court couldn't deal with the number of orders. We heard that, I think from Steve. I didn't hear Judge Robertson say that. He seemed to be saying that the FISA Court actually worked quite well except for the issue of adversariality.

So my recommendation would be to go back to the pre-Protect America Act of individualized orders for any communication involving an American. And I think that would be more constitutionally sustainable as well.

MR. NOJEIM: It would be useful if unclassified summaries of significant FISA Court opinions were made public. It is important that if you make that recommendation that you articulate a standard that the summary must meet.

For example, in the Classified Information Procedures Act the summary that the defendant must receive has to provide the defendant substantially the same opportunity to defend as would the classified information itself. That's a useful standard.

It's certainly not a standard that would be appropriate here, maybe something along the lines of, the summary must inform the public of the nature of the legal question and how it was resolved. That might be useful and that might not even be enough.

How would the summary be prepared? In the CIPA context the government prepares it and then there is a fight, a fight about whether the summary meets the standard. I think that then the judge resolves that fight.

I think some fighting is good, and that maybe there ought to be an ombudsperson who takes the position that, who tries to take the public's interests into account in having an adequate summary.

And one word on programmatic surveillance. We haven't done that on Americans. We don't do that on Americans. We don't collect all records about Americans for the purpose of watching all of us.

Programmatic surveillance, if it occurs, is something that's about people who aren't in the U.S., I think. And if that's not the case, well, we need to learn a little bit more about exactly what programmatic surveillance is being conducted.

MR. SALES: I think Greg's right but not for the reason he thinks he is. We don't do programmatic surveillance on Americans because we do not in fact look at the data of all Americans.

My understanding of the 215 program is there's a distinction between the collection of the data, which then goes into a warehouse like in

Indiana Jones, right, next to the Ark of the Covenant.

And then the second stage of the process is upon a showing of reasonable suspicion, the individualized determination that we're all calling for, or that some of us are all calling for here, that is the moment at which humans eyeball the data, right.

If you're an American, Google right now knows an awful lot more about you than the NSA. And the only circumstances in which the NSA is going to be looking at the data that has been collected under 215 is if there's a reasonable suspicion that the data is relevant to an ongoing investigation to protect against terrorism or espionage.

Good, right, if there's relevant data to a terrorism investigation, I think the feds should be looking at it.

But I think the critical question is how strong is that firewall that prevents the feds from looking at that warehouse of data in the

absence of the necessary predication, individualized suspicion? And that goes back to the questions about oversight.

Now as far as specific recommendations are concerned I have a couple. The first one is, has to do with minimization. So I'm concerned, having reviewed the minimization rules that were leaked recently about mission creep.

I think the standard for the use of data collected through programmatic surveillance for other purposes is if we find evidence of federal criminal, or actually criminal activity. I think that's far too low a standard. These sorts of tools are incredibly important for protecting against terrorism.

The cost benefit analysis looks very different however when we're talking about running down a tax cheat who's two years behind on his 1040s, right. I prefer to see a much stricter standard there.

You can use this information for investigations of important federal crimes, or

crimes involving the threat of death or serious bodily injury, or child exploitation, something along those lines.

Also my second recommendation is to consider more thoroughly whether Section 215 is the appropriate vehicle for programmatic surveillance of business records.

I can see some potential value in collecting that data, right. In order to do programmatic surveillance, in order to connect the dots, you have to have a big data set. It's no good to say we're only going to collect data on Mohamed Atta if we don't know who Mohamed Atta is in the first place. That's the whole point of the collection is to develop the data field that allows us to identify the bad guys. So it's no good to say you can only collect on bad guys. We don't know who they are.

I'm not sure that 215 is the appropriate vehicle for donig this. As several other panelists have said this seems to have been intended to go for individual records rather than

bulk records, records already in existence rather than mandating the creation of a huge data set.

So I think further exploration of whether Congress should consider additional legislation to put this on a more solid legal footing would be appropriate.

MR. MEDINE: In the first panel in particular we heard a lot of questions raised about the FISA Court and how it could operate in more of an adversarial way because that's how our American litigation system works best is when there are people on different sides.

And many states around the country have public advocates appear in the utilities context where a utility seeks a rate increase and individual consumers don't come in and oppose it, but there's a governmental entity, a public advocate who comes in to argue the citizen's side of that question.

Should there be an institutional, in your view, institutional entity that appears as a government entity or with appropriate security

clearances, who appears to oppose FISA Court orders and have the chance to litigate with the government, or should there be some other structure to create more of an adversarial context?

MR. BAKER: Sure. So this has been talked about for years number and it's not been adopted, and I can speculate why.

But so just a couple of quick observations. So number one is you're trying to balance, I think, the legitimate need for the President to obtain timely and accurate foreign intelligence information with the privacy and civil liberties of Americans, right.

And so you're trying to do something quick and well, okay. And so where you have to be careful, I think in this area, this can be done, I think you could create such an entity. You can give, maybe it's a federal employee of some sort and the person has the right clearances and they're dropped into the system somehow. I mean there's probably some way that you could work it

out.

But there is a lot of process that goes on already within the agency before the request comes over to the Justice Department, at the Justice Department, back and forth with the agency, with the FISA Court, which has obviously the judges on it, but it also has a staff of permanent legal counsel who are senior attorneys, you know, experienced, who go back and forth with the government all the time. You know, this is part of the system now.

So if you now interject yet another person into the system you have to think about, okay, what is that going to do to the speed and agility of this program? I don't have a good answer for you, but I think that's part of the reason why it hasn't been adopted before.

We got pounded on all the time because we were too slow, we demand too much from the agencies, all kinds of complaints. So that was what was happening at the Justice Department on a regular basis. That's what we were hearing.

So if this new person then asks questions, demands answers, you're going to have to think about how it's going to impact the ability of the process to move quickly.

MR. DAVIDSON: I think it would be important to separate a large part of the FISA Court's work which does involve individual applications from, let's call it the occasional task to consider a government application, and a consequent order that sets in motion a larger system of collection, whether it be the annual order under the FISA Amendments Act or 90 day orders under Title V, Section 215.

You know, in the circumstance of the daily work, and I shouldn't say too much about daily work because that was Jim's bread and butter for many, many years, the system is dealing with the kind of occasion that's presented when a United State's attorney seeks a search order in a particular matter, it's very fact-dependent, moving very quickly, in contrast to the point in the process in which there is intended to be

reflection.

So one aspect of the FISA Amendments Act is that the government is to make its application for its annual order thirty days before it seeks to put that order, you know, into effect, so that there is a time for process.

So then the question would become what would be the role of the individual within the system and what could be the role of people outside of the system if legal issues could be identified for some kind of public briefing?

And I think the reality is, but others more involved in the civil liberties community could comment, that unless they have an opportunity to articulate those concerns, the confidence that there's someone from the government who's doing that in a closed setting won't be as strong as if it might be articulated by individuals or groups who take this at heart as central to their purposes.

MR. MEDINE: And Judge Robertson did suggest that judges are used to dealing with

search warrant requests ex parte and are quite comfortable evaluating them, but it was more problematic to do program approvals.

But other thoughts on that? Sharon.

MS. BRADFORD FRANKLIN: So I'd just start out by saying that The Constitution Project hasn't taken a specific position on this proposal, but Judge Robertson is a member of our Liberty and Security Committee and I would encourage you to take very seriously his proposal.

As he pointed out, it's probably less necessary when you're looking at a traditional individualized FISA warrant, which is more analogous to a traditional warrant in the criminal context, and much more important when you're looking at programmatic surveillance or an argument for a new interpretation of the scope of Section 702, or Section 215, or any other applicable authority and building in some kind of adversariness, particularly in that process I think would be very important and would help.

MS. GOITEIN: And I think relevant to

that point, I think Ken said that that's what's happening right now in the Section 702 context is pretty much exactly analogous to the criminal context.

And of course the major difference is that in the criminal context there's an individualized showing of probable cause to get a warrant. There's no such thing as, judge, approve this one year program in which we will get criminal warrants on the following people, on the following unnamed people using these, you know, targeting procedures, could never happen.

So it is very different, the level, you don't have the level of protection that the law affords in a criminal context when you're talking about these orders.

So I do think that it is more important for that reason to inject some adversariality into the process. I think the ombudsman idea is a good idea.

I think the idea of making the court's role less about programmatic approval and more

about individualized warrants goes along with what I was saying before about changes to Section 702.

The only other thing I would add is that I actually think a lot of the functions that the FISA Court is performing today are functions that don't have to be in a secret court. These are functions that could be sort of kicked back to the regular courts.

I mean if, you know, if the FISA Court is an Article III Court, I guess, and so if there's a case for controversy for the FISA Court's purposes, then there's one for another Article III Court's purposes as well. I don't understand why some of these more significant legal questions can't be brought before a regular court somehow.

MR. NOJEIM: Just a thought, in a regular criminal case, yeah, there's a magistrate considers the application of the government for a search warrant, it's ex parte, but there's often a check at the end. You know, you get the evidence and then it's tested, that search is tested in court.

We don't have that test in this context. There's no after the search test about whether it was constitutional or lawful. So to make up for that, you could have the process built in up front and make it adversarial.

I agree with Mike's point that it doesn't have to be the case that the ombudsman weighs in on every warrant application, every search application that comes in front of the court, and with Jim's point that that could slow it down unnecessarily.

But I think you have to leave that to the ombudsperson because to try to articulate, well, don't weigh in unless it's a really important question, you know, it might be an important question that involves one search. And you need to allow for that ombudsperson to decide when that question is important.

MR. SALES: I think there's a lot of value to having a devil's advocate, or ombudsman or, you know, whatever the nom de guerre would be for this official, especially in requests to

approve surveillance programs, as opposed to individual discreet surveillance requests as individuals.

I share the concerns and misgivings about time being of the essence in certain cases, but I think there's a way to write the statute in a way that accommodates those concerns. You know, the devil's advocate shall have a right to participate unless the attorney general certifies that blah, blah, blah.

FISA actually has mechanisms like that already and you could import that kind of scheme where the default rule is you have a devil's advocate performing an adversarial check, but there's an exception for truly exceptional exigent circumstances.

MS. BRADFORD FRANKLIN: Can I just add to that, I think you could have a system where if it is truly an emergency, if it's certified as an emergency, then the surveillance begins. And at that point the ombudsman shows up, you have the proceedings, and if in fact it turns out that it

wasn't permissible, the surveillance ends and none of the information that's been gathered can be used.

MS. COLLINS COOK: So I was hoping to turn to a slightly different topic, and building on some of the issues that have been raised earlier about incidental collection, and I think that's been raised as a concern.

So I was hoping, and actually just to change things up a little bit, the order, if I could start with you, Sharon, actually because you had referenced this, and thinking about addressing the issue of incidental collection, if it needs to be addressed whether it should be at the collection point, the access point, the use point, and how we should think about it and whether there are different approaches.

MS. BRADFORD FRANKLIN: The answer's all the above.

On the collection point, the issue goes to the justification for how this complies with Fourth Amendment standards. So we've known all

along, long before these recent disclosures, that under the FISA Amendments Act it's legal to collect communications where the target is a foreigner located abroad, or supposed to be foreigners, maybe unknown, located abroad, and an American may be on the other end of the communication. And that was called incidental collection.

The problem is that the term incidental suggests de minimis, suggests it doesn't happen very often, suggests it's not that broad in scope, all sorts of things which really are very misleading it appears, in light of recent revelations.

We've had some members of Congress trying to get a scent of that and what the real scope is for a long time and haven't still gotten full information on what the scope is.

But if it turns out that there are a lot of Americans whose communications are being intercepted under programmatic surveillance where you're not making an individualized showing of

suspicion about anyone, right, because you don't even have to have an individual target and show suspicion about Mohamed Atta, or whoever, under the programmatic surveillance, that starts to undermine how you can make an argument that Fourth Amendment rights are being respected for the American on the other end.

So at the collection point we would want to make sure you have a much more rigorous showing to the FISA Court that you have procedures in place to really make it incidental and limited to the Americans on the other end.

Or you should turn to the earlier showing where you had a showing of actual suspicion. So it's more parallel to the other context where you're talking to somebody who there's a criminal warrant against, a Title III warrant or something against them.

Then as far as once post-collection, we've made a recommendation to try and build in safeguards at that point.

So let's say you have this database, you

know that there are communications where Americans are on at least one end in that database, if you want to go through and search through for information on a specific U.S person with recognized Fourth Amendment rights, at that point you should go make your showing of probable cause to the FISA Court.

And we have some more detailed recommendations that we spelled out.

MS. COLLINS COOK: Thank you. Did others want to weigh in on this? Go, to your left.

MR. SALES: Briefly let me answer that question in the context of the 215 program. So one way to design a program to minimize the privacy and civil liberties hit is to minimize the government role with respect to maintaining the data.

So an alternative way of doing the 215 program would be instead of the government serving a 215 order on service providers and saying give us your data, an alternative arrangement would be a data retention requirement.

Congress writes a statute that says ISPs shall keep whatever type of data Congress specifies for a certain period of time.

And you know what, data storage can be costly. Much less so than it used to be, but it still imposes a cost so we're going to provide a subsidy to Verizon to warehouse all this data for a period of five, ten years, whatever Congress thinks is an appropriate amount of time.

And that way the only circumstances in which the government then gets the data are circumstances in which there's a demonstration of whatever the legal standard is, relevance, reasonable suspicion, probable cause, whatever the appropriate standard is, that the information is relevant to an ongoing investigation to protect against international terrorism or espionage.

So you know, this solves or has the potential to solve the problem of misuse, right. There are good reasons why the government might want to have this information and there are bad reasons.

You know, there's a pretty girl in line at the airport security checkpoint, I want to find out, you know, what she's all about. That obviously is a misuse of authority.

Well, if the government doesn't have that data in the first place, but rather sort of outsources the responsibility for collecting and maintianing it to the ISPs themselves, then that sort of scenario is a lot less likely to materialize.

MS. COLLINS COOK: Aren't there a series of other scenarios that could arise, so that's taking as a given that perhaps that data would only be available through something akin to a FISA order, but I think that you would have to expect that were these repositories of information with the service providers instead, that that would be available through a wide range of legal mechanisms, and whether there's a cost to that that should also be considered.

MR. SALES: Absolutely. Yes, so there are at least two mechanisms I can think of for

acquiring that data, the FISA pen trap authority or the 215 authority itself.

Here you're using those authorities to get individualized data points rather than big bulk databases, right.

But part of the cost benefit analysis you have to do is, you know, how nimble is it, how nimble is the process for getting that data?

Maybe you need it in exigent circumstances more quickly than upon application to the FISA Court. So you could build in an emergency procedures exception to that process like we have elsewhere in FISA, I think.

MR. MEDINE: I wanted to get other panelists' thoughts. I mean the proposal does solve one problem, which is the government doesn't have the data and therefore the potential to misuse the data, but it also makes the private sector keep data a lot longer than it might otherwise have.

And one privacy protection is destruction of information, and now if information is being

kept, there's also an incentive for the private sector once they've got all this data sitting around that they're paying to keep or being subsidized to keep, they might as well use it for other purposes.

And then there's the added complication that this data may only be valuable if merged with data from other companies to paint a fuller picture.

So what's the tradeoff here in terms of is it better for the government to have the bulk data under a legal structure with accounting and audits, or is it better for the private sector to have it and only have the government access it on an as-needed basis?

Greg.

MR. NOJEIM: It's better for the private sector to have the data that the private sector needs to engage in its business. I think that a new data retention requirement imposed by the government on the private sector creates more problems than it solves.

As you said, David, if the data isn't there, the bad guys can't get it, it can't be breached, hackers can't get it. If the data isn't there it can't be turned to other purposes.

You know, if the data, if there's a five year data retention requirement, imagine all the entities that are going to want that data. Law enforcement is going to want it, and they're going to want it for all kinds of investigations.

And as we know from our work in other contexts, the standards for getting that data are way too low. It'll be the first step toward other data retention requirements. I mean today it's the phone records, what's it going to be tomorrow, IP addresses? Is it going to be content? I just think it's a very dangerous line to cross.

I think Congress considered it and ultimately decided that it was not the right thing to do.

Again, the right data retention rule is that companies should retain the data that they need for business purposes and they should get rid

of personally identifiable data as soon as they can when it does not serve a business purpose.

MS. GOITEIN: I just want to agree that I think that's not the solution. I think that's equally problematic in its own right to require the telephone companies and the other companies to keep this information.

It reminds me a little bit of the Freedom of Information Act. You have a right to ask the government for records it already has. You don't have the right to ask the government to create records for your use.

I think, you know, the government has a right under certain circumstances to get, or statutory rights anyway, to get information about Americans. But to require us to generate and keep information about ourselves for the government's convenience, it's a form of that to say that companies have to keep this information on us, and it's a slippery slope.

MS. BRADFORD FRANKLIN: And if I could just quickly push back on the notion that the

government should ever have access to all this bulk information without the kind of showing of suspicion or contact chaining that Liza was talking about either.

Professor Steve Vladeck on a panel once, I don't even remember what the context was, but somebody said wouldn't it just be easier if we could gather all this information. He said, yeah, it would be easier if the police could go and break down everybody's door and scoop up everything in our houses.

And you know, it's an extreme example, but the Fourth Amendment is there for a reason. We need to require a sufficient predicate before the government should be able to get this information. The fact that it's easier shouldn't be enough justification.

MS. COLLINS COOK: Jim, I think you --

MR. BAKER: Yeah, thank you very much. Just one quick comment.

I'm not sure where I come out on whether it's better to have the government have it or the

private sector and so on. So I'll just put that aside for one second.

But if, as you're thinking about that if you decide to recommend that the private sector maintain the data, keep in mind, I think, I haven't looked at it in a while, but there are seven or eight different ways in the Federal Code to get dialing data, and under a whole bunch of different types of predications from probable cause all the way down to relevance and so on, subpoenas, and orders, and all kinds of different things.

So if the providers have it and the word gets out in the law enforcement community, which obviously it will, there's lots of ways to get that data that have different levels of oversight connected to them, and so you want to think about that as well.

MS. COLLINS COOK: I think we sort of changed the question midstream, but I did want to invite other panelists to weigh in on the question of incidental collection.

MR. DAVIDSON: What was the very last thing you said?

MS. COLLINS COOK: Incidental. And if anyone else wanted to weigh in on that specific question.

MR. BAKER: I was just going to say I mean, I think -- go ahead.

Just incidental collection is dealt with and deemed and thought to be consistent with the Fourth Amendment because it's reasonable because in part it's done, it's obtained in connection with a legitimate government purpose for obtaining the information, and then there are minimization procedures connected with the acquisition, retention and dissemination of that information.

And so the thinking has been for a long period of time with respect to incidental collection that it's okay because it's reasonable for those reasons.

People may disagree. People may not think that's sufficient and so on, but that definitely has been the thinking.

MS. GOITEIN: I have one very specific thing to say on minimization because even if you go back to an individualized order requirement for American's international communications, you'll still have incidental collection so you'll still need to have minimization procedures.

I do not understand the logic for a rule that if you don't know where a person are, where a person is, then you can reasonably assume that they are a non-U.S. person who is overseas.

To me that is not consistent with the statute where you have to have a reasonable belief that the person is a non-U.S. person overseas. And you know, at a minimum I think that the default needs to be changed.

If you really have no information, no knowledge, the Fourth Amendment I think requires you to assume that it could be a U.S. person and be more protective, not less.

MR. NOJEIM: I think we have to pay more attention to the fact that the statute that we have on the books for FAA surveillance enables the

government to compel U.S. companies to collect up communications of people just because they are abroad.

When you look at the limits that are in the statute, a purpose of the surveillance has to be to collect foreign intelligence information, but the foreign intelligence information is very broadly defined. And it makes sense, I think, to have a broad definition of FII when you're talking about surveilling agents of foreign powers, which is where that comes from, the traditional FISA in U.S.

But when it's just foreignness and collecting information about people who are abroad, I think we might need a more limited collection regime.

50 U.S.C., I'm sorry, 15 U.S.C Section 1801(e)(1) has the description of what foreign intelligence information is, and I think that collecting information about a potential or actual attack by a foreign power, sabotage or international terrorism, clandestine intelligence

activities is already pretty broad and that you might consider whether it is consistent with concepts of international human rights and the necessity that there has to be for collecting information, whether you could limit the collection up front about information about people who are abroad.

We have, we, the United States, has embarked on an international campaign to promote Internet freedom around the world. I don't think that part of that campaign ought to be that mere foreignness ought to be enough to allow for surveillance.

I don't think that our government would say, for example, that the government of Germany should be able to collect the communications of people in the United States just because that's where we are and that we're not Germans. I think you have to pay some attention to that.

MR. DAVIDSON: Can I suggest a focus for the board, and that is the Congress will turn to the many important questions that have been

discussed through the day when it has to, and it will have to initially when the sunset for business records is reached in the middle of 2015.

I think, and this is an opinion, I think unfortunately the sunsets for the FISA Amendments Act and for business records have not been aligned.

An alignment would permit looking and encourage looking at this system in an integrated way. These are all provisions of FISA. Something may have come in through the PATRIOT Act, something may have come in through the FISA Amendments. They're all provisions of FISA and they are intended to, or in fact work in an integrated manner.

So at least by the middle of 2015 the Congress will be turning to this. It's actually not too soon to begin to think about what that sunset debate should be. These sunset debates just creep up on people.

Important to any debate, which is more than a debate of should we now extend it another

four years and get by this temporary crisis and the possible loss of authority.

But if it is to become an occasion to think fundamentally about the collection system that we have, then questions need to be identified well in advance in order to determine which of those should be responded to empirically and which of those are philosophical matters that could be discussed, you know, at any time.

So for example, you know, questions have been raised about incidental collection. And certainly I know within the Senate there are senators who've articulated the importance of having some process by which the intelligence community helps to identify what the actual impact of its collection system is.

Some of those involve privacy concerns. So that one of the problems considered in how deeply one could look at how much incidental collection involving Americans comes in through a system that's not focused on them, but focused on others, is that the process will involve looking

at the communications of Americans. One might invade privacy in the course of trying to learn something about privacy.

Well, there's a balance there. And an entity that is concerned about the overall issue, you know, of the privacy and civil liberties of Americans could begin a consideration that I think would have importance within the intelligence community and the Congress, which is, how do you find out how a system is working? What are the downsides? What are the risks? What are the benefits?

Sometimes, you know, we have to have some infringement on privacy to learn what the infringement on privacy might be.

I'm not suggesting the answer to it, but trying to identify those questions now in 2013 and 2014, rather than waiting to 2015 might mean there's a possibility that they'll be considered factually and deeply at that time.

MS. COLLINS COOK: Thank you. We did want to give an opportunity to the other board

members to ask a question, if they did have one.

Given the time we have and the number of panelists I would urge something akin to a speed round. So if you could go straight to, maybe not red, but yellow, and let's try to keep our responses to a minute to the questions.

Or maybe I'm getting ahead of myself, but I assume you have questions.

MR. DEMPSEY: My question is about 702, and in part it's directed largely to what I would consider to be the three civil liberties representatives in the middle of the table, although I know you all care deeply about civil liberties.

On 702, I think we have to confront the fact the a number of witnesses this morning talked about the sort of historical perspective. To my mind, what really changed around 2000, 2001, etcetera, was the fact that a large percentage of the communications of foreigners passed through or were available in the United States on U.S. territory, in the hands of U.S. based service

providers.

Previously when the government wanted to get the communications of foreigners they had to go overseas. And if you read the history of NSA and so on, you find out about all the different methods that the NSA used overseas to collect the communications of foreigners with zero oversight. Zero.

Now that comes into the United States and it's available from U.S. based service providers. And I do think that there is, you know, credibility to the argument that 702 is a tightening of rules as to what previously was the practice for the government to obtain the communications of persons reasonably believed to be abroad.

And I think that even if you have a tight definition of reasonably believed to be abroad and a tight definition of foreign intelligence value, the numbers would still exceed the capability of any court of any size to do particularized approvals.

So I mean I guess my question is, A, are you prepared to accept that premise, assuming my premises are correct?

And then if that is the premise, that what used to be truly, truly bulk when you did it overseas, now is subject to limitations, yes, you have the incidental collection problem, but what is your reaction to my statement of the premise and the problem and what I see now as the impetus behind 702?

MS. GOITEIN: I would say that it was loosened in one way and tightened in another. So I would say that Section 702 probably did in practice tighten the standard for pure foreign to foreign communications.

But for foreign to domestic communications there had been a requirement, had always been a requirement since 1978, of course before then all bets were off, but there had been a requirement that if an American were a party to a communication --

MR. DEMPSEY: We had, I mean again, this

is ancient history now. We had huge antennas aimed at huge parts of the world collecting everything, including communications from abroad to the United States.

MS. GOITEIN: That you're saying were outside of FISA, that weren't covered by FISA?

MR. DEMPSEY: FISA had no extraterritorial application.

MS. GOITEIN: Right. I mean I think if you interpret FISA as how Congress wanted to regulate the protections that it felt were appropriate for the domestic, I'm sorry, not domestic, the international communications of Americans, then I have to say that I think the government might have found a sort of technological loophole in its ability to, you know, go overseas and catch this information that was falling from satellites, or however it was getting it.

But it doesn't seem that it was consistent with the spirit, even if it was consistent with the letter of FISA, it doesn't

seem like it was consistent with the spirit because Congress --

MR. DEMPSEY: FISA is explicitly orders for collection inside the United States. FISA left totally unregulated, everybody knew that, there's no doubt that everybody knew that it left unregulated what was happening outside the United States.

MS. GOITEIN: I understand, that's why I I'm drawing a distinction between the spirit and the letter.

And also, I mean I think, the law and our understanding of the law has to evolve along with the technology, right?

MR. DEMPSEY: Well, but how do we then, okay, but then technology has changed. What do we do about it, assuming that now things which previously were totally unregulated and truly bulk now fall within some structure of regulation?

Again, I'm just not sure that the particularized, saying it has to be particularized, I honestly don't think that

scales.

MS. BRADFORD FRANKLIN: I want to address that piece and just make clear that actually our Liberty and Security Committee's recommendations do not say end programmatic surveillance.

Instead the recommendations are to build in greater safeguards at the front end to limit the scope of the programmatic surveillance to make sure that foreign intelligence is the primary purpose, and to provide more information to the FISA Court Judge so that he or she can really evaluate the targeting and hone it in and make incidental collection be more like the normal traditional meaning of incidental.

And then post-collection to have more safeguards in effect for American's rights. So we have not actually recommended eliminating all programmatic surveillance.

MR. NOJEIM: So I would accept that as a premise but not the only premise. Another premise is that there is more of that communication and more human interaction that is now available

through surveillance than ever there was before.

And it used to be much less perfect, the ability of the government to conduct the surveillance. Now it is approaching a near certainty level and it seems to me that something has to substitute for the friction that used to be in the system because there wasn't an ability to collect all this information about all human interaction, or close to all human interaction that we have now.

MR. DEMPSEY: Greg, I thought you were going on a different point, which I just want to draw out and then yield to Judge Wald or to Rachel.

But the world, another thing that has happened in the past fifteen, twenty years is the world has globalized. I think we now have the largest percentage of people who are lawfully in the United States, the largest percentage of U.S. persons who are foreign-born since maybe the 1890s, right.

So again, when we were outside the United

States targeting people outside the United States thirty years ago, it was sort of rare that any of those would actually be talking to people inside the United States.

I do think now with globalization there might be an argument that there's a larger likelihood of picking up, Jim Baker is nodding his head, if I can note that, a larger likelihood of picking up foreign to domestic communications.

MR. NOJEIM: I think that's right. And I think it would be useful to have some reporting about the extent to which under FAA that is occurring, FAA, the FISA Amendments Act, that that is occurring.

And the government hasn't even conceded that it can make an estimate, that it couldn't even take a sample of FISA Amendment Act surveillance to figure this out, and I think it could.

MS. GOITEIN: And I think to the extent that what you're saying is that an individualized court order requirement would be unworkable

because now today there are so many international communications that, you know, run through fiber optics and that involve Americans and people overseas, I mean to me that just sort of shores up my point that --

MR. DEMPSEY: No, honestly I was making the argument that a large percentage of purely foreign to foreign is also -

MS. COLLINS COOK: Right, right, and I'm fine with treating those differently.

I'm just saying that to the extent that, because when I talked about an individualized order requirement, I was merely talking communications for which an American was on one end of the communication.

And as far as that's concerned, I mean to the extent that that is such a massive part of the surveillance that the government is doing that it, you know, would slow things down too much to get individualized orders, I mean that just reinforces my point that we have a massive Fourth Amendment problem here if the government is collecting that

much of American's content, communications, whether those communications are overseas or otherwise.

And, you know, whether or not the technology has changed or not, we have to grapple with that Fourth Amendment problem. I realize we're the policy panel.

MR. BAKER: Just real quick, I don't necessarily agree with some of the premises of your analysis, so I just wanted to say that. I don't really have the time, and this is not really the place to have a full-blown discussion of that.

But let me just say something that I've said publicly before, which is pre-FAA, pre-Protect America Act, before all that, my statement is that FISA worked in wartime. And I think that's worth a longer discussion with you all, but I'm just saying that. That was my belief at the time, that's still me belief today.

MR. DEMPSEY: I'm sorry, I didn't hear that.

MR. BAKER: That FISA worked during

wartime.

MR. DEMPSEY: Meaning?

MR. BAKER: Meaning FISA, before the FAA, before the Protect America Act, FISA worked in the sense that it protected the privacy interests, the legitimate privacy interests of America, of Americans, and also protected the national security.

MS. WALD: Okay. This is sort of half a comment, a question, move on incidental collection of U.S. persons.

It's been somewhat, I'm reading a lot of the material that that is out in the public, that's perhaps one of the key points people worry about.

And assuming for the moment we're past, that somehow we get past the individualized warrant and they are collecting incidental information on U.S. persons, two things which have been brought up in your panel and this morning's, and I just want to underline it if you have any reaction, and that is a second look at two parts

of that.

One is the use and dissemination. Now way back in the December reauthorization, this is of course on 702 I'm talking about, there was a debate. Some of the senators were asking, saying, well, can we get some numbers on how many U.S. persons are being collected in the course of this?

My remembrance, I hope it's correct, of it was that they said, no, we can't. Okay. Which led me in reading it to wonder what 702(l) in the actual statute, when it tells the inspector general what to do, it tells him with respect to acquisitions authorized under A of that 702, you should review the number of disseminated intelligence reports containing a reference to a U.S. person identity and the number of U.S. persons' identities subsequently disseminated by the element concerned in response to request for identities, and then with respect to acquisitions authorized, the number of targets later to be determined to be in the U.S. in the extent

possible, whether they were reviewable.

Then all that goes to the attorney general, the DNI, but not to the public. The thought occurs to me, what great risk would there be to national security in disseminating that kind of information if it's already being collected by the inspector general?

Because like one of the panel members, I wondered as we went through many, not just these, but many of the broader contexts of many of the acts and found out that when people talk about minimization, as it was brought up in the morning, it can mean many things.

In some contexts it means, for instance, if they collected it by mistake when they shouldn't have, it goes out apparently. It's deleted. Well, it's taken to some cloud that's not as accessible as other clouds or whatever.

However, if it's incidentally collected it's kept in there. It may be tagged and there may be some attempt to protect the specific identity, but it's kept there and it's used and

it's available for, and it can be disseminated, as I understand it, you know, for not just the law enforcement but to, which I've always wondered what it really means, if it's necessary to make foreign intelligence understandable, whatever that means.

And so it seems to me that that's an area which I think, or at least initially deserves more, because my guess is we are going to end up collecting, however it goes, your premise or not, a lot of incidental information.

And I think that could help, I think, to heighten the trust perhaps if Americans get a better specific notion of both the dimensions and the actual usages. Because I think it's an area of total confusion, at least it's still that for me.

That's more of a comment than a question, so I'll go on to Richard.

MR. SALES: If I could, just a very quick reaction to that. You may as well put me on red because I'll be very quick.

There actually is some precedent for the disclosure of very high level aggregate data about national security operations. So the intelligence budget, the overall sum previously was classified and now has been declassified.

In the criminal law context, every year we have a wiretap report that reveals how many Title III wiretaps were issued. So I think it's certainly possible to have that kind of information.

MS. WALD: But am I not right that in Title III, it's been a long time since I've been in the criminal area, but in Title III minimization means if you collect information in a telephone call, you know, about his wife having problems, that kind of thing, it gets thrown out? That doesn't happen in many, many of these programs.

MR. SALES: I think that's right. Minimization looks different in the Title III programs.

MS. WALD: Yeah, it stays. It stays in

those data banks. It may be restricted, you know, tagged, but it stays there accessible for whatever.

Rachel, I think was the one --

MS. BRAND: It's more of a comment. So we, the PCLOB, have to look at all aspects of this issue and our statute specifically mentions the fact that there's nothing that's more harmful to security or to civil liberties than insecurity.

So you know, we can't discuss privacy and civil liberties impact in a vacuum. And the discussion here has been a little sterile in that regard. You almost wouldn't know we were talking about terrorism because we haven't been talking about it very much, frankly.

So you know, we don't have time to do it now, and I'm, you know, we don't really have time for more questions, but to the extent that you are weighing in with us, providing us advice, it would be useful to know if the broad kind of collection reflected in the alleged 215 order is going to occur, what restrictions or limitations would be

useful?

So destruction dates, limits on access, you know, targeting guidelines and those sorts of things.

You know, just talking about the two sides of the coin here, the government's talked a lot about the benefits of these programs in terms of thwarting plots, and we haven't yet had a chance to fully get into the extent to which that's credible. You know, we'll be getting more information about that from the government as we go along with our analysis.

But if it turns out that these programs are unbelievably useful and have thwarted more plots than you can possibly imagine, and that sort of the national security imperative means that we have to keep them, then what?

I'm not saying that that's the conclusion. I'm just, it would be useful for us to know what your recommendations would be for cabining the privacy damage that that would cause, so to speak. So that would be useful to us going

forward, or to me at least going forward.

MR. DAVIDSON: If I could say a word in relation to that. I'm not sure that the test is always or necessarily most importantly whether some particular plot was foiled by the use of a particular authority.

I do believe there's a way of looking at metadata collection if everyone would permit, even in terms of privacy and civil liberties. The more that is known about who should be looked at more closely, to narrow down the use of other more intrusive authorities because there's a means of identifying those particular individuals who merit that closer look, that may very well work to reduce the intrusiveness of more robust forms of content collection.

And so you wouldn't get out of that benefit that a particular plot was foiled. You may get out of that benefit you didn't have to go out and collect content because you had a way of being reasonably certain that that individual was not in communication with others of concern.

So there may be several questions to ask about the benefit of metadata collection.

MR. MEDINE: Okay. With that, that's a good endpoint for our discussions, so thank you very much for the panel.

We will take a ten break and then welcome any members of the audience who's like to make brief comments on these subjects to come up to a microphone and make those comments. So we'll be back in about ten minutes. Thank you.

(Off the record)

MR. MEDINE: Okay. Thank you. We're going to resume our final session, which is the opportunity for members of the public to make comments. Just in the interests of time, we're going to limit comments to two minutes. And Diane, who has been our timekeeper will enforce that.

So one other thing is that the session is being transcribed and so those who choose to come up and make a public comment have an option to preserve their privacy and be anonymous and don't

identify themselves.

But if you would like to be identified for the record, we would appreciate it, it's in your interest to identify yourselves. So it's really up to the speakers whether you want to be anonymous or not.

AUDIENCE MEMBER: David, thanks. Evan Hendricks, Privacy Times. Thanks for the day, thanks for devoting attention to this.

I think when you talk about the collection of phone records of millions of Americans that are not suspected of any wrongdoing, it's an affront to the Fourth Amendment, which means we're supposed to be secure in our papers and effects. And the intention there is our personal information.

So I think, to me, the credibility of the board is going to depend on how strongly and how effectively will you advocate against the phone metadata collection program. I think there's no justification for it under the Fourth Amendment.

And I think one of the defects in the

process is you are finally the only entity to address privacy within this administration's tenure.

There's been no privacy counselor to address these issues along the way. There's been no privacy advocate in front of the FISA Court. There's been no privacy advocate or anyone to stand up for the American people in front of the intelligence committees. It's totally been missing in action, and I think that's a huge defect.

And on the issue of minimization, I think, I hope you're familiar with William Denny's Thin Thread Program, which he developed back in the early 2000s, which is a way of collecting the information they need and dropping the information on Americans that were not legal to collect at that time.

That program, which costs about three million dollars, and it was rejected, and instead they've wasted billions and billions of dollars on dragnet programs that haven't worked.

So I think you should also look at which tail is wagging the dog, and that's again, the beneficiaries of all this dragnet surveillance have been military contractors like SAIC and Booz Allen Hamilton that have made billions of dollars and have developed programs that weren't as good as ones that were developed in-house. Thank you.

MR. MEDINE: Thank you for your comment. Next.

AUDIENCE MEMBER: Hi, my name is Adam Marshall. We were talking a lot about metadata today, and the various privacy implications associated with it. I just thought I'd bring something to the attention of the board that might help you crystallize kind of what metadata can do.

So MIT has put out a very interesting tool called Immersion. You can find it just by Googling it. And it basically has you log into your Gmail address and then it scans the metadata of your Gmail account, so only the two from fields and the time. And then you can kind of explore your relationships that your metadata says about

you.

And after you're done kind of poking around for a while and freaking yourself out, you are then given the option to either delete your metadata from the MIT server or to let it remain of the server. It's, you know, secure and encrypted and such.

So I would encourage the members of the board, if you have a Gmail account just to try this out to see what it says about you, and then see whether you feel like deleting it or not. And if you do feel like deleting it, just ask what that says.

MR. DEMPSEY: What's the name of the program again?

AUDIENCE MEMBER: It's called Immersion.

MS. BRAND: With an I?

AUDIENCE MEMBER: With an I, yes. It's done by MIT.

MR. MEDINE: Thank you for your comment.

Is there anyone else who would like to make a comment? Any board members like to make

any comments?

All right. I wanted to thank everyone for coming today. I wanted to thank the panelists for engaging in some excellent discussion. I wanted to thank the board staff, Sue Reingold and Diane Janosek for helping make this event flow as smoothly as it did.

These are tough issues. There are strong interests on both the national security and privacy and civil liberties side and we appreciate the chance to have discussions about them.

It does just occur to me in a broader sense, maybe not to lose sight of the fact it's something we take for granted, we have a federal agency here who's hosting a public discussion giving people a chance to critique their government surveillance programs.

I think that in a way is a testiment to what a great country we have, that we can have this kind of discussion and how important it is to maintain these kinds of values to have an open and free discussion about them.

And going forward, the board will take into account what we've learned today, continue to look into these matters and eventually prepare a report for the President and Congress in a public forum on these two programs.

With that, thank you very much for coming.

(Whereupon, at 4:14 p.m., the meeting was adjourned.)

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