PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

Public Hearing Regarding the
Surveillance Program Operated Pursuant to
Section 702 of the Foreign Intelligence
Surveillance Act

March 19, 2014

The public hearing was held at the Renaissance Mayflower Hotel, 1127 Connecticut Avenue NW, Washington, D.C. 20036 commencing at 9:00 a.m.

Reported by: Lynne Livingston

BOARD MEMBERS

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

PANEL I
Government Perspective on Section 702 Foreign Intelligence Surveillance Act

James A. Baker, General Counsel, Federal Bureau of Investigations
Rajesh De, General Counsel, National Security Agency
Robert Litt, General Counsel, Office of the Director of National Intelligence
Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, Department of Justice

PANEL II

Legal Issues with 702

Foreign Intelligence Surveillance Act

Laura Donohue, Professor of Law, Georgetown University Law School

Jameel Jaffer, Deputy Legal Director, American Civil Liberties Union

Julian Ku, Professor of Law, Hofstra University

Rachel Levinson-Waldman, Counsel, Liberty and National Security Program, Brennan Center for Justice

PANEL III

Transnational and Policy Issues

John Bellinger, Partner, Arnold and Porter

Dean C. Garfield, President and CEO, Information Technology Industry Council

Laura Pitter, Senior National Security Researcher, Human Rights Watch

Ulrich Sieber, Director, Max Planck Institute for Foreign and International Criminal Law, Germany

Christopher Wolf, Partner, Hogan Lovells

PROCEEDINGS

MR. MEDINE: Good morning. Welcome to the Privacy and Civil Liberties Oversight Board's hearing on the 702 Program.

I'm David Medine, PCLOB's chairman. It's 9:05 a.m. on March 19th, 2014 and we are in the grand ballroom of the Mayflower Hotel located at 1127 Connecticut Avenue, NW, Washington, D.C.

This hearing was announced in the Federal Register on March 10th, 2014. As chairman, I will be the presiding officer.

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

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

(Aye)

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

I want to thank the many panelists who

will be participating in today's hearing for agreeing to share their views with the Board.

I also wanted to thank the Board's staff, Sharon Bradford Franklin, Sue Reingold, Peter Winn, Diane Janosek, Brian Frazelle, and Simone Awang for their efforts in making this event possible.

Last year PCLOB agreed to provide the President and Congress a public report on two federal counterterrorism programs, the Section 215 program under the USA PATRIOT Act and the 702 program under the FISA Amendments Act. The report on the 215 program was issued on January 23rd, 2014.

Our focus today will be on the Section 702 program under the FISA Amendments Act. The purpose of this hearing is to foster a public discussion of legal, constitutional, and policy issues relating to this program.

A few ground rules for today, 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 documents or information, but they should keep in mind that in some cases they remain classified. Therefore, while discussing them, neither the Board members nor speakers in a position to do so will confirm the validity of the documents or information.

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

The second panel with consist of academics and advocates who will focus on legal issues, including statutory and constitutional issues. After the first two panels we will be taking a lunch break.

The final panel will consist of a mix of academics, advocates, and private sector

representatives and will focus on transnational and policy issues.

Board members will each pose questions during each panel with questions in rounds for each Board member. Panelists are urged to keep their responses brief and to permit the greatest exchange of views.

The program is being recorded and a transcript will be posted on PCLOB.gov. Written comments from members of the public are welcome and may be submitted online at regulations.gov or by mail until March 28th.

Today's hearing will focus on 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.

Information is obtained with FISA court approval based on written directives from the Attorney General and the Director of National Intelligence to acquire foreign intelligence

information. This law permits the government to target non-U.S. persons, someone 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.

We will now turn to our first panel, and I understand that Bob Litt will be making an opening statement for the panel.

MR. LITT: Thank you, and thank you for the opportunity to appear on behalf of the whole group here and talk about Section 702.

I would like to give a brief overview of Section 702 to set the stage, and we'll be glad to fill out some of the points I make here in response to questions.

Section 702, as you noted, enables us to collect intelligence against foreign targets who are outside of the United States while robustly protecting privacy rights.

Under Section 702 the FISA court approves annual certifications submitted by the

Attorney General and the Director of National Intelligence that identify categories of foreign intelligence that may be collected. We then target selectors such as telephone numbers or email addresses that will produce foreign intelligence falling within the scope of the certifications.

The FISA court also has to review and approve targeting and minimization procedures. The targeting procedures ensure that we target only non-U.S. persons who are reasonably believed to be outside of the United States, that we do not intentionally intercept totally domestic communications, and that we do not target any person outside of the United States as a subterfuge to actually target someone inside the U.S.

The minimization procedures ensure that consistent with foreign intelligence needs, we minimize the acquisition and retention of non-public information available about U.S. persons and that we prohibit the dissemination of

such information.

I want to make a couple of important overview points about Section 702. First, there is either a misconception or a mischaracterization commonly repeated that Section 702 is a form of bulk collection. It is not bulk collection. It is targeted collection based on selectors such as telephone numbers or email addresses where there's reason to believe that the selector is relevant to a foreign intelligence purpose.

I just want to repeat that Section 702 is not a bulk collection program.

Second, from a legal point of view persons who are not U.S. persons and who are outside of the United States do not have rights under the Fourth Amendment and so the Constitution doesn't require individualized warrants to target them.

In fact, the type of intelligence that is covered by Section 702 targeting foreigners outside of the United States has historically been viewed as part of the President's inherent

constitutional authority and I'm not aware of any other country that brings this kind of collection under this sort of judicial process.

Third, collection under 702 is subject to extensive oversight by all three branches of government. We can explain the oversight in more detail later, but it includes extensive review of collection activities under Section 702 by inspectors general, by the Department of Justice, and the Office of the Director of National Intelligence. It includes reporting of all compliance incidents to the Foreign Intelligence Surveillance Court, and it includes periodic reports both to Congress and to the court.

As the documents that we've declassified and released make clear, the Foreign Intelligence Surveillance Court carefully scrutinizes our activities under this section. And while there have been a number of compliance incidents over the years, the court has never found any intentional efforts to violate the requirements of Section 702.

Fourth, the fact that the communications of U.S. persons may be incidentally intercepted when we target valid foreign intelligence targets is neither unexpected nor unique to Section 702 collection.

Both the statute itself with its required minimization procedures and the legislative history make completely clear that Congress knew full well when it passed Section 702 that incidental collection of communications of U.S. persons would occur when they're in communication with valid foreign targets.

And it's important to note that this kind of incidental collection occurs all the time in other contexts. When we conduct a criminal wiretap or a wiretap pursuant to Title I of FISA we will likely intercept communications of persons who are not targets. When we seize someone's computer we may find communications with persons who are not targets.

The minimization rules under Section 702 which the FISA court approves is consistent

with both the statute and the Fourth Amendment are designed to protect the privacy of persons whose communications are incidentally collected, while still allowing the use of information that is lawfully collected for valid foreign intelligence and law enforcement purposes.

Finally, I want to close by just emphasizing that Section 702 is one of the most valuable collection tools that we have. Many of the specific achievements of Section 702 have to remain classified so that we aren't revealing exactly who we're targeting and what we're collecting. But it is one of our most important sources of information, not only about terrorism but about a wide variety of other threats to our nation.

And unless one of my colleagues has something to add, I think we're ready to address your questions.

MR. MEDINE: Great, thank you very much for that statement.

I wanted to start off and pick up with

your discussion of incidental collection, and again just to make clear that under this program, even though the target may be a non-U.S. person there will be times when the conversations, either by email or telephone, the person on the other end will be a U.S. person.

And so my question to the panel is whether because you're gathering communications of U.S. persons if that implicates Fourth Amendment concerns? And if so, do you believe there's a foreign intelligence exception to the Fourth Amendment? And if not, how is warrantless collection of information of U.S. persons permissible?

And then to follow up on Mr. Litt's comment analogizing this to a traditional wiretap, is there a distinction here where on a traditional wiretap the court has, there's been a judicial determination with particularity of a particular collection, whereas here there's only broad programmatic court approval and not approval of the specific collection?

So I guess broadly speaking, can you address the Fourth Amendment concerns regarding incidental collection?

MR. WIEGMANN: Sure, I'll take that. So this is, as Bob said, collection that is targeting non-U.S. persons overseas who don't enjoy Fourth Amendment rights under controlling Supreme Court precedent. So that affects the Fourth Amendment analysis.

That's not to say that U.S. persons whose information is or whose communications are collected incidentally doesn't trigger a Fourth Amendment review. It does. Those people still have Fourth Amendment rights, but what the courts have said is that, what the FISA court has said is that the minimization procedures that are in place render that collection reasonable from a Fourth Amendment perspective.

We think there's an exception to the warrant requirement. Before FISA was enacted in the 1970s a number of courts held in a number of different circuits that there is a foreign

intelligence exception to the warrant requirement under the Fourth Amendment, in light of the special needs of the government to collect foreign intelligence, weighed against the privacy interests of U.S. persons concluded that you don't need a warrant when you're engaged in foreign intelligence collection.

So then the only remaining question is, is it reasonable under the Fourth Amendment to collect information on U.S. persons incidentally when you're targeting non-U.S. persons. And what the FISA court has held is that it is reasonable in light of the minimization targeting procedures that we have in place. So I don't know if that answers your question, but.

So the way you look at it is the warrant requirements not applicable to foreign intelligence collection still have a reasonableness requirement with respect to incidentally collected U.S. persons, and that in fact, it is reasonable in light of the procedures that we have that are designed to ensure that we

are targeting only non-U.S. persons.

MR. MEDINE: And could you address why the minimization procedures make it a reasonable form of collection under the Fourth Amendment?

MR. WIEGMANN: Yes, so the minimization procedures address, and the targeting procedures address the acquisition, retention, and dissemination of U.S. person information.

And so those procedures all are designed to protect those U.S. persons whose information might be incidentally collected.

So for example, you can only disseminate information about a U.S. person if it is foreign intelligence, or necessary to understand foreign intelligence, or is evidence of a crime.

You have retention rules. I believe in some cases, for NSA for example, you have a five year retention limit on how long the information can be retained. And so these are procedures that the courts have found protect U.S. privacy and make the collection reasonable for Fourth

Amendment purposes.

MR. MEDINE: And under the minimization procedures I understand that the agency, the NSA, FBI, the CIA have their own minimization procedures and they're not the same with each other?

MR. WIEGMANN: That's right.

MR. MEDINE: Can you address why that shouldn't be a concern that this information is not being subjected to the same minimization standards?

MR. WIEGMANN: So each of them have their own minimization procedures based on their unique mission, and the court reviews each of those for CIA, FBI, NSA, and it's found them all reasonable for each different agency. They're slightly different based on the operational needs, but they're similar.

MR. MEDINE: Would it make more sense then if the same set of minimization procedures apply across the board for this kind of information?

MR. WIEGMANN: I don't think. Again, just to contrast, for example, FBI and NSA that are using information in different ways. The FBI has a little more latitude with respect to U.S. person information in terms of criminal activity and evidence of a crime than NSA, which doesn't have that law enforcement mission. So I think it is important to have some differences between the agencies in terms of how they handle the information.

MR. MEDINE: And is it the practice that all information that's collected under 702 is subject to the minimization procedures?

Some questions I think have been raised in some of the comments that were submitted as to whether address books or other information would be considered communications that would be subject to minimization, or is it the approach that all information collected under 702 is subject to minimization?

MR. WIEGMANN: All U.S. person information is subject to minimization procedures.

MR. MEDINE: I think my time is up.

MS. BRAND: First of all, thanks to all of you for being here this morning. We appreciate your taking the time and making yourselves available.

I want to continue on the Fourth Amendment discussion. Could one of you explain the process both inside the executive branch and then with the court of conducting the Fourth Amendment analysis and seeking the court's approval of the Fourth Amendment analysis and what kinds of opinions on the Fourth Amendment you've had from the court, to the extent that you can talk about it. Help us to understand how that works.

MR. WIEGMANN: So, you know, the FISA court operates a little bit differently than a regular court in the sense that it's ex parte, but. So that means only the government is there. There's not a party on the other side.

But other than that, we are briefing the legal issues in much the same way as we would

in a regular proceeding where there is a party on the other side. So we have an obligation to persuade the court that the collection under 702 is lawful, that it complies with the Fourth Amendment, and as I just explained to the chair, that minimization procedures comply with the Fourth Amendment.

So we would brief that issue explaining the Fourth Amendment procedures, and the court issues opinions and has issued opinions going through the Fourth Amendment analysis and finding that 702 collection, including the minimization targeting procedures meets the Fourth Amendment standards. So it's a full-up kind of regular legal briefing on that.

MR. LITT: And if I could just add something to that, it is typical in matters that involve the collection of evidence for these proceedings to be conducted ex parte. Wiretap or search warrant applications are also all done ex parte, even if they happen to present significant legal issues. So this is nothing novel in terms

of the approach that's taken there.

MR. DE: And if I could have one point. So in addition to what Brad was articulating, the court reviews this at least annually, the Fourth Amendment analysis.

As you all know, the 702 process requires annual certification. As part of that certification process every year the minimization and targeting procedures for the various agencies are submitted to the FISC, which by statute has to conduct a Fourth Amendment analysis on those procedures as part of that annual review process.

MS. BRAND: So the Fourth Amendment analysis is once a year of the program overall?

MR. DE: Well, the court has consistent jurisdiction over the program all year. The point I was making is that as part of the annual certification process, by statute the court is required to do a Fourth Amendment analysis of the annual, of the procedures that are submitted annually.

MR. BAKER: It gets evaluated at least

once a year.

MS. BRAND: Can you elaborate on that? What would there be in addition to that once a year analysis?

MR. DE: There could be a variety of factors. There could be a need to change procedures in the year, so that would prompt another analysis. I don't believe we've done that but that could be one circumstance.

There could be a variety of compliance matters that raise particular concerns to the court, in which case the court may want to do a review off-cycle.

So I think we wouldn't presume and say it only had to be once a year, but at a minimum by statute it needs to be once a year.

MS. BRAND: Okay. Bob, you talked about 702 not being bulk collection. I'd like to delve into that a little bit more, it's not bulk collection. You talked about selectors. We need to elaborate on that a little bit, I think. What is it? It's not bulk you say, but what is it?

MR. LITT: Sure. Well, I think it's probably helpful to talk about what bulk collection is first of all.

And if you look at the President's policy directive there's a definition. I don't have it in front of me, but it's essentially bulk collection is collection of communications without relying on some sort of discriminant to ensure that you're targeting particular collection.

It's sort of viewed sort of more informally, it's getting a whole bunch of communications, hanging onto them and then figuring out later what you want.

This is not that. This is a situation where we figure out what we want and we get that specifically. And so that's why it is targeted collection rather than bulk collection. Is that helpful?

MS. BRAND: But I'd like to get a little bit more into what is it that you're getting. So you have a selector, I mean.

MR. LITT: Sure. So Raj probably can

talk to this a little better than I can.

MR. DE: So if I could, I'd step back and just talk about the different types of collection under Section 702, which I think is a necessary predicate to understand how collection occurs.

So there's two types of collection under Section 702. Both are targeted, as Bob was saying, which means they are both selector-based, and I'll get into some more detail about what that means. Selectors are things like phone numbers and email addresses.

Both are affected by compulsory legal process, both types are conducted with the assistance of electronic communication service providers, and both types of collection under 702 are subject to the same statutory standards, so just as a predicate.

The first type is what's now been come to be known as PRISM collection, so just using that shorthand for a moment. And under this type of collection, communications to or from specific

selectors, again, things like phone numbers or emails, are provided with the assistance of ISPs pursuant to directives.

The second type of collection is the shorthand referred to as upstream collection. Upstream collection refers to collection from the, for lack of a better phrase, Internet backbone rather than Internet service providers.

It is also however selector-based, i.e. based on particular phone numbers or emails, things like phone numbers or emails. This is collection to, from, or about selectors, the same selectors that are used in PRISM selection. This is not collection based on key words, for example.

This type of collection upstream fills a particular gap of allowing us to collect communications that are not available under PRISM collection.

But given the unique nature of upstream collection there are different minimization procedures that apply, to get to the chair's question earlier.

The reason procedures aren't always the same for different types of collection, as Brad articulated, is that there are both different mission interests and different privacy interests at stake.

MS. BRAND: I see my time is up, so.

MS. COLLINS COOK: Thank you for coming here this morning. We really appreciate your time on this and happy to be a part of this dialogue here.

I wanted to follow up on a couple of points that have already been raised, but first, we've talked about the Fourth Amendment implications of the collection. We've also talked about the fact that, or it is known that the information that's collected can subsequently be queried.

Do you consider that subsequent query a search for the purposes of the Fourth Amendment? And if not, why not?

MR. WIEGMANN: No, I would say that the search occurs at the time that the collection

occurs. So when the information, as Raj just explained, from a particular selector is acquired by NSA, then that's the time at which the search occurs.

Once you've lawfully collected that information, subsequently querying that information isn't a search under the Fourth Amendment, it's information already in the government's custody. And so I don't think there are any other contexts really in general in which a warrant is required to search information already in your custody.

MS. COLLINS COOK: Following up on that, I think some have suggested that whether as a matter of Fourth Amendment necessity or as a policy, as a matter of policy that you should seek court approval before doing a query of a U.S. person identifier.

Can you talk a little bit about what the operational impact of such a requirement might be?

MR. WIEGMANN: Sure, and this is

something I guess some of my colleagues could talk about the operational impact. But as I said, in general with other types of collection, whether it's collection under Title I of FISA, which is your regular collection under which you've gone to the FISA court and already gotten approval to target a particular agent of a foreign power in the United States, or moving over to the criminal side if it's information collected under the Wiretap Act, commonly known as Title III, under which you're conducting surveillance, let's say of an organized crime figure or in a drug case of an individual, in all of these contexts we collect information.

We don't, once we've collected it, we've gotten the necessary court approvals to obtain the information, we don't then have to go back to court to query the same information that we've already collected lawfully a second time to say is it okay to look at it. We've already gotten the conclusion that it's legal to collect it.

And if you have to go back to court every time you look at the information in your custody you can imagine that that would be quite burdensome and difficult, to have to go back every time to look at information that's already in your custody. But I can let the FBI and NSA address it a little bit.

MR. DE: If I could add a couple of points and then I'll turn it to my colleague from the bureau.

Just one basic point, we've been talking about U.S. person queries and I just articulated two types of collection. Just to clarify, U.S. person queries are not allowed under what I described as upstream collection. So as I articulated, there may be different reasons to have tailored procedures, minimization procedures for different types of collections. So such queries are not allowed for upstream.

Adding to Brad's point about lawfully collected information, so once information is collected pursuant to 702, the government can and

often will review what it needs to in that information.

Querying that lawfully collected information, one way to think about that is a way to more efficiently review that which the government already has in its possession and can review all of.

And so to get to your question about policy limits on querying that data, one also needs to understand that that information is at the government's disposal to review in the first instance, and querying it is just a way to organize it.

Secondly -- thirdly, if I could add there are standards in place for querying that information, at least for NSA. Such a query, and we're talking about PRISM collection, must be reasonably likely to return foreign intelligence information.

And then finally, in order to disseminate any U.S. person information that may result from such a query it has to be necessary to

understand the foreign intelligence or evidence of a crime is apparent from our publicly available procedures.

But on the operational element, let me turn that to Jim.

MR. BAKER: So just at a high level I think let me make a couple of comments. So first I think you have to think about the fact that you're creating a new and special category of information, as Brad was saying, right. So this would be information that had already been acquired pursuant to lawful process.

We normally will query that. We'll look through that. When something comes in, we'll look through our collected materials to try to find -- a threat comes in, let's say for example. We look at our collected materials, we try to figure out what we have, and then, you know, move forward as expeditiously as possible.

So you would be creating a new category of information that sort of would be off-limits from the normal type of collection that we do.

And I don't pretend to fully understand all the implications that that would have.

But a couple that come to mind, first of all, obviously would be delay. So you would have some additional process that you would have to go through, and I'm sure there would be some kind of emergency carve out and so on, but you'd have to think about and factor in the reality that you would be introducing delay into the system.

You would also then as a result potentially create a gap. There are several types of gaps, I guess. But you would have, there would be a disinclination for people, because either they don't have the facts, or it's just too hard or whatever, to actually go and pursue that extra pot of information.

So there might be some type of connection between what we can look at normally, this material, and then other types of material. And having that type of gap might, you know, actually create a blind spot for us in terms of intelligence collection.

You'd also have to think about, I think, the technical complexity of what it is that you're suggesting. So this is going to have to be segregated in some way, treated differently. And we'd just have to think about that. That could lead to, you know, training issues, technical costs, things like that.

So it's, you just have to actually do it in a way that would be different than from other types of data that we handle, so that's sort of at a high level some of the things that come to mind.

MR. LITT: Beth, can I add one brief point to this which is that over the last decade, decade and a half, there have been a number of commissions that have been set up to investigate after a variety of terrorism incidents, 9/11, Fort Hood, the underwear bomber and so on. Consistently every one of those commissions has found that we need to eliminate barriers to making use of the information that's lawfully in our possession in order to better protect the nation.

And this, requiring some kind of additional process before we can query this information runs directly contrary to the recommendations of all those commissions.

MS. COLLINS COOK: Thank you. I see that my time is up.

MR. MEDINE: By the way, I should say in the excitement of getting into the questioning I never had actually a chance to introduce the panelists. And so I just wanted for the benefit of the audience, you're familiar to us, but for the benefit of the audience we have Jim Baker, who's the General Counsel of the FBI, Raj De, who's the General Counsel at NSA, Bob Litt is the General Counsel at the Director of National Intelligence, and Brad Wiegmann, who is the Deputy Assistant Attorney General at the National Security Division of the Justice Department.

Again, thank you all for being here.

MR. DEMPSEY: Thanks, and thanks to the witnesses for being here. They are very well-known to us. I think everybody should

realize that we've now spent many, many days with these gentlemen and with many, many of their colleagues at all their agencies going through this information, and delving deeply into this.

And there's been a huge amount of dedication of time on the part of the agencies to make sure that we have everything that we ask for and to make sure that all of our questions are answered. And so, you know, all the Board members really appreciate the amount of time that you've dedicated to talking with us.

And I think it is very important here to be one hundred percent clear, and I think there has been a lot of misunderstanding about the 702 program, and I think I do see issues with the program and things we're talking about, but I think it's very important to narrow the subjects of controversy, or discussion, or concern.

And I'm afraid that Raj may have partly reinserted a problem here when you said that U.S. person selectors were not used for upstream collection, or for upstream searches they're not

used at all, period, at the collection stage.

You were saying that U.S. person identifiers or selectors are not used to search the acquired database of communications that were otherwise acquired on a particularized basis under the upstream program, correct?

MR. DE: Correct. I definitely would prefer not to introduce more ambiguities. Let me be absolutely clear, Section 702 collection of any flavor, upstream or PRISM, is only targeting non-U.S. persons reasonably believed to be located abroad.

The topic I was discussing was, is in the realm of that lawfully collected targets information, once it's in the government's possession a secondary issue arises as to how one can search through that data. And the issue that we were discussing was whether those searches can be conducted using U.S. person identifiers within that lawfully data. And the answer to that question is no with respect to upstream collection.

MR. DEMPSEY: And here when you're talking about search and collect and acquire, all of those terms you're using to mean in a colloquial sense when the government collects, obtains, puts into its database, acquires, you're not parsing those words for 702 purposes. There's not a distinction between the search, the collection, the acquisition, right? It's all, you're using those things all that refer to the same activity.

MR. DE: There's no parsing between acquisition or collection.

So there are some theories out there that when the government receives the data it doesn't count as collection or acquisition. That is incorrect. Acquisition and collection for these purposes are the same thing.

But the term search is a different term. Search, as we were just discussing, means searching information that has already been lawfully acquired or collected.

MR. DEMPSEY: Although the first --

okay, so now we have two meanings of search. It's so hard to be clear on this. Brad was explaining a search occurs when you first collect or acquire. That is the Fourth Amendment search.

MR. DE: I think he was speaking to the use of the term in the Fourth Amendment, not the use of the term for purposes of this.

MR. DEMPSEY: And then querying, then there's a second use of search meaning query. So you query your database?

MR. DE: Correct.

MR. LITT: That's the term that we typically use rather than search in that context.

MR. DEMPSEY: Right. In that case a query is not a search for Fourth Amendment purposes.

MR. LITT: Right.

MR. DEMPSEY: Briefly talk a little bit about this 51 percent theory. So persons reasonably believed to be outside the United States, and there's been some talk about, well, so there may have been some slide somewhere, I don't

know where this came from, but some notion that, oh, if it's a 51 percent likelihood, therefore 49 percent of the time we might be wrong, that the person's not outside the United States and that's permitted under 702. Can you comment on that.

MR. DE: Sure. So I think the bigger picture question that that gets to how a determination is made for purposes of the statute that you are in fact targeting a non-U.S. person reasonably believed to be located abroad.

So as Bob articulated, and I'm sorry for repeating this but just for clarity, the statute does not allow us to target U.S. persons, it does not allow the government to target anybody within the U.S., it does not allow for reverse targeting, it does not allow for the intentional collection of wholly domestic communications.

So as to how we establish a reasonable belief that the target is in fact a non-U.S. person reasonably believed to be located abroad, there is no 51 percent rule that if you are 51 percent sure it is a non-U.S. person located

abroad that is sufficient. That is not the rule, and I don't honestly know where that misconception has come from.

The foreignness determination, which is shorthand for referring to the determination that it is a non-U.S. person reasonably located to be abroad, is based on a totality of the circumstances.

So what does that mean? That means that an analyst must take into account all available information. It means that an analyst cannot ignore any contrary information to suggest that that is not the correct status of the person. And it also means naturally that any such determination is very fact-specific to the particular facts at hand.

I did a little checking and it turns out in our internal training materials, at least at NSA, we actually ask our analysts a question along the lines of, if you have four pieces of information that suggests a person is abroad and two pieces of information that suggests a person

is domestic, given that the score is four to two is that sufficient to establish foreignness?

And the correct answer to that is, no, it is not sufficient because it is not a majority test. It is a totality of the circumstances test. One must take into account the strength, credibility, and import of all relevant information.

But just to add on to that, to your bigger point about confidence in that determination, analysts have an affirmative obligation to periodically revisit the foreignness determination. So it is not a once and done system.

Moreover, targeting determinations must be documented ex ante before any collection occurs. That documentation is reviewed, every determination is reviewed in 60 day increments by the Department of Justice and the Office of the Director of National Intelligence to determine if they agree with that determination.

And then finally, the targeting

procedures, as we mentioned, which account for a lot of this are reviewed annually by the Foreign Intelligence Surveillance Court and approved to be consistent with the Fourth Amendment and the statute obviously.

MR. WIEGMANN: And if I could just add from the DOJ perspective, as Raj said, we reviewed all of those foreignness determinations and we found an error rate of less than .1 percent basically. So that equates to essentially less than one in a thousand cases in which we're finding that NSA is making erroneous foreignness determinations.

MR. MEDINE: Judge Wald.

MS. WALD: Thank you again. I think that the NSA has said that in some of its information that if information about U.S. persons is collected incidentally to a 702 search that was targeted on a non-U.S. person and the incidental information about U.S. persons is found not to have any foreign intelligence value it will be, quote, purged.

Can you explain exactly what purging means? Does that mean that it can subsequently not be used at all, or it can be subsequently used or retained for some purposes? And finally, at what point and by whom would this decision of non-intelligence value be made? There's a lot of sub-questions.

MR. DE: Sure. Well, let me step back for a moment. If the information is determined to not have --

MS. WALD: Could you just speak a tiny bit louder because I'm at the tail-end of this table.

MR. DE: Certainly. If information is determined to not have foreign intelligence value then it is required to be purged.

What purging means is removed from NSA systems in a way that it cannot be used, period.

MS. WALD: For any reason at all?

MR. DE: Correct. There are extensive requirements we have gone through with the Foreign Intelligence Surveillance Court to ensure to the

best extent humanly possible that NSA's technical systems can, in fact, purge data as required by both our minimization procedures and the Foreign Intelligence Surveillance Court.

MS. WALD: But just to pursue that a little bit, in your experience is that to purge or not to purge decision made early in the process or is it kept in there until the analyst or whoever has a chance to do some more hunting around and see whether or not maybe other things would suggest that that does have intelligence value?

In other words, if there's such a concern about U.S., as there is in outside groups, about U.S. incidental information that's in the files and later there's a possibility of it being queried, I wonder how extensive this purging operation really is?

MR. DE: To purge or not to purge, that is the question.

MS. WALD: Yes.

MR. DE: So our procedures require that the determination about foreign intelligence value

be made as early as possible in the, what one in the technical sense calls the processing cycle. So it is not something that by default can be ignored.

That being said --

MS. WALD: And who makes that?

MR. DE: An assessment as to foreign intelligence value is made by foreign intelligence analysts.

MS. WALD: By the analysts who are working on it?

MR. DE: Correct, as they would be the ones who have the most relevant information.

But that also goes to a bigger point as to the nature of intelligence analysis. I think you all would appreciate that it's difficult to determine without context the foreign intelligence value of any particular piece of information. In fact, that's why the intelligence community is often encouraged to connect the dots of various pieces of disparate information.

And so I think we would hope and expect

that analysts make that determination about foreign intelligence value within the context of all available information.

But to your point as to if information is not reviewed, what is the default? This is a large reason why we in fact have default retention periods for data. And for example, for NSA the default for PRISM collection is a five year retention period.

But that's also a reason why that retention period is adjustable, or at least is tailored to the specific nature of the collection.

So for example, for upstream collection the retention period is two years, recognizing the nature of, the unique nature of upstream collection and that it may have a greater implication for privacy interests.

MS. WALD: Okay. The President required, I think he required in his January directive that went to 215 that at least temporarily the selectors in 215 for querying the databank of U.S. telephone calls metadata had to

be approved by the FISA court.

Why wouldn't a similar requirement for 702 be appropriate in the case where U.S. person indicators are used to search the PRISM database? I mean what big difference do you see there?

MR. LITT: Well, I think from a theoretical perspective it's the difference between a bulk collection and a targeted collection, which is that the --

MS. WALD: But I would think that, I'm sorry for interrupting, Bob. I would think that message, since 702 has actually got the content.

MR. LITT: Well, and the second point I was going to make is that I think the operational burden in the context of 702 would be far greater than in the context of 215.

If you recall the number of actual telephone numbers as to which a RAS, reasonable articulable suspicion determination was made under Section 215 was very small.

The number of times that we query the 702 database for information is considerably

larger. I suspect that the Foreign Intelligence Surveillance Court would be extremely unhappy if they were required to approve every such query.

MS. WALD: I suppose the ultimate question for us is whether or not the inconvenience to the agencies, or even the unhappiness of the FISA court would be the ultimate criteria.

MR. LITT: Well, I mean I think it's more than a question of inconvenience. I think it's a question of practicability.

MR. DE: And if I could add one point to that. I think one must also look at the underlying nature of the collection program at issue. And so I think we should be clear not to conflate the 215 program with the 702 program, and as you mentioned, one deals with metadata and one deals with content.

But the important point being the latter is directed at content collection targeting non-U.S. persons located abroad, whereas the 215 program, although it deals with metadata, did not

have such a necessary distinction.

MS. WALD: It did have a selective, I mean the 215 program and the original --

MR. MEDINE: I'm going to, your time, the Judge's time has expired, but we'll have an opportunity in another round to continue that discussion.

I want to shift to a different topic, which is about communication, about searches or about queries, which is, and I'm happy to have you explain it, but my understanding basically is that you are looking for other peoples' discussion of a particular selector or email term.

But I'd like to get back to some of the definitions here, which are there are some terms here that would be helpful to understand your view of, which is what is a target? What is a tasking? What is a selector? What's a directive?

If you could explain those terms, because I did want to shift to how those terms might apply in the about context.

MR. WIEGMANN: Okay, I can take a stab

at that. So a target is the -- maybe I should start with selector since that's the operative term that the others build on.

A selector would typically be an email account or a phone number that you are targeting. So this is the, you get, you know, terrorists at Google.com, you know, whatever. That's the address that you have information about that if you have reason to believe that that person is a terrorist and you would like to collect foreign intelligence information, I might be focusing on that person's account.

So when you go up on that selector, we say go up on or target that selector, that means we're collecting information, we're going to the provider and getting information related to that person's account.

So we're intercepting in real time and then collecting the historic communications of that particular account.

Okay, so that's what we mean by targeting a selector. You're using that selector,

you're providing that to the company, the provider, to get information on that account, or if it's a phone number on that phone number.

So that's when we say selector it's really an arcane term that people wouldn't understand, but it's really phone numbers, email addresses, things like that.

And targeting, it means that's the one you're trying to get. They may be in communication with other email addresses or other phone numbers and so forth. Those are not the targeted numbers or accounts, those are others that are incidentally acquired because they're on the other end of these communications. So target is the one you're going after.

And the statute requires that that target be a non-U.S. person located overseas. And so that's the foreignness determinations that we're talking about as we go through at great lengths to make sure that that target is in fact belongs to a non-U.S. person that is located overseas.

The other two questions?

MR. MEDINE: Tasking or task.

MR. WIEGMANN: Tasking is when you're going and saying, okay, I want to task this account means I want to collect information from that account. So that's the collection.

MR. LITT: You task a selector.

MR. WIEGMANN: You task a selector. So you're identifying, that's when you take that selector to the company and say this one's been approved. You've concluded that it is, does belong to a non-U.S. person overseas, a terrorist, or a proliferator, or a cyber person, right, whoever it is, and then we go to the company and get the information.

MR. MEDINE: And directives.

MR. WIEGMANN: So directives are the orders that go to the companies that say they have to comply with the lawful tasking. So that's the kind of more overarching order that goes to a company provider and says, okay, you have a legal obligation to comply with the taskings that are

given to you and here are the rules and everything. And that's all provided to them.

Is that a fair summary? I'll ask my colleagues to see if that is --

MR. DE: Keeping target as the statutory term. A term like selector is just an operational term to refer to something like an email or phone number, directive being the legal process by which that's effectuated, and tasking being the sort of internal government term for how you start the collection on a particular selector.

MR. MEDINE: Okay. So I guess building on that, what's the statutory rationale for about collections, because if the target is the email account or phone number, what is the justification for gathering communications between two persons, it may even be two U.S. persons who are discussing that phone number or that email address, but they are not themselves, there's no to or from that particular email address or particular phone number, why is that targeting that is permissible under the statute?

MR. WIEGMANN: Right. So the conclusion there again in a typical case, you're right, if you're targeting, you know, bad guy at Google.com you're targeting that person's accounts, their communications.

Why abouts collection is different is it's not necessarily communications to or from that bad guy but instead about that selector.

And so what the court has concluded is that when the statute uses the term targeting of a non-U.S. person overseas, targeting that selector qualifies under the statute for targeting that non-U.S. person overseas.

So it doesn't have to be targeting necessarily to or from, but can also target the communications that are about that particular selector.

MR. MEDINE: So that's a different meaning of target than earlier, which is where you're focusing on an account, now you're discussing targeting means discussions about that account.

MR. WIEGMANN: About that selector, correct.

MR. DE: It is always focused on that account, so I think the key is, the misperception that some may have that about collection is somehow about a key word or about the person that may be behind that account.

But all collections under Section 702, whether it's upstream abouts, which is a subset of upstream, or PRISM is all based on the selectors at issue.

MR. MEDINE: But does it raise -- oh, I see my time has expired so I'll --

MS. BRAND: I'm glad to see you're following your own rules.

Just to follow-up on that because that's a good line of inquiry, just to make sure that everyone understands. So you're saying that if someone is emailing about Rachel Brand or about explosives that would not be a permissible about query under your explanation?

MR. DE: So I would like to --

MS. BRAND: But you could, you could perhaps get it about Rachel Brand at --

MR. DE: Just so that, because I think this is an issue that all of us slip into, clarifying querying for collection.

So we are discussing now the collection of information. Abouts is a type of collection of information.

MS. BRAND: I'm sorry, right. Yes, that's right.

MR. DE: And so all collection of information is based, focused on selectors, not key words, as you just mentioned like terrorist, or like a generic name or things along those lines.

MS. BRAND: Okay.

MR. DE: And it's the same selectors that are used for the PRISM program that are also used for upstream collection. It's just a different way to effectuate the collection.

MS. BRAND: Okay. I think a large part of the function of these hearings is a public

education function and so I thought David's questions were great to explain the meaning of different terms, and I'm glad that you're willing to bear with us asking you some questions that we've already discussed with you in private. But I think it's helpful for everyone to understand what we're talking about.

And along those lines there was some discussion in Pat's questions about purging data that doesn't turn out to be foreign intelligence information.

But can you explain how on the front-end you implement the requirement that, not only that the target be a non-U.S. person reasonably believed to be abroad but that you expect to get foreign intelligence information through the collection, that's a separate statutory requirement. How do you go about ensuring that you're collecting that type of information?

MR. DE: Sure. So in our earlier discussion we skipped right to the foreignness determination, but that's actually a second step.

There has to be a reason one actually wants to collect intelligence from the particular selector in the first place.

And then one has to get to the fact, is this a type of collection permitted under the statute? So there has to be a valid foreign intelligence reason to do that collection.

But beyond that there has to be a valid foreign intelligence reason within the ambit of one of those certifications that the FISC approves annually. Those are certifications on things like counterterrorism, encountering WMDs, for example, weapons of mass destruction.

And so when an analyst needs to make a determination as to the valid foreign intelligence purpose for which they want to effectuate collections, they must also document that.

That is documented in a targeting rationale document in advance, ex ante, and those are always reviewed by the Justice Department and the Director of National Intelligence every 60 days.

MR. WIEGMANN: This is an important point for non-U.S. persons because people think about, okay, well once you've concluded that it's a non-U.S. person overseas then you can collect whatever you want. As Raj said, that's really not the case.

It really is targeted, not only based on the identity of the person and the location of the person, but also that you're trying to get foreign intelligence. And so it's an important protection really in the statute that is designed for non-U.S. persons. It's not blanket collection of any non-U.S. person overseas. It's aimed at only those people who are foreign intelligence targets and you have reason to believe that going up on that account that I mentioned, bad guy at Google.com is going to give you back information, information that is foreign intelligence, like on cyber threats, on terrorists, on proliferation, whatever it might be.

MS. BRAND: What can you tell us in an unclassified setting about the documentation of

foreign intelligence purpose or the oversight to ensure? I mean we've talked a little bit about that in past questions, but can you give us anything more specific?

MR. WIEGMANN: They do have to document that at NSA and every -- it's essentially called a tasking sheet, I think. And on that sheet they are documenting the foreign intelligence purpose that they are trying to pursue in going after a particular target.

And those are all reviewed together with the foreignness determination by the Department of Justice on a regular basis.

MS. BRAND: That's a separate sheet for every selector?

MR. WIEGMANN: For every single one, that's right.

MR. BAKER: And I think, at least with respect to FBI, I think the review that Raj mentioned earlier is done every 30 days on these tasking decisions, I guess you'd say, the foreign intelligence and the foreignness determination.

MR. DE: And if I could put that into the broader context of if the question really is getting at what is the process within which that happens, even before that happens we have training for analysts as to how they should document this material, we have audits of our databases, we have a comprehensive compliance program, we have spot checks, even within NSA prior to the 60 day reviews that are done by the Department of Justice and DNI, for us anyway.

There are also quarterly reports to the FISC on compliance with the program, semiannual reports to the FISC and to Congress, and annual inspectors general assessments, and as I mentioned, the annual certification process by the FISC.

So I think those decisions are, while they're one very granular aspect of the program, are conducted within the context of this broader regime.

MS. BRAND: Okay. And I see that my time just ran out.

MS. COLLINS COOK: I wanted to ask one additional question about abouts. Can you do about collection through PRISM?

MR. DE: No.

MS. COLLINS COOK: So it is limited to upstream collection?

MR. DE: Correct. PRISM is only collection to or from selectors.

MS. COLLINS COOK: I wanted to shift to a separate topic. One of the things that I have found both concerning and frustrating through the process of our evaluation of programs is how to both assess and articulate the efficacy of these programs.

And Mr. Litt, you had begun speaking about this in your prepared remarks. And I'd like to ask a couple of questions. One, how do you assess the efficacy of a particular program? How do you think we should be assessing the efficacy of a particular program?

And three, it's not really a question, it's more of a comment which is, please don't give

me a series of success stories and then say that's how you evaluate the efficacy of the program. Because I think that's an initial response from the government often in response to a question, either from a body like ours or from the media.

But how do you assess the efficacy of the program, how periodically do you do so, and how would you encourage us to assess the efficacy?

MR. LITT: Well, let me start on that, and I want to start by saying that I completely agree with you that sort of individual success stories are not the way to evaluate a collection program and its utility.

The way you evaluate collection programs is going to depend in part on what the particular program is for.

In this case, we have in fact the Office of the Director of National Intelligence has attempted, part of our job is to try to determine that resources are effectively allocated within the intelligence community budget.

And so we have done studies to try to

look at, okay, what are our collection priorities, how much reporting is generated on these priorities, and where do those reports come from, what kind of collection source, to the extent we can identify that. And that's one of the ways that we've determined that Section 702 is relevant.

Another thing is just by looking at the sheer nature of the information that we get and its utility towards a whole variety of national priorities. That's a more impressionistic approach, and yet you can see time and again in important intelligence reports that are provided to policy makers that it's derived from Section 702 collection.

So those are two ways that I would look at estimating the value of a particular collection.

MR. DE: If I could just add on to that. With respect to this program or any program I think intelligence professionals will tell you that any tool must be evaluated in the context of

the other tools in which it is utilized.

All intelligence tools are used in complementary fashion with one another and to isolate one particular tool and evaluate its effectiveness in isolation probably doesn't do us justice as to what's valuable and what's not.

It also depends on the type of tool. Different types of intelligence programs are used for different purposes. A program like Section 702 is used for different purposes, for example, than a program, a metadata program with telephony metadata.

One may be a discovery tool to help pursue more specific collection and others may be used as in fact the specific collection that follows from that.

Third, there may be uses in which the PCLOB has recognized in terms of either directing the government in certain directions or at least helping to shape the focus of the government.

And so I think the absolute wrong question is how many plots did this tool stop.

And you can fill in the blank for what this tool refers to. But that is absolutely the wrong question, and I think it won't do us justice to figure out what we need as a government.

MS. COLLINS COOK: I have time I think for one last question. What is the view of the various agencies as to whether or not 702 is an effective and valuable program for the United States?

MR. BAKER: I think it is an effective and valuable program for the United States.

And if I could just address your last question as well. I mean I think you really, in order to understand whether it's effective and useful you have to think about what your goals are with respect to this particular program.

And the goals for this program, like many other collection programs are to obtain I think timely, accurate, informative foreign intelligence information about the capabilities, plans, intentions of foreign powers, agents, actors, and so on and so forth.

And so I think really what you're talking really is, I think, developing a good metric to understand whether this program is worth all of the costs associated with it. And so I think you'd want to look at the amount of information that you, that we acquire, but also then obviously the quality of it. How good is it? And I think you can slice that a lot of different ways, as my colleagues have suggested.

So I think that's really what I would recommend you be focused on. But you have to, because this is a broad-based foreign intelligence collection program you have to look at not only, I mean you have to look at counterterrorism but you have to look more broadly than that because this program is not limited just to counterterrorism.

MR. DE: I agree it's definitely an effective program. I think the one point I should have added is that the review that Bob mentioned happening within the executive branch is not limited to the executive branch.

Congress also reviews the effectiveness

of this program, as well as the 215 program. And I think that's part of the rationale behind having sunset clauses for various programs is that when those statutory provisions expire, as did the 215 program twice in the last five years and as did 702 in 2012, Congress undertakes, as it should, an evaluation of the effectiveness of the programs.

MR. LITT: So I completely agree that it is an effective and important program and I really want to emphasize the last point that Jim made, which is that this program should not be considered solely as a counterterrorism program. This program has utility, has significant and exceedingly important utility in areas outside of counterterrorism.

MR. DEMPSEY: Trying to clear up another issue in terms of the participation of service providers and the awareness of service providers in the 702 implementation, is 702 implemented, all 702 implementation is done with the full knowledge and assistance of any company that, from which information is obtained, is that

correct?

MR. BAKER: Yes. The answer to that is yes.

MR. DEMPSEY: So early on in the debate there were some statements by companies who may or may not have been involved in the program saying, well, we've never heard of PRISM. But whether they ever heard of PRISM, any company that was, from whom information was being obtained under 702 knew that it was being obtained?

MR. LITT: Correct.

MR. DE: PRISM is just an internal government term that as a result of the leaks became a public term. But collection under this program is done pursuant to compulsory legal process that any recipient company would have received.

MR. DEMPSEY: So they know that their data is being obtained because --

MR. DE: They would have received legal process in order to assist the government, yes.

MR. DEMPSEY: One thing I read in one of the statements is under 702 you could target entire countries or regions, is that correct?

MR. DE: So all collection under 702 is based on specific selectors, things like phone numbers or email addresses. It is not a bulk collection program.

MR. DEMPSEY: And a selector would not be an entire area code, for example?

MR. DE: Correct, correct.

MR. DEMPSEY: Going back to the constitutional -- oh, one other set of questions.

Even I've lost track now of what you've already said here versus what you've said elsewhere. But in terms of where you make a determination that a person is a non-U.S. person outside, reasonably believed to be outside the United States and then you later discover that that was good faith but wrong, the person was in United States, or the person was a U.S. person, do you track that, and what do you do when you discover that, and how often do you discover?

I'm not talking about the roamings, I'm talking just about you thought he was outside the United States and that was just wrong, or you thought he was a non-U.S. person and that was just wrong, how often does that occur?

MR. DE: So I'll defer to Brad on the sort of overarching review, but if I could just make a point about what happens. So yes, we keep track of every time new information comes to our attention to suggest that a prior intelligence evaluation was incorrect, even if it had met the legal standard.

Every such incident is a compliance matter that has to be reported to the FISC and ultimately in semiannual reports reported to the Congress.

And third, that sets in process a purging process by which information that should not have been collected if it had not met the legal standard needs to be purged from NSA systems.

I think Brad can speak to the level of

accuracy of those.

MR. BAKER: Just real quick, it's the same. The item is de-tasked and the information is purged.

MR. WIEGMANN: Right. So just to distinguish again between two different types of compliance issues. One is the roamer example that you mentioned.

So this is, let's say we're up on a cell phone that we believe belongs to a bad guy who's outside the United States, a foreign person, and then that person shows up in Chicago, when that happens we de-task that cell phone. That means we're no longer collecting the communications.

That's a compliance incident that's reported but it's not an erroneous determination. It's based on the movement of the individual.

So putting those cases aside, in cases where we just kind of get it wrong, we think the email account or the phone is located overseas but it turns out that that's wrong, or it turns out

that we think it's a non-U.S. person but it is a U.S. person, we do review every single one to see if that's the case.

And our review at Justice we decided to review, and as I mentioned earlier, we think it's less than one in a thousand cases where they make that determination erroneously.

MR. DE: And this probably bears worth repeating that the initial determination is not a once and done, so there is an affirmative obligation for analysts to reaffirm the foreignness determination on a periodic basis, which contributes to the ability to make sure that determination is in fact fresh and current, which of course contributes to the accuracy of that determination.

MR. DEMPSEY: Going to the constitutional issues, back to those for a second, the FISA court has determined, I mean they must they must determine every year that the program is being implemented consistent with the Fourth Amendment.

The very first time they determined that, there was an opinion that they issued. That one is, am I right, not yet public?

MR. WIEGMANN: I think that's correct.

MR. DEMPSEY: Isn't that a good candidate for declassification?

MR. LITT: We have a lot of good candidates for declassification.

MR. DEMPSEY: Yeah.

MR. LITT: In all seriousness there, we are, there are a lot of documents that we have that we are reviewing for declassification that include not only FISA court opinions but a whole variety of other documents.

MR. DEMPSEY: The FISA court in 2008 when they last considered the constitutionality of a program, the predecessor to 702, the court issued a redacted but largely unclassified opinion conducting a relatively full Fourth Amendment analysis.

And there's been some Fourth Amendment analysis conducted in this situation, and if

you're sort of talking about, you know, the Rosetta Stone kind of Ur document, then the very first court opinion should have been the most fulsome explanation of the constitutionality of the program.

I think that -- I mean I hear Bob saying there's a lot of opinions out there, but to me this one seems to be one that would explicate at least one court's judgement on this because it's been the basis of -- I assume all the rest just said nothing has changed that would merit us to reconsider our very first judgement.

MR. WIEGMANN: So I mean I think it's among the opinions. We're committed to reviewing all the opinions of the FISA court to determine which ones can be declassified in redacted form. So I imagine this will be among those that are reviewed. So absolutely, I don't disagree. It'll be among the opinions that will be reviewed.

MR. DE: I just don't want to leave folks with any mysterious misimpression. I think the Board has access to everything and so one

shouldn't have to assume anything about subsequent opinions. The Board has in fact reviewed everything.

And so I just don't want -- what I think would be an unfortunate consequence would be for folks to take away the impression that there is a mysterious opinion that has some secret analysis, and I don't think that's the case. I don't think you intended to suggest that.

MR. MEDINE: The Board does have access to it but I think the question is whether the public should have access to it as part of the debate. But it's Judge Wald's --

MR. DEMPSEY: The public had access to the 2008 --

MR. MEDINE: It's Judge Wald's turn.

MR. WIEGMANN: So just one other thing I would add on that is that 702 collection has now been challenged by a number of criminal defendants when 702 information is being used against them in their cases. And so we'll be filing public briefs and we can expect some more decisions in that area

as well.

So that's another way that the constitutionality of 702 will now be on the public record, or I mean the opinions on it, and the briefs and everything will now be a matter of public record.

MR. MEDINE: Judge Wald.

MS. WALD: Okay. By whom and under what substantive criteria is the initial decision to use a U.S. person selector for searching the PRISM base made? I mean who decides let's do that? What's the substantive criteria on which they make it?

You don't have to go into the review process. I know the decision will be reviewed up and down. But how does that get made? What's the substantive basis?

MR. DE: So I can speak for NSA in particular.

MS. WALD: So just to clarify, that means if it goes to one of the other agencies, not NSA, CIA or FBI or something, they make their own

substantive decisions for querying?

MR. DE: Yes. The 702 program perhaps as a necessary predicate is one that all agencies operate on their own and have their own minimization procedures which would address topics like searches.

NSA's procedures in this regard, in this element have been made public and so the standard is that such a query needs to be reasonably likely to return foreign intelligence information.

MS. WALD: Be reasonably likely. And who is it made by initially?

MR. DE: It's made by the analyst.

MS. WALD: By the analyst who's working on that particular case, okay.

My other question is that the President did, if I understand his directive correctly, direct that there be some changes in the treatment of non-U.S. persons as to the limits on and retention of the data acquired incidentally to bring them more in line with those of U.S. persons

incidentally where there is no foreign intelligence value apparently.

Can you tell us a little bit more specifically if anything has been done in that regard or is being contemplated vis-a-vis 702?

MR. LITT: So I think first of all it's important to understand the point that somebody made, it may have been Brad made earlier, which is that there are already protections to some degree built into the system there. The protections for non-U.S. persons are not as great as those for U.S. persons because U.S. persons are protected by the Fourth Amendment.

But there is a requirement that we can't target a selector unless we have reason to believe it's of foreign intelligence value. And there's sort of a general principle that the intelligence agencies, their job is to collect, analyze, and disseminate foreign intelligence information, not random information.

I think what the President has directed is that we go back and look at our procedures and

not only with respect to 702, but with respect to signals intelligence in general, assess whether, the extent to which it's possible to provide limitations on collection, retention, and dissemination that more closely track those for U.S. persons.

For example, Executive Order 12333 provides specific categories of personal information about U.S. persons that can appropriately be retained and disseminated.

There's a list of them in Executive Order 12333 and the President has asked that we assess whether we can apply those same sorts of rules to personal identifiable information of non-U.S. persons.

MS. WALD: Right now, just to follow-up, right now if you get incidental information about a foreign person in the course of targeting another foreign person and you look at it, do you use the same criteria and look at the same review and say, well, you know, he was just talking to his grandmother or something, there isn't any

foreign intelligence there, and you purge it?

MR. DE: Any time there is not foreign intelligence value to collection, by definition it would be purged.

But I think an important point to be made as you are articulating, Judge, is incidental collection, just to explain that term a little bit, all communications obviously have two ends. One end is the target and the other is presumably not a target. We don't know. One doesn't know ex ante.

And so by definition there will be incidental collection of non-U.S. persons, as well as U.S. persons. Historically, constitutional protections obviously have only applied to the U.S. person subset.

MS. WALD: I understand.

MR. BAKER: Can I just make a comment about that?

MS. WALD: We don't have time. Okay, quickly on the last time, I found it very provocative when you were answering Beth Cook's

question about if you're going to assess the efficacy of a program you have to look at it in terms of its efficacy and the holistic view of all of the programs.

I guess it's inevitable that I would ask the question, but how can anybody except you people do that, because so many of your programs, I think, are just unknown, even to the FISA court? They're not all FISA supervised, and certainly the outside world doesn't know about many of them. So you know, how in effect can an outside assessment be made?

MR. DE: If I could just address it since it was in response to my comment. Certainly I think I would not suggest that there should be a public evaluation of all intelligence programs. I think, for example, this Board as access to information about counterterrorism programs and so I would expect that any evaluation would be in the context of the other CT programs that you have the jurisdiction to review.

As with Congress, as I mentioned, they

reevaluate programs on a periodic basis. And I think the public record now indicates that there is a fairly robust exchange between the executive branch and the legislative branch on a variety of programs. And so I think that's where traditionally the evaluation has occurred.

MR. LITT: Yeah, I was just going to say that we've managed, we've set the balance between public disclosure and the need for secrecy by empowering the congressional intelligence committees. We're required by statute to keep them fully and currently informed of intelligence activities, and we do. They know about these programs and they have the opportunity to evaluate them, and they do.

In fact, they passed an Intelligence Authorization Act that includes a lengthy classified annex that is very prescriptive with respect both to reports that it requires of us and directions as to what we should, you know, where we should be spending our money.

So that's sort of the external

oversight and the way we've said, okay, well, we need to have oversight of these but they still need to remain classified.

MR. MEDINE: Did you want to finish? I don't know, you wanted to make a point earlier about foreign intelligence.

MR. BAKER: I had several points I wanted to make. But let me just on that real quick, I mean I think the, even the addition of Congress having oversight of it, the courts in certain circumstances, and then also obviously the President and all of the executive branch officials, we have an obligation to make sure that in addition to adherence to the law and taking care that the laws are faithfully executed, to spend our time and spend our money on programs that are effective and not be wasting our time on things that are not.

I mean that flows from the President to the DNI, the Attorney General, Director of the FBI, Director of NSA and so on. We should be focused on things that are useful and collecting

information that produces the kind of intelligence information that I was talking about before.

So the other comment that I just wanted to make was just with respect to FBI, our personnel only have access to the databases when they've received the proper training with appropriate oversight and operating consistent with the court-approved standard minimization procedures when they're doing their query activity.

MR. MEDINE: I wanted to shift to a different subject, which is attorney client privilege. There were some press reports a couple of weeks ago about collection of information that may involve attorney client communications.

But I want to focus particularly on the NSA minimization procedures, which I understand do exclude attorney client communications but only in a very narrow context where the client is under criminal indictment and the United States, basically on a federal criminal indictment.

That seems like a very narrow

interpretation of attorney client privilege. I wanted to see if that is the interpretation you apply in minimizing communications, and if it is what impact there would be if it was expanded to the more normally accepted definition of attorney client privilege, which is basically lawyers and clients consulting with each other?

MR. DE: So we have written a letter to the ABA and commented on it to the Board and to the public, I think it's a public letter now, which explicates in fuller detail than I probably can off the top of my head as to our procedures.

But I think one fundamental premise is that analysts are under an obligation to identify for the Office of General Counsel any time they encounter something that may be potentially privileged.

And I think as all of us who are lawyers, I think that probably encompasses every one up here on the stage, knows just because a communication is with a lawyer does not mean it is in fact a privileged communication. So it's

helpful to have a lawyer involved to determine that.

While I can't speak to any particular incident that may have been written about in the press I think there's a couple of big picture points that are worth making. One is our office has historically provided a range of advice to minimize to the extent possible the collection of attorney privileged material.

MR. MEDINE: That's privilege just where there's a criminal indictment or are you viewing privilege --

MR. DE: Beyond the criminal. So the point I'm trying to make is that while there may be a specific provision in the 702 procedures that addresses the criminal context, there's a reason why we ask analysts to consult counsel, because the advice can often be tailored to the specifics of a circumstance far outside the criminal realm, recognizing the import of attorney client privileged material in context, even outside the criminal context.

MR. MEDINE: I want to talk a little bit about reverse targeting where you target someone overseas potentially with the view of collecting information about a U.S. person in the United States, and that's impermissible.

There seems, again maybe this is a somewhat technical point, but there seems to be somewhat of a quirk in the statute. It says that you can target people reasonably believed to be outside the Unites States, you cannot reverse target someone outside the United States if the purpose is to target a particular known person reasonably believed to be in the United States.

Does that permit targeting a person outside the United States with the intent of gathering information about U.S. persons not in the United States?

MR. WIEGMANN: No.

MR. MEDINE: Why not?

MR. WIEGMANN: There's a separate provision that bars targeting U.S. persons outside the United States and so if you were doing that

and you are trying to target a U.S. person outside the United States, you couldn't do that.

MR. MEDINE: So you wouldn't do the reverse targeting procedure?

MR. WIEGMANN: I don't know if you would call that reverse targeting --

MR. DE: There is another statutory provision that prohibits the targeting of U.S. persons outside the U.S. under 702 --

MR. MEDINE: Even reverse targeting? Again, I'm not talking about -- I agree it's clear that you can't target a U.S. person outside of the United States, but what if I find a non-U.S. person that I know is in communication with a U.S. person who's also outside of the United States, is that permissible?

MR. WIEGMANN: No.

MR. DE: No.

MR. MEDINE: Because?

MR. WIEGMANN: Because you would be targeting, if your real purpose is to target that U.S. person, you're targeting that person.

MR. MEDINE: So reverse targeting in your view is the same as targeting? The prohibition on reverse targeting is co-existent with the prohibition on targeting?

MR. WIEGMANN: Well, I mean again I think of reverse targeting as a geographic issue essentially when you're targeting, let's say you have a legitimate target overseas but you really want the communications of a U.S. person or a non-U.S. person inside the United States, but the statute says you can't do that.

MR. MEDINE: Right, but --

MR. WIEGMANN: But as we were just explaining which is if you have a U.S. person that you're interested in overseas, you can't use 702 to target them either and I don't think --

MR. MEDINE: Or reverse target them?

MR. WIEGMANN: What's that?

MR. MEDINE: If you know that that U.S. person is in communication with a non-U.S. person and both of them are overseas --

MR. WIEGMANN: Right.

MR. MEDINE: Could you target the non-U.S. person to get the U.S. person's communications?

MR. WIEGMANN: You couldn't do it for that purpose but if the non-U.S. person overseas is a valid foreign intelligence target that you're interested in their communications, sure, you can target that person. And the fact that they're incidentally communicating with a U.S. person overseas, that's okay. I wouldn't consider that reverse targeting.

You still have to have that legitimate target. I don't know if that answers your question, but.

MR. MEDINE: It did.

MR. BAKER: I'm not going to read it now and take up your time, but take a look at Section 704 A 2, and that may address the kind of concern that you're focused on perhaps, but perhaps not.

MR. MEDINE: Okay. I wanted to get back to efficacy. As you know, our charge is to

look at the balance between national security and privacy and civil liberties, and I think following up on Ms. Cook's question -- sorry, I'll just hold that until the next round.

MS. BRAND: I wanted to go back to upstream collection a little bit. I've seen some statements in the public domain about the volume of upstream collection vis-a-vis the volume of PRISM collection. What can you tell us in a public setting about that?

MR. DE: I think the best publicly available information is from the October 11th, 2011 opinion that has now been declassified in which there was a rough estimate there, and forgive me for if it's not precise, but that about 10 percent of collection is upstream. On the order of magnitude, I just don't know the exact number.

MS. BRAND: Okay. So you said in an earlier round of questioning that upstream, collection from upstream is retained for a shorter period of time than collection from PRISM and you

said that the reason for that distinction is that there's a potentially greater privacy concern with respect to upstream collection.

Can you elaborate on why, whether the additional privacy concerns that pertain to upstream.

MR. DE: Sure. And a lot of this is laid out in this court opinion that's now public. This is from the fall of 2011. I think because of the nature of abouts collections, which we have discussed, there is potentially a greater likelihood of implicating incidental U.S. person communication or inadvertently collecting wholly domestic communications that therefore must need to be purged.

And for a variety of circumstances the court evaluated the minimization procedures we had in place and as a consequence of that evaluation the government put forth a shorter retention period to be sure that the court could reach comfort with the compliance of those procedures with the Fourth Amendment. And so two years was

one element of the revised procedures that are now public.

MS. BRAND: So from what you just said that if using a legitimately tasked about term a wholly domestic communication is collected, it has to be purged?

MR. DE: If one recognizes it, yes. In fact, there's a --

MS. BRAND: Even if it has foreign intelligence information?

MR. DE: There are specifics. Off the top of my head I can't articulate all the particular exceptions in the minimization procedures but there are an elaborate set of detailed procedures that are now public that discuss how upstream collection must be treated in order to account for this concern.

And it has things like data must be segregated in certain ways where the risk of collecting a wholly domestic communication is higher, there's a shorter retention period.

Wholly domestic communications are not

permitted under the statute, and so therefore as a default rule, yes, it must be purged.

MS. BRAND: Jim, was there something you wanted to add?

Okay. I want to use the word incidental collection there again, and your definition earlier seemed to be that by incidental you mean, by incidental U.S. person collection you mean that the person on the other end of the phone from the non-U.S. person abroad is a U.S. person. That's your definition, right?

Is there another definition that you're aware of? Because you seem to be -- okay.

I think there's been some frustration with the use the term incidental in that context because it's not accidental, it's intentional. It's actually unavoidable. And so I just wanted to make sure that we're all on the same page, that by incidental you mean not accidental, not unintentional, but this is actually what we're doing.

MR. LITT: It is incidental to the

collection on the target. It is not accidental, it is not inadvertent. Incidental is the appropriate term for it.

MS. BRAND: Okay.

MR. DE: And I'd say that term I think has been used far beyond this program and historically, so there's no judgement intended. That is just a term.

MS. BRAND: Okay, okay. I'll hold the other questions for another round.

MS. COLLINS COOK: Just following up on David's question, I think it goes to a broader point which is that there is a perception that this statute is fairly complicated, there's got to be loopholes or idiosyncrasies in there somewhere.

But let me just ask you, would it be the view of the United States government that it is appropriate to use 702 to intentionally target U.S. persons, whether directly or through reverse targeting, whether they are inside the United States or outside the United States?

MR. LITT: No, definitely not.

MR. DE: No.

MR. LITT: That is not permissible.

MS. COLLINS COOK: I wanted to also follow up on a question about the abouts. And I apologize, again just for folks understanding that we spent six and a half hours talking with folks about just the oversight mechanisms in place and were unable to get through that entire conversation. So I apologize if you've said this before today.

The collection methods, procedures that you use with respect to abouts, those procedures, are they approved by the FISA court?

MR. DE: Yes.

MS. COLLINS COOK: Are those transparent to Congress?

MR. DE: Yes.

MS. COLLINS COOK: I think we haven't necessarily, we started to allude to this but can you talk a little bit about your impression of how the intel committees in particular view their obligations with respect to oversight of your

programs and whether you have found in your experience that to be pro forma or in any way lacking?

And let the record reflect a few, not quite eye rolls, but I think the response was, no, they have not found this to be pro forma in any way.

MR. LITT: I've been on this job now for getting on towards five years and I have found nothing about my interactions or our institutional interactions with the intelligence committees to be pro forma.

They have fairly substantial staffs which have a lot of experience. Some of them come from the community. They know, they dig very deeply into what we do. The DNI occasionally uses the term wire-brushing for the interactions that we have with the committees, so it's not a pro forma interaction in any way.

MR. DE: If I could add one point, on programs like 702 that we're talking about today for example, we all lived through the

reauthorization of Section 702 in 2012.

That process was not simply in connection with the intelligence committees, but I can remember numerous briefings where we would go up for a member, for all member briefings that the intelligence committees would host for the Congress.

So I don't want to leave the impression that it's only with the intelligence committees, particularly for a program like 702 that needs to be voted on by all members of Congress on the basis of a sunset clause.

MS. COLLINS COOK: I want to make sure that my colleagues have time for their last round of questions so I'll cede my time.

MR. DEMPSEY: Going back to the minimization procedures question, and specifically the incidental collection question, am I right that the rule is that whether the information is inadvertently collected, that is you were tasking on the wrong selector or some mistake was made and you got something that you didn't intend to get

that's inadvertent, or you were correctly targeting the right account and then you collected communications to or from a U.S. person that's incidental, the procedures say, minimization procedures, rules say that if you never discover that it was inadvertent and never discover that it was incidental, you never realized that it was a U.S. person collection, it's deleted after five years?

The basic rule is you keep it for five years, you keep everything for five years, two years on upstream, five years on PRISM, and then it gets deleted. That's the baseline rule, right?

MR. LITT: Correct.

MR. DEMPSEY: And then you on top of that the rule is that if then you, through analysis, through reviewing it that it was inadvertent or incidental collection on a U.S. person you must immediately purge? Bob's shaking his head.

MR. LITT: There's a difference in the way inadvertent and incidental, as you're using

those terms, are very different concepts.

Inadvertent refers to a collection that was not authorized by law. That is purged.

Incidental --

MR. DEMPSEY: Purged unless?

MR. LITT: Unless, as Raj mentioned, that there are certain exceptions. I'm certainly not able to recite them but they do exist. But they're fairly narrow.

Incidental is collection that is authorized by law. And at that point the rules relating to U.S. persons kick in and if you determine that it has no foreign intelligence value you purge it.

MR. DEMPSEY: Right, but I mean what's your response to the argument, well, fine, that just means that if you think it's valuable you can keep it, if you don't think it's valuable then you purge it?

MR. LITT: But it's lawfully collected.

MR. DEMPSEY: Fair enough. But you do, if it is of interest to you, you do keep it?

MR. LITT: If it's of potential foreign intelligence value --

MR. DEMPSEY: Minimization means --

MR. LITT: If it can be useful to providing the intelligence that policy makers need or to protecting the nation against threats, then yes, we keep it for the required period.

MR. WIEGMANN: So again, to make it more concrete, if it's a terrorist overseas, he is calling a number in the United States that belongs to a U.S. person, we want to keep that information. It is incidental, the fact that we're getting the U.S. person number and we're targeting that non-U.S. person overseas, but he's calling Minneapolis, we want to keep that communication because it's of high interest to us.

MR. DE: One point I would add is just that minimization refers to steps in the process, everything from collection to review to dissemination. And so I think we're talking about one element here, and to retention. And so there are different stages in the process.

To disseminate that information a certain threshold would have to be met and so forth.

MR. DEMPSEY: Yeah, I wish there were some way, I mean I know it's totally now embedded both in law and guideline and practice, but minimization means different things.

Minimization means keep it for five years and then delete it, minimization means don't disseminate identifying information, minimization means delete it unless it's intelligence information. Those are very different.

MR. LITT: Well, they all fall within the statutory definition of minimization essentially. I'm going to mangle it a little bit, but it's procedures that are designed to minimize the acquisition, retention, and dissemination of information about unconsenting United States persons consistent with the need to produce foreign intelligence information.

And so you're going to have different minimization rules based on the particular

missions of the agencies. You're going to have different minimization rules depending on the nature of the activity you're governing. You're going to have different minimization rules depending upon the nature of the information. But minimization is that entire category of rules.

MR. DEMPSEY: But it is a little bit of a circular definition which means different things in different contexts. Sometimes it means you've --

MR. LITT: I'm not sure I'd say circular but I would say it means different things in different contexts.

MR. WIEGMANN: It's a balance.

MR. BAKER: If I could just real quick just to emphasize, you know, as Bob was just alluding to, the FBI does have its own standard minimization procedures with respect to this type of activity. I assume you've had access to those.

So anyway, there's a lot on the table that we just talked about with respect to minimization, but I would direct you to those as

well in terms of understanding the FBI's role.

MR. MEDINE: Judge Wald.

MS. WALD: When a U.S. person information that's been, quote, incidentally acquired and kept for legitimate reasons or whatever in the base is disseminated to foreign governments, as is permitted under certain circumstances, it said that it's usually masked.

I think it would be useful for public consumption to know what the masking process entails, and in what circumstances it isn't masked, and whether or not the different agencies can use different criterias for masking or it's all centralized by Justice or the Attorney General's provision.

MR. DE: Well, I can speak just for masking generally at NSA, and abstracting from the second party issue for a moment, is substituting a generic phrase like U.S. person for the name of the U.S. person that is actually collected.

And that U.S. person is a legal term. Obviously that means an individual or it could

mean a U.S. company or firm.

I don't think there's a centralized process. That's how we do it at NSA. I think that's how other agencies do it as well.

MS. WALD: But different agencies decide how to interpret their own criteria as to what should be masked and what shouldn't?

MR. LITT: It's part of the, in the 702 context it's part of their minimization procedures.

MS. WALD: Well, so what does that tell me? No, I mean specifically as to whether or not in what circumstances it's not masked, that's up to each agency, or not?

MR. LITT: Yeah, it's done on an agency by agency basis.

MR. WIEGMANN: But generally speaking, I think the minimization rules of each agency generally would not permit you to disseminate U.S. person information where that is not either foreign intelligence or necessary to understand that foreign intelligence. So in other words --

MR. DE: Or evidence of a crime.

MR. WIEGMANN: Or evidence of a crime for FBI.

So in other words, if I need to, if it's Joe Smith and his name is necessary if I'm passing it to that foreign government and it's key that they understand that it's Joe Smith because that's relevant to understanding what the threat is, or what the information is, let's say he's a cyber, malicious cyber hacker or whatever, and it was key to know the information, then you might pass Joe Smith's name.

If it was not, if it was incidentally in the communication but was not pertinent to the information you're trying to convey, then that would be deleted. It would just say U.S. person. It would be blocked out.

So they were in communication with, and it would just say U.S. person. So that's essentially how it works I think more or less in all the agencies. Is that a fair description, Raj?

MR. DE: Yeah, the basic parameters for FISA collection are articulated in the statute, the big principles of necessary to understand foreign intelligence or evidence of a crime. And then that's effectuated through the minimization procedures that each agency has. That's for 12333 collection. It's articulated, as Bob mentioned, in 12333.

MS. WALD: With those last subpart, would those, just take NSA as an example, would those mask criteria also include foreigners, non-U.S. person's information?

I mean suppose the government of Romania asks some question which might require a Rumanian non-targeted person who's in your PRISM base, would these masking procedures, etcetera, apply there too or are they just for U.S. persons?

MR. DE: In today's rule, masking procedures are for U.S. persons because they are derivative of the constitutional requirement, the minimization procedures that need to conform with the constitutional parameters for U.S. persons.

MS. WALD: So it would be up to the agency to decide whether they thought it was right or wrong to give that information to a foreign government?

MR. DE: I think there's two points to mention. One is no information would ever be disseminated unless it had foreign intelligence value.

MS. WALD: No, I know.

MR. DE: That's the entire point of disseminating that information.

MS. WALD: But having made that decision in terms --

MR. DE: If I may continue. The second point is that I think what the President has directed the DNI to examine in the PPD is what protections could be extended to non-U.S. persons. That's the study.

MS. WALD: And that's what you're working on?

MR. DE: That's the issue we're evaluating now.

MR. BAKER: One quick comment though. If I'm not mistaken, if you look in 50 USC 1806, which is Title I of FISA but I think also applies to Section 702, it says, and I don't think it restricts it with respect to U.S. person or non-U.S. person, that no federal officer or employee can disclose, can use or disclose information at all except for a lawful purpose.

So the information could only be disclosed for a lawful purpose. And I believe that's across the board.

MS. WALD: I don't have anything more.

MS. COLLINS COOK: I wanted to make sure I understood though both Judge Wald's question and the response.

I understood her to be asking under what circumstances dissemination could be made to a foreign government.

Are there separate agreements and procedures that might govern in that instance or are analysts able to simply decide they would like to provide foreign intelligence information to

foreign governments?

MR. DE: At least our procedures, our publicly available procedures have provisions that address sharing with second party partners. I don't have at my fingertips the details, but I can certainly get back to you on that. But they are now public and articulate the circumstances under which information can be shared with second party partners. Those procedures are approved by the FISC annually.

MR. LITT: I think that the critical point is that these are part of the minimization procedures that have to be approved by the FISA court to the extent we're talking again about Section 702.

MS. WALD: The minimization procedures are only for U.S. persons, aren't they?

MR. LITT: Yes, that's right.

MS. WALD: But I was talking --

MR. LITT: But there are general rules about when we can share FISA information.

MR. MEDINE: All right. Well, I want

to thank the panel very much for spending a fair amount of time with us today and discussing these issues in a public setting and we appreciate it.

And we'll take a short break and then we'll resume at eleven o'clock with our second panel. Thank you.

(Off the record)

MR. MEDINE: We're now ready to begin our second panel, and we are very pleased to be joined by Laura Donohue, who's a Professor of Law at Georgetown University Law School, Jameel Jaffer, for a return engagement, Deputy Legal Director at the ACLU, Julian Ku, who's a Professor of Law at Hofstra University, and Rachel Levinson-Waldman, who is Counsel for Liberty and National Security Program at the Brennan Center for Justice, and each will make a brief set of remarks, if you want to start.

MS. DONOHUE: Sure. Thank you very much for the opportunity to be here today. I'm looking forward to the discussion on 702.

I'd like to confine my remarks to four

central areas, just my initial remarks, and raise statutory and constitutional concerns.

First is with regard to targeting. I'm particularly concerned about four areas here. First is the inclusion of information about targets, and not just to or from targets.

Second is the burden of proof regarding whether somebody is a U.S. person or not.

Third is with regard to the burden of proof regarding the location of the individual. That is, if the NSA in either instance does not confirm, does not actually know where they are, the assumption that is built into the minimization and targeting is that it is neither a U.S. person, nor are they domestically located. And there is no affirmative duty for due diligence on the NSA to actually check their databases to find out if that individual is or is not a U.S. person and is or is not in the United States. And then the implications for the right to privacy.

In the second area on the post-targeting analysis, I'm particularly concerned

about the role of FISC, that it's severely circumscribed and that we're having warrantless searches.

So in the last panel we heard about that moment at which the information is obtained is not a search because it's foreign intelligence and there's an exception for the gathering of the intelligence.

But when information is then used for criminal prosecution, then at that point when the data is searched, if it were a case where if I were, say, speaking with a mobster in the United States and they happened to overhear incidental to my communications that I was engaged in other criminal activity, they would have to go to a court to obtain a warrant to then put a wiretap on my phone and listen to the content of my communications.

In this situation they don't do that and then they find that individuals are implicated in criminal activity and refer it for criminal prosecution.

And I would be happy to address the 2002 Foreign Intelligence Surveillance Court of review opinion that addressed this aspect, but it was with regard to Title I where there was probable cause that had already been established that the target in that case was a foreign power, an agent of a foreign power.

In this particular case, the individual is not themselves the target of any investigation and so the prerequisite Fourth Amendment threshold has not been met.

The third area is the retention and the --

MS. COLLINS COOK: Can you slow down just a bit? I can't keep up. Thank you.

MR. MEDINE: And we also have a court reporter who's probably her fingers are slowing down.

MS. DONOHUE: Sorry, I beg your pardon. I realize we only have a few minutes, and I also have written remarks which I'll be submitting.

MS. COLLINS COOK: I have reviewed

them. Thank you. I've reviewed what you've submitted thus far.

MS. DONOHUE: Right. So I will be submitting on these particular points following the hearing.

On the third area, the retention and the dissemination of data, and this came up with Judge Wald's question on the previous panel, there are a number of exceptions in terms of when the information itself has to be expunged.

The foreign intelligence information exception I would direct your attention to. It's not defined in either Section 702 specifically, or in the minimization or targeting procedures.

It is, however, defined in FISA to include any information that would be helpful for foreign affairs, which would include economic information, it would include political information, it would include a whole range of data.

The retention, dissemination for criminal prosecution, I've raised the Fourth

Amendment concerns. We're starting to see now in courts what's called parallel construction where individuals where information has come from intelligence agencies' programs, is then passed on to law enforcement, who then must create a parallel trail for probable cause, but the actual tip or initial indication of criminal activity came from intelligence.

And it essentially covers the traces that this initially arose within FISA or within Section 702, and I have increasing concerns, certainly as a scholarly matter, about the growth of parallel construction.

The client attorney privilege you had already mentioned in the last panel. That continues to be, I think, an area of some concern, not just because it's, not just in the post-indictment stage but in terms of all communications with attorneys prior to and in the context of the interception of content.

The retention of encrypted communications was not mentioned in the last

panel. All encrypted communications are retained according to NSA documents, as well as the technical barriers. If there are technical barriers they also will simply keep the information.

The other aspects of this have to do with multiple databases and CIA access, which I was surprised you didn't have the General Counsel of the CIA on the last panel. We now understand from NSA documents that the CIA has a separate set of minimization procedures and also uses Section 702. And I think that's important to take a look at what those procedures are, both the targeting and the minimization.

Finally, the fourth area that I'd just like to raise is the First Amendment concerns that I have. As has been well-recognized in the judicial system, First and Fourth Amendments often travel hand in hand, especially in national security when political matters are on the line.

And in this particular instance not only do we have a general First Amendment concern

but we know that if individuals visit IP addresses, for instance, that have been associated with particular targets, then their correspondence, communication, emails, etcetera, and other information is also retained.

What if that IP address is Al Jazeera, let's say? What if that IP address happens to be a media or a news site that's been associated with a particular area of concern? Then I think there are also First Amendment implications that follow from that.

So in conclusion I'd be happy to talk in more detail about each of these areas, the targeting, the post-targeting analysis, the retention and dissemination of data, and the final First Amendment concerns.

MR. MEDINE: Thank you very much. Mr. Jaffer.

MS. DONOHUE: Thanks.

MR. JAFFER: Thanks for the opportunity to appear before the Board.

The ACLU's view, as you already know,

is that Section 702 is unconstitutional. The statute violates the Fourth Amendment because it permits the government to conduct large scale, warrantless surveillance of Americans' international communications, communications in which Americans have a reasonable expectation of privacy.

In our view, the statute would be unconstitutional even if the warrant requirement didn't apply because the surveillance it authorizes is unreasonable.

As I discuss in more length in my written testimony, the statute lacks any of the indicia of reasonableness that the courts have looked to in upholding other surveillance statutes, including Title III and FISA.

But the point that I would like to emphasize today is that even leaving the constitutionality of the statute to the side, the government is claiming and exercising more authority than the statute actually gives it.

I say that for three reasons. First,

while the statute was intended to augment the government's authority to acquire international communications, the NSA's minimization and targeting procedures give the government broad authority to acquire purely domestic communications as well.

That's because the NSA's procedures allow the agency to presume that its targets are foreign, absent specific evidence to the contrary, and because the procedures don't require the government to destroy purely domestic communications obtained inadvertently.

Instead, they permit the agency to retain those communications when they're believed to contain foreign intelligence information, a phrase that is defined very broadly.

Second, while the statute was intended to give the government authority to acquire communications to and from the government's targets, the NSA's procedures also permit the government to obtain communications that are merely about those targets.

And that practice, in my view, finds no support in the language of the statute or in the statute's legislative history. But it's a practice that has profound implications for individual privacy.

In order to identify the communications that are about its targets, the government has to inspect every communication. To endorse the practice of about surveillance is to say that the government can surveil literally everyone, or at the very least that it can surveil every communication in and out of the country.

Finally, while Section 702 prohibits reverse targeting, the NSA's procedures authorize the government to conduct so-called back door searches, searches of communications already acquired under the FAA using selectors associated with particular known Americans.

Given the absence of any meaningful limitation on the NSA's authority to acquire international communications under Section 702, it's likely that the NSA's databases already

include the communications of millions of Americans.

The NSA's procedures allow the NSA to search through those communications and to conduct the kind of targeted investigations that in other contexts would be permitted only after a judicial finding of probable cause.

And if I have thirty more seconds I would like to make just one final point. Today we're focused on Section 702, but it's important to understand that Section 702 is merely one expression of a broader philosophy.

Yesterday the Washington Post reported that the NSA has built a surveillance system called MYSTIC capable of recording all of a country's phone calls, allowing the NSA to rewind and review conversations as long as a month after they take place.

MYSTIC is the logical endpoint of the arguments that the government is making here today. So the stakes and the conversation that we're having today are very high. It's very

difficult to believe that democratic freedom would survive for long in a system in which the government has a permanent record of every citizen's associations, movements, and communications. Thank you.

MR. MEDINE: Thank you. Professor Ku.

MR. KU: Thank you, and thanks also for the opportunity to appear before the Board today.

I just want to remind -- I have a different view I think from most of the panelists, and I apologize for not getting my remarks ahead of time.

I just want to remind the Board of two under-emphasized points of constitutional law that I think should frame our understanding of the U.S. government's surveillance practices under Section 702.

I mean first, it is important to remember that Section 702 and FISA itself need to be interpreted and understood against the history, and tradition, and the background of the President's broad, inherent executive power under

the Constitution to conduct electronic surveillance of foreign governments and foreign agents, especially overseas.

Second, although we often speak loosely of the Fourth Amendment's limitations on this presidential foreign surveillance power, it's worth noting that courts have repeatedly upheld wide-ranging, warrantless U.S. government surveillance overseas, even of U.S. citizens.

So these two constitutional observations should frame any legal assessment of Section 702 and FISA in general.

If you keep in mind the background and where we're coming from rather than where we are, 702 is not an ineffectual attempt to regulate lawless executive conduct, as the critics would have it.

In actuality, Section 702 almost certainly requires more limitations than are actually required by the Constitution and may even, although I'm not taking that position, but could in some circumstances encroach on the

President's foreign affairs powers to conduct foreign intelligence activities.

So let me just briefly elaborate on these two claims about constitutional law, which I'm sure some folks might disagree with, but this is not a dispute that U.S. presidents have long exercised the power under the Constitution to conduct foreign intelligence, and this uncontroversially flows from the President's role as the chief of foreign affairs under the Constitution. And almost every court considering the question has concluded that the President, has agreed that the President possesses an inherent constitutional authority to conduct foreign surveillance. And this is undisputed by any court.

In other words, there does not need to be statutory authorization for the President to engage in foreign surveillance.

Prior to the enactment of FISA in 1978, the executive branch claimed, and the courts did not dispute that it possessed a broad

constitutional power to conduct surveillance for foreign intelligence purposes, even inside the United States and usually without a warrant.

So prior to the enactment of Section 702 and its predecessors, the executive branch claimed a constitutional power to conduct warrantless surveillance in foreign countries for foreign intelligence purposes, whether or not that surveillance included a U.S. citizen who was physically overseas.

So given this history I'd ask the Board to keep in mind that Section 702 and its predecessors placed more constraints on the executive branch's conduct of overseas foreign intelligence gathering than has ever been imposed in prior, in the past.

You might conclude that we need even more constraints, but we should not kid ourselves that existing constraints or even more constraints as proposed by some other folks, are consistent with historical practice and tradition and moves us further toward constraints.

As to my second point, I do not believe the Fourth Amendment imposes limitations on foreign intelligence as strict as those employed, imposed by Section 702. And let me just briefly explain the two reasons why.

First, it is very clear the Fourth Amendment does not apply to non-U.S. citizens and when they are outside the territory of the United States. And the Supreme Court confirmed this in the 1990 decision of The United State versus Verdugo-Urquidez.

So foreign citizens or the surveillance of foreign citizens outside of the United States is completely unconstrained by the Fourth Amendment.

Second, the courts have confirmed that it's highly unlikely the Fourth Amendment's warrant requirement applies to surveillance of U.S. citizens when they're outside of the United States, especially when the surveillance is conducted for foreign intelligence purposes.

No court in the United States has held

that a warrant is required for a search of a U.S. citizen when they are overseas if that search was conducted for foreign intelligence purposes.

Some courts like the second circuit have even held that no warrant is ever required for an overseas search, while others have relied on a broader foreign intelligence exception.

So there is further details here about the reasonableness, and courts have generally interpreted the Fourth Amendment's reasonableness requirement very generously in favor of the government when conducting overseas searches.

Again, in light of this long history and tradition of the United States conducting essentially unsupervised foreign intelligence gathering without any statutory authority, this is actually the tradition in the U.S. system prior to the enactment of FISA, then more recently Section 702.

So just to conclude, if you look at Section 702, the government faces a complete ban on the intentional targeting of any United States

person reasonably believed to be outside of the United States. And there are other procedural mechanisms, as you know about.

But I don't believe that actually the Fourth Amendment would actually require if there was no Section 702, the Fourth Amendment would require that the government could not intentionally target a U.S. citizen overseas and their communications.

So let me just conclude, I believe Section 702 should be understood as a sensible compromise between privacy interests and the continuing need to conduct aggressive foreign intelligence gathering. Congress has given its blessing to broad-based overseas surveillance that was already occurring pursuant to the President's inherent constitutional power.

Congress has now imposed limitations on those activities that go beyond what I believe the Fourth Amendment requires, but I think that's a small price to pay, and many of us agree, to minimize privacy intrusions into Americans'

overseas communications. And the courts are involved to provide oversight.

This is the type of political compromise and cooperation between different parties and different branches of government that we always wish, we always say we want, and so I think we should applaud it rather than condemn it.

MR. MEDINE: Thank you.

Ms. Levinson-Waldman.

MS. LEVINSON-WALDMAN: Thank you, of course, for having me here. I have a few brief comments and then I hope we'll also have a chance at some point potentially to respond to comments that were made during the first panel or during this panel.

So I'm just going to focus briefly on two primary issues that are reflected in my written submission for now.

First, I know of course that the Board is particularly interested in whether this about collection complies with the letter or spirit of Section 702. And based on the structure of the

statute, we believe that it doesn't.

Briefly, there are two main restrictions reflected in Section 702 on the collection of communications. So that would be the first, the acquisition cannot target U.S. persons or persons known to be within the United States. This is a geographic or nationality and residence restriction.

And second, that the purpose of the acquisition must be to acquire foreign intelligence information. And that's basically a content restriction. What that means is that the content of the communications that can be picked up by electronic surveillance is regulated by the foreign intelligence restriction, while the class of people who are subject to electronic surveillance is regulated by the targeting restrictions.

When communications that are about a target are collected, we believe sort of the what and the who of the collection are conflated, and that that's contrary to the clear structure of the

statute.

And we know that the results of the collection, our intention with the foreign intelligence requirement of the statute, that is, if communications that merely mention certain targets are collected then we know that significant quantities of communications that contain no foreign intelligence information whatsoever are acquired, which would appear to undermine the significant purpose requirement in the statute.

And of course this has been confirmed in the 2011 FISC opinion that was referred to that's been declassified. We learn in fact that the NSA does acquire tens of thousands of wholly domestic communication in the course of conducting that about collection.

And so for those reasons we do think that the about collection is contrary to the meaning and the structure of the statute.

And second, let me briefly mention one of the main contributions I think the Board can

make as part of its review, and I think that some of these questions came out in the first panel, which is to shed more light on some of the ways that Section 702 is being used.

It appears that what we don't know about Section 702, certainly for the public, still outweighs or outnumbers what we do know.

Obviously there will always be things that will be properly classified and kept secret, but it seems that there are many unanswered questions that the Board is in a position to help answer, help shed some light on.

So those questions would include certainly questions about how targets, and selectors, and key words are used. Some of those were answered in the first panel, but I think some of those answers also raised more questions.

There has been the suggestion, the strong suggestion from the 2011 minimization procedures that all encrypted communications can be retained by virtue of their being encrypted, and finding out if that, in fact, is true. And if

not, if the PCLOB can obtain and provide additional information about that provision.

And finally, and this is something that Laura mentioned as well, that domestic communications can be shared with law enforcement agencies if they are reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed.

In addition to raising, I think, a host of constitutional issues at the very least, and practical issues, one of the things that we don't know is whether there are minimum standards for how severe, for instance, such a crime has to be in order to share this information, which of course has been collected without a warrant.

So I hope that the answers to some of these questions also will come out during this process. Again, thank you for the opportunity to address the Board.

MR. MEDINE: Great, thank you very much for your opening statements. I'm going to ask you some questions but any panelist should feel free,

I may ask them to a specific person but anyone should feel free to jump in.

Professor Ku, you talked about the limited applicability of the Fourth Amendment to overseas collections, and maybe, and suggesting there's certainly no warrant requirement and a very generous reasonableness standard.

One question I have is the collections that we're talking about under 702 technically are happening in the United States. That is, the electronic communications provider is in the United States while admittedly the target is outside of the United States. Is that a distinction that you think has any constitutional significance?

MR. KU: That's a great question. I mean I think it reflects the difficulty of this, which is the technology is changing our, the way the Fourth Amendment was interpreted in some of these older cases, right.

So in the classic Fourth Amendment overseas case it was the guy searching through the

house or the apartment physically overseas of the U.S. citizen, or of the phone call that occurred on the foreign networks, right, in the foreign country.

Here we have this kind of weird situation where you have phone or communications sort of transiting through the United States. And I do agree that that might raise a harder Fourth Amendment issue, but I do think that the larger thing to keep in mind is that the geography matters because if there's a foreign person on the other side of the line, so to speak, that's I think in part the way the communication is an international communication. It has different implications for that perspective.

But I do agree that the Fourth Amendment, the territorial aspect of the Fourth Amendment would be less significant in that context.

I think the broader point though is that the courts have been very generous, both domestically and internationally about

surveillance conducted for foreign intelligence purposes.

So even, so the territorial distinction was something that FISA created, because prior to that I think FISA, the foreign intelligence gathering occurred both domestically and internationally, and the fact that it was for foreign intelligence was what mattered.

FISA has created this sort of territorial division, which I think is becoming less important with the changes in the types of communication we have.

MS. DONOHUE: If I may add to that. You know, Professor Ku brings up the exception for foreign intelligence gathering for purposes of surveillance. That's very different from the acquisition of information for purposes of prosecution. And here courts have very clearly ruled that even in cases of national security or domestic security, a warrant is required.

This is U.S. vs. U.S. District Court, a case handed down in 1972 in which there were three

individuals conspiring to bomb the CIA. And the court said that the executive branch, quoting Justice Brownell (phonetic) and others said the court -- the executive branch is not a disinterested neutral observer and cannot be put in the position of having to determine whether a search will be reasonable. They have to seek a third opinion on that.

In Katz as well in 1967, some of the justices in that case, Justice Byron White said, went beyond the decision and said basically we should not require a warrant procedure for the magistrate's judgement if the President of the United States, or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable.

And other justices responded very angrily to that statement. Justice William Brennan, Justice William O. Douglas, they pointed out that there was a conflict of interest here. They said, look, neither the President nor the

Attorney General is a magistrate. In matters where they believe national security may be involved they are not detached, disinterested, and neutral as a court where the magistrate must be.

The Foreign Intelligence Surveillance Court of Review has also considered whether or not information obtained from FISA warrants could be used in the event of a prosecution.

In the case that brought down the wall in 2002, the court looked to Title I of FISA where probable cause had been established that an individual was a target, sorry, that the target was a foreign power or an agent of a foreign power and said in that case you have this review that has gone on specific to that target by the Foreign Intelligence Surveillance Court.

In Section 702, individuals who may be brought up on criminal charges are not themselves the target of any investigation. No probable cause has been established for their involvement as a foreign power or an agent of a foreign power.

Instead, once the content of

conversations are obtained, then the government may go through, analyze the information and look for evidence of criminal activity, which can then bring them into a courtroom to face criminal charges, and at no point is this warrant requirement, which the court has held for domestic security cases. So here you have a U.S. person on U.S. soil and the court has said in U.S. vs. U.S. District Court, you have to have a warrant in that situation.

So to use the veneer of, well, we're just collecting foreign intelligence and the executive branch has the right to do this under Article II, yes, perhaps the executive branch can gather intelligence but if there are criminal penalties associated then you also need to meet the requirements of the Fourth Amendment for U.S. persons.

MR. MEDINE: I'd like to give Professor Ku a chance to respond, although I can do it on my next round.

MR. KU: Okay. Well, I mean I'm not

going to go through all the cases. And I think that the way I understand this is the way you think about this is the foreign intelligence purpose, right. The foreign intelligence purpose has been sort of an important part about whether there's an exception to the warrant requirement, or if there's a foreign intelligence purpose, sometimes a primary purpose, or a purpose, depending on how you define it. And then there's the, whether that gives a question of reasonableness, where there's legitimate government interests that goes to the reasonableness.

The reason I'm emphasizing the significance of the foreign intelligence purpose aspect of this and the territorial aspect of this is because I do think it's relevant to analysis.

This is, in fact, what's going on here is a collision between our law enforcement and intelligence goals here, right. So the U.S. government is gathering a lot of information for foreign intelligence purposes. It's also using

sometimes that information.

Some of that information is, although not I think so far frequently, leaking into criminal prosecutions. But if we start from the perspective of foreign intelligence gathering, right, this is Article II, this is where we start, and this is something that's largely been unregulated.

What's changed is that the nature of communications have changed so that many of the communications that were essentially gathered unsupervised for foreign intelligence purposes are being sort of routed in a different way so that it falls within, technically speaking, what we might consider a different sort of format, which then looks more like a classic Fourth Amendment case.

But I think that the larger point I'm trying to emphasize here is that this is, there are real Fourth Amendment issues here with respect to law enforcement.

But this is also about foreign intelligence gathering. It's not just a total

sham. It's not as if the government is claiming here that this whole thing is a scheme in order just to gather information for criminal prosecution.

Essentially they're both interests here that are part of this analysis. And that legal analysis with respect to foreign intelligence gathering needs to be considered and it should frame our analysis of what's going on here as well.

MS. BRAND: Thank you. So it's a good segue actually what you said, Professor Ku, because I want to understand, Professor Donohue, what you were saying, and I may not have taken the best notes, so forgive me.

But walk me through the argument, because a second ago you said that you were making a distinction between collection for foreign intelligence purposes and I think you said collection that was focused, was for the purpose of prosecution.

So are you, is it your view that 702

collection is for the purpose of prosecution?

MS. DONOHUE: It's one of the two stated purposes for which the information can be retained once it is collected. So it can be --

MS. BRAND: But that's different. But I'm asking about you said collected for the purpose of prosecution, I thought. I mean what is, I guess what I'm trying to get at is, is this distinction between foreign intelligence purpose and criminal purpose relevant at the collection stage only, or at all stages, or what? Help me understand what you're talking about.

MS. DONOHUE: Yeah, so in the previous panel Brad addressed this point. He mentioned that in the context of it's the moment at which the information's obtained that a search occurs, right.

So if we do our Fourth Amendment analysis at that point, then the moment at which you're obtaining the wiretap evidence is the search, at which point you would require a warrant under these.

And I believe Professor Ku's point is, no, you don't need a warrant if it's for foreign intelligence purposes at the moment you acquire the information with the international nexus to it. And he's citing Verdugo-Urquidez where there was no nexus to the United States and a search occurred overseas.

The problem is in the case, and this gets back to my first point, which I apologize if I spoke too quickly at the beginning of the panel, which is with regard to the targeting. If it is not just information to or from the target, or held by the target, but any information about or relating to the target.

And here, it's interesting, I was a little bit confused by the earlier panel because according to the actual documents the NSA has released, the NSA can actually use computer selection terms and other information such as words, or phrases, or discriminators to scan content.

So if it can collect all of the

international communications and then scan the content of those communications, then I would argue that is a search for purposes of the Fourth Amendment at the point of collection.

MS. BRAND: But let me get to this distinction though between foreign intelligence and a criminal purpose, because 702 requires not only that the collection be a non-U.S. person abroad but also that there be a foreign intelligence purpose, that the information be reasonably believed to be, to collect foreign intelligence. I'm not quoting the statute.

But doesn't that statutory requirement suggest that it has to be for a foreign intelligence purpose? And it might also then collect evidence of a crime, which then there are procedures for what to do with that information.

But it seems like you're suggesting that you think that the collection itself is for a criminal purpose, and that's what sort of piqued my interest and I wanted to understand what you were saying there.

MS. DONOHUE: Sure. So to push on this a little bit, under FISA to be a foreign power one is not a U.S. person, right, one is a foreign power or an agent of a foreign power. Not all of the agents of a foreign power require criminal showings, but many of them do.

So to say that this is purely a foreign intelligence purpose when an individual can be targeted based on being either a foreign power or an agent of a foreign power, in which case there is criminal activity involved and there may be the element of criminality from the outset. So it's not as though criminality is not an aspect of the foreign intelligence gathering generally.

MS. BRAND: Professor Ku, do you have -- Jameel, it looks like you wanted to respond.

MR. JAFFER: Well, I was just going to speak to the foreign intelligence exception more generally, if you want to pursue this.

MS. BRAND: Go ahead. Go ahead.

MR. JAFFER: Well, so I just want to caution the Board about starting from the premise

that there is in fact a foreign intelligence exception to the warrant requirement. The cases in which courts have held that there is such an exception predate FISA. There's arguably one exception to that, but the vast majority of them predate FISA.

And so their rationale has been undermined by practice under FISA over the last thirty-five years. The rationale for those cases was in large part that the courts might not be capable of overseeing collection or surveillance for foreign intelligence purposes. But the courts have been doing precisely that now since 1978.

But even if you accept that there is in fact a foreign intelligence exception to the warrant requirement, you have to ask the question of how broad that exception is.

And all of those cases, those pre-FISA cases, involve cases involved situations in which there was probable cause to believe that the target was a foreign agent, the surveillance was approved personally by the President or the

Attorney General, and the primary purpose of the surveillance was to gather foreign intelligence information.

And Section 702 doesn't include any of those requirements. So no court has ever approved a foreign intelligence exception to the warrant requirement that is broad enough to read Section 702. Section 702 is a broader statute than any foreign intelligence exception recognized so far would allow.

I think that it may also be important to emphasize that concluding that the warrant requirement applies doesn't mean that the government has to get a warrant before surveilling legitimate foreign targets. It doesn't mean that in order to surveil, you know, some suspected terrorist outside the United States the government necessarily needs to get a warrant.

But at the very least it means that the government needs to take reasonable measures to avoid acquiring Americans' communications without warrants.

It means it has to not acquire them in the first place where it cannot acquire them.

When it does acquire them, it has to destroy the communications that it acquires relating to U.S. persons.

And when in narrow exceptions it retains those communications, there should be a back-end warrant requirement so the government doesn't access Americans' communications without a warrant. That's what compliance with the warrant clause would mean.

MR. MEDINE: Ms. Cook.

MS. COLLINS COOK: So thank you all for coming. I find these panels to be incredibly helpful and informative.

Ms. Donohue, I would like to -- Professor Donohue, I apologize, I'd like to follow-up on something you mentioned at the very end of your opening remarks, and that's your position that 702 raises First Amendment concerns.

I think it's clear from my previous separate statement on our 215 report that I don't

necessarily approach the First Amendment analysis the same way, but what I would find helpful from you is if you could just describe your approach to when the First Amendment would be implicated, when concerns arise, and when something would be unconstitutional based on First Amendment concerns.

So for example, would a traditional wiretap raise First Amendment concerns, and would it potentially be unconstitutional under First Amendment concerns?

Would a traditional grand jury subpoena for bank records or credit card statements that could reveal payments to lawyers or payments to various charities or associations, would that raise First Amendment concerns? Would it be unconstitutional under the First Amendment?

So if you could just walk me through on the spectrum where you're finding concerns and where you're finding violations.

MS. DONOHUE: Sure. And just to return back to Ms. Brand's point, I agree with Jameel on

the analysis about what point it would kick in for a warrant requirement is the point at which it's either about the information, because I feel like I didn't quite answer what you were asking me and I want to make sure that I do, I answer it.

It's the point at which you're getting information about that particular individual, which is a different target, and then you analyze that information, then at that point I would believe that the Fourth Amendment warrant requirement would apply.

Okay, so in response to the First Amendment question, so the courts have recognized that there is a close link between the First and the Fourth Amendment. And I frequently find whether it's in remote biometric identification systems in view of public space and facial identification, you know, that there is a First Amendment context there as well. So it tends to be in the shadows in the room.

In this particular context, the way that I see it present is with regard to the target

that is in the statute. It's very clear that the target cannot be selected --

MS. COLLINS COOK: I'm sorry, can you actually answer the question that I had posed, which was, for example, starting with a traditional --

MS. DONOHUE: Oh, yeah, so I do not see a traditional wiretap as implicating First Amendment. I do not see --

MS. COLLINS COOK: Why?

MS. DONOHUE: Because --

MS. COLLINS COOK: Even though it could, for example, reveal the fact that I belong to the ACLU, or I have called my attorney, or I'm discussing, you know, private contents and communications. So why not?

MS. DONOHUE: Because there's a balancing that occurs with regard to the element, in this case of probable cause that you have committed, are committing, or are about to commit a crime under Title III, in which case having gone before a neutral, disinterested magistrate, a law

enforcement officer says, oh, no, I suspect that Professor Donohue is engaged in this bad activity. And I think that that balancing test basically takes that situation out of a First Amendment context.

MS. COLLINS COOK: So let's take a grand jury, and then a pen register trap and trace. So a pen register trap trace, there's definitely no determination, no probable cause. So does a traditional pen register trap trace, which would reveal potential phone calls to the ACLU, to my lawyer, very private, the existence of potentially private conversations, does that violate the First Amendment?

MS. DONOHUE: Again, with prior judicial approval and review, no.

MS. COLLINS COOK: Okay. So let's take a grand jury subpoena which can be issued by a prosecutor. So in the absence of beforehand judicial review, does that violate the First Amendment?

MS. DONOHUE: No. I would say --

MS. COLLINS COOK: So what's the factor --

MS. DONOHUE: Well, it's the same for administrative warrants, I would say in the case of administrative warrants. Here's where the tipping point is for me with PRTT, let's take Section 215 as kind of a bulk metadata collection program, or Section, what is it, 402, right, for these bulk collections of pen register trap and trace type information.

When you have the bulk collection of information in a way that changes the political discourse in society, then I think you have a First Amendment question that arises.

MS. COLLINS COOK: Okay. So is if there is a perception that there is a change in political discourse, then you have a concern about a First Amendment? It's not necessarily prior judicial review, particularized probable cause?

I'm just struggling to understand, you know, at what point there's a First Amendment implication and at what point there's a First

Amendment violation, because to me, I think it's a bit of a sea change to look at either traditional or really these FISA authorities as violating the First Amendment. I do think that that's a fairly novel approach.

MR. JAFFER: But to be fair -- to be fair, the distinction between individualized surveillance and bulk surveillance is also a bit of a sea change. And so I think the question is whether the bulk surveillance, the fact that the government is now engaged in bulk surveillance, I mean I understand that there's some dispute over the vocabulary, but the fact that the government is engaged in bulk collection or bulk acquisition of this information makes the First Amendment relevant in a way that it perhaps wasn't relevant in the context of individualized surveillance of the kinds that you were describing.

I mean I think that your question perhaps goes more broadly to the question of incidental overhears, you know. When the government defends Section 702, one of the

government's defenses is that all of this information is, about Americans is overheard incidentally.

You know, I go into this in a little more detail in my written submission, but I don't think it's fair to call this kind of collection incidental in any conventional use of the term. The collection of Americans' information is entirely foreseeable, and in fact, it was the purpose of the statute.

If you look at the statements that administration, then Bush administration officials made to justify the statute or to advocate for the statute, they were quite forthright about the purpose of the statute. And the purpose in their view was to give the government broader authority to collect information, collect communications between people outside the United States, and people inside the United States.

And obviously there's no illegitimacy to the government's interest in collecting those communications. The question is whether there are

sufficient safeguards in place, but that's why I say that incidental is probably the wrong word.

But if the government is relying on the incidental overhear cases from the Fourth Amendment context, those cases were, involved very different contexts. Those were cases in which the surveillance was individualized. It was based on a probable cause warrant.

The scale of the surveillance of the incidental collection was much different. And the fact that there was judicial oversight at the front-end provided a kind of protection for incidentally overheard people that doesn't exist under a statute like 702.

MR. MEDINE: Let's give Jim the chance to ask some questions, then we can come around.

MS. DONOHUE: Okay.

MR. DEMPSEY: Thanks. Thanks to the witnesses.

A question for Jameel and for Rachel on the abouts. What actually is, quoting the words of the statute, what is the strongest textual

argument against about surveillance?

Because the statute says the targeting of persons, never really refers to even the collection of communications or interception, etcetera, so if you're collecting something about somebody, isn't that almost paradigmatically targeting the person? Where's the text?

MS. LEVINSON-WALDMAN: I mean I think one of the -- right, there's obviously ambiguity in the statute in part, and this is one the things that I mentioned in the written submission is that target isn't defined.

And I have to say some of the answers in the first panel, which answered some questions about target and selectors, I think also opened up new questions.

I do think the strongest statutory argument, literally looking at the language, is what the statute talks about.

So it says here, literally just looking at 1881 A, subpart A, Attorney General and Director of National Intelligence may authorize

jointly the targeting of persons reasonably believed to be outside the United States to acquire foreign intelligence information.

So as I say, you sort of see implicitly, but I think you do see implicitly these two sort of halves of the targeting requirement, the foreign intelligence requirement and this kind of nationality and geographic restriction, and that when what you're doing is collecting about communications, what you're doing is kind of adding together, you're kind of conflating, you're morphing together these different parts of the statute so that the targeting has usually been literally thinking about the facility that's being used --

MR. DEMPSEY: Excuse me. The government has determined that a person is outside the United States and that collecting information about that person will yield foreign intelligence.

MS. LEVINSON-WALDMAN: Well, but I think that may be what's suggested by the about collection, but I think the foreign intelligence

determination is a separate one, right.

The government identifies these targets or selectors which have generally been to or from. And in fact we know, especially from Judge Bates's opinion that thousands, tens of thousands of communications are collected using the about targeting, the about collection, that are wholly domestic, that have no foreign intelligence value, which I think undermines an argument that there has been some determination of foreign intelligence value there, because to some extent the results are sort of speaking for themselves.

MR. DEMPSEY: Because then you would be questioning the legitimacy of the to and froms because they only do abouts about people that they also do to and froms, so you can't say that the foreign intelligence determination of the abouts is illegitimate because then you call into question the to and from.

MS. LEVINSON-WALDMAN: Well, but I think the to and from is pretty clearly contemplated by the statute, right? You target a

person, you are trying to find communications to or from them, understanding that those will have foreign intelligence value.

MR. DEMPSEY: Let me go to Jameel. Jameel, what is the best textual argument against abouts?

MR. JAFFER: Right. Well, let me first I think agree with what I think Rachel was saying at the outset, which is that the statute I don't think explicitly forecloses about surveillance or explicitly authorizes about surveillance.

But I think a fair assessment of the statutory structure and some of the statutory text leads to the conclusion that about surveillance was not contemplated by Congress. And I'll answer your question.

MR. DEMPSEY: The text, yeah.

MR. JAFFER: So here are a few aspects of the statute that I think show that Congress was contemplating, that the target would, himself or herself, be the person whose communications were acquired.

First, a definition of electronic surveillance. It says the acquisition of the contents of any wire --

MR. DEMPSEY: This is not electronic surveillance. 702 explicitly does not cover electronic surveillance.

MR. JAFFER: Well, I think that the point I'm making is relevant nonetheless.

MR. DEMPSEY: Electronic surveillance definition is irrelevant to 702. It is not -- 702 does not regulate electronic surveillance.

MR. JAFFER: I think the point that I'm trying to make is just that the entire statutory scheme, both FISA and the FAA, contemplate that the person who is the target will be the person whose communications are actually acquired.

If you look at the definition of aggrieved person, for example, which does apply in the FAA context, aggrieved person to implicitly contemplates that the person who will be raising the claim as an aggrieved person is a person whose communications are actually acquired.

And in fact, if you conclude otherwise what you are concluding is that the target would be an aggrieved person even if his or her communications weren't acquired, which I think is a nonsensical conclusion and one that the government itself would reject.

But I think it follows from accepting that about surveillance is contemplated by the statute.

And if I could just make a sort of broader point about about surveillance, we have sort of combed through the legislative history for discussions of this kind of surveillance, and it's possible we overlooked something, but we have not found any exchange in the legislative history around the FAA that suggests that Congress was contemplating about surveillance.

To the contrary, when people discuss, when legislators discuss the kind of surveillance that would take place under the statute, they discuss surveillance of the target.

And even on the government panel this

morning one of the panelists used the example, bad guy at Google.com, you know, which again is suggesting that the surveillance that's going on is of the target himself or herself.

And in defending the statute before the Supreme Court, the Solicitor General and the Justice Department more generally characterized the statute as one that allowed the government to collect targets' communications.

So you know, I think that this is an entirely a foreign concept, foreign to the legislative history and foreign to the text of the statute.

MR. MEDINE: Thank you. Judge Wald.

MS. WALD: Let me pick up on the about thing and pose one of those terrible hypotheticals. If you had a to and from, you had a targeted, a legitimately targeted person and in the process of collecting information you got, you came across this email between, I'll be facetious a bit, the grandmother of one of them to the grandmother of somebody else saying something

along the lines of, my grandson was talking to me and he was telling me all about this wonderful service he did by plotting, I'm using an extreme, plotting to blow up a facility kind of thing, I mean how would you take care of that situation where you had it between two people who are not the to and froms? You wouldn't ignore it, would you, or would you? I mean how would you handle that if you had no abouts?

MS. DONOHUE: I'm not sure whom that's directed to.

MS. WALD: I don't care.

MR. MEDINE: Who would you like it directed to?

MS. WALD: What?

MR. MEDINE: Who are you asking?

MS. WALD: Well, the two people who've talked about what about abouts, Mr. Jaffer and Ms. Levinson-Waldman, I think.

MR. JAFFER: Well, I'm not a hundred percent sure I understand the question. The question is, you know, if you were conducting

about surveillance and you come across evidence of a terrorist plot, do you really expect them to ignore it? Then no, I don't, you know.

But that's like asking, you know, if the government breaks into a home unconstitutionally and finds evidence of a terrorist plot, do I expect them to ignore it? I don't.

But we still need to ask the question what are the proper limits on the government's surveillance authority in the first place, and I think that we need to draw those limits in a way that's consistent with the Constitution.

I'm not sure that I'm answering your question.

MS. WALD: Well, you are except that I'm puzzled, too. I'm not sure I know the answer where, as I say, you had -- maybe that's an extreme example about where they have a plot, but where there's actually some foreign intelligence information which even everybody would agree had some relevance to a legitimately targeted

individual, and it's right there, and it's picked up.

MS. LEVINSON-WALDMAN: Then I think I would echo Jameel's points to some extent and sort of elaborate to say that I do think that there are always hypotheticals, presumably for any of these programs, for Section 702, for Section 215, for other collection programs that are going on where there could be some piece of information out there that might be useful that would be collected by a program.

I think it's dangerous to build surveillance programs and to think about the constitutionality and the practicality based on hypotheticals, and especially when we know that there is significant over-collection that occurs and significant collection of Americans' communications.

I think the hypotheticals are, may need to be thought about, but I don't think that they can drive how we think about the constitutionality and the statutory implications of the collection.

MS. WALD: In other words, you or anybody over there wouldn't consider if that happened, some other means that the government might have to take that about information and go to somebody, to some authority and say can we keep this, can we use this, etcetera, etcetera?

MS. DONOHUE: So what I'm a little bit confused about, and I did hear the previous panel say, oh, well, there would be all sorts of procedural implications if we had to return to a judge on the Foreign Intelligence Surveillance Court to get approval to do further monitoring.

What I'm a little bit confused about is if that information was appropriately obtained in the first place and it indicates that other people are implicated, why they wouldn't go back for a Title I electronic search and they would have what they need for that?

MS. WALD: Well, if it's two grandmothers, they're probably not -- they're just chatting. They're probably innocent. All I'm saying is I guess the only reason I raised it is

I'm trying myself to figure out are there not some gray areas here, and wondering if you had any solutions short of about authority which you find is too broad, and completely ignoring it?

But let me not use up my whole five minutes. Thank you.

I did want to ask you about, as you know, the President's review commission said they wanted to see a warrant, an actual, go get a warrant for probable cause before you could search the data using a U.S. person indicator.

My question to you is, and we've heard some reasons why they think that's very onerous, including the fact that the President's review commission's recommendation was it had to be a probable cause warrant that the person was about to commit something, do bodily injury, or about to commit some terrorism crime.

My question to you is if you think there are legitimate, and you do, problems under the Fourth Amendment with using U.S. person indicators to surveil the PRISM data, would

anything short of a probable cause warrant such as they recommended satisfy you, i.e., I'm just throwing this out, you know, having, going back to, say, to the FISA court and having them look at it to see if it, either post or pre, before they used it, approving this so-called, you know, selector, etcetera, that was in fact a reasonable cause to believe that the person had information or didn't have information?

MR. JAFFER: I don't think that would be sufficient. I think that you need a warrant at the back-end and --

MS. WALD: But what kind of a warrant warrants --

MR. JAFFER: A warrant based on probable cause and --

MS. WALD: Probable cause of what?

MR. JAFFER: Well, so I think it could be foreign intelligence probable cause, although I hope that the panel will, that the Board will think about the scope of the definition, the definitions of foreign agent, foreign power, and

foreign intelligence information.

But I think that foreign intelligence probable cause could be sufficient for that particular process, or obviously criminal probable cause.

But I also just want to say that I don't think back-end procedures alone are enough, no matter how strong they are. And I think that, you know, I know that the Board can't talk about the Washington Post report from yesterday, but if you just take it as a kind of hypothetical, you know, if you accept that back-end procedures are enough and that we'll focus solely on the protections on searching, and dissemination, and analysis of information in the government's hands, there's nothing to prevent the government from recording every phone call, copying every email, creating a permanent record of everybody's movements, associations, and communications. And the only question we'll be asking is when can the government access it.

But the creation of that kind of

massive database will have huge implications for the way that ordinary people operate in society, both the way that they interact with one another and the way that they interact with their government.

People who believe that the government is surveilling every movement and every communication, believe justifiably that it's doing it, will act differently. They won't go to controversial websites and they won't engage in controversial communications that are necessary for any democracy.

MS. WALD: I'll save, I know my time is up. I'll wait for the next round. I have another question.

MR. MEDINE: I want to go back to that back-end searching, basically the U.S. person searches, and this really is two questions.

One is the government panel asserts that this is lawfully obtained information and therefore should be permissibly used without any further Fourth Amendment implications. And why

that's not a persuasive argument.

And then two, if it's not persuasive, what is the procedure that you envision? And again, I think it's different from Professor Donohue where you're using that U.S. person information to get more information. You're just saying let's use the information we've already collected under some other, under authority for, say, criminal purposes or foreign intelligence purposes.

So I guess it's two parts. Why isn't is already legally usable? And if it's not, what procedure would you apply to access it? And that's to any panelists.

MS. DONOHUE: So as a statutory matter I would come back to the burden of proof with regard to whether that information that's being collected on targets, they are indeed U.S. persons or non-U.S. persons and located outside the United States.

So here the statute is silent, and I share Mr. Dempsey's textual analysis of the about

question. I think the statute is silent there as well. But in regard that the statute does say where you know that somebody is a U.S. person, you know, you have Sections 703 and 704 that you have to operate under.

MR. MEDINE: Again, we're not targeting the U.S. person, we're targeting a non-U.S. person, and Congress clearly knew that at the other end of that phone call could be a U.S. person and still authorized that kind of collection without a warrant.

And the question is, why isn't that sufficient to then say, okay, this information was lawfully collected, now we can do searches based on it?

MS. DONOHUE: Because it isn't certain that the person on whom you're collecting the information really is a non-U.S. person. So the burden of proof on the NSA is to say, to establish that this individual is a non-U.S. person.

But in fact, so the assumption that all

the collection that's going on currently is of non-U.S. persons I think is an erroneous one. And it's one -- and the reason why I think it's erroneous is because the NSA is under no obligation to check and see and make sure that that individual is not a U.S. person.

To the contrary, they have in their documents they say, well, they may check these databases, they may check these other databases. There's no obligation that they do so.

Mr. De in the previous panel referred to the totality of the circumstances type tests that say they have two strikes against, four strikes for, they look at everything. There is nothing that obliges them to then go back and dig up more information to find out in that particular circumstance.

And not only that, but actually if you look at the requirements for what is required to positively identify, to conclusively determine it in the minimization procedures, the bar is actually significantly high.

It means that you know their name, you know their title, your know their address, you know their personally identifiable information in the context of activities conducted by that person that are related to that particular person. A reference to a brand name, manufacturer's name, Monroe Doctrine, etcetera, that's not sufficient.

So not only are they under no obligation to establish that but in order to establish it, it's a very high bar. So it's not clear to me that that information is lawfully collected in the first place.

MR. MEDINE: Ms. Levinson-Waldman, do you want to weigh in on that?

MS. LEVINSON-WALDMAN: I think the other thing I was going to add, if I'm understanding the question correctly about why is it not okay to do searches on information that's been lawfully collected, I think there's also an element of bootstrapping.

So that it was lawfully collected for a purpose, for a foreign intelligence purpose, and

that you're right, of course Congress knew that U.S. person information was going to be incidentally collected through that process, but then there are these minimization procedures.

And so kind of almost bypassing those procedures and allowing that body of information to be collected without meeting a fairly high bar, some kind of probable cause warrant seems like kind of going back and bootstrapping your way into that information in a way that is very different from searches of, I think, any other, almost any other body of lawfully collected information, because the standard for which it's obtained, that foreign intelligence standard and purpose is so different.

MR. JAFFER: I mean I actually think there are two kinds of bootstrapping. The first is pointing to the fact that foreigners outside the United States lack Fourth Amendment rights in order to collect huge volumes of communications to which Americans are a party.

And then the other is pointing to the

foreign intelligence purpose to gather information which is then later used in criminal prosecutions. So that's to state the problem. It's not a solution to the problem, but I think that's where the concern comes from.

MR. MEDINE: Professor Ku.

MR. KU: If I could just add, I mean I'm not sure that's bootstrapping. I think that's sort of the purpose, right. The purpose is -- it's not that they're not also collecting it for foreign intelligence purposes.

It's also true that if in the old days they came across a letter from an American person to a foreign person, it seems unlikely to me that because an American sent the letter that means they can't -- but they lawfully obtained the letter, it's unclear to me why they couldn't use that letter.

And so I'm a little, possibly it's bootstrapping, but it's, there's a long history of going after foreigners and doing foreign surveillance.

I'm not sure that -- I think the only difference I think is technology does make it easier for it to flip back into the states, but I'm not sure that fundamentally this is a really different thing.

MR. MEDINE: Thank you. Ms. Brand.

MS. BRAND: Thank you. Well, it seems like there are some fundamentally opposing world views about the Fourth Amendment on the panel, and I want to, I mean this Board is not going to move Fourth Amendment law. So I want to get to what you think the law is and what you think the law should be, because I think there might be some conflation of those two things going on here.

First of all, Professor Ku, thank you for submitting your comments this morning, your written comments. I haven't had a chance to read them yet so I just want to ask you a question to make sure I understand where you're coming from.

You talk about inherent executive authority to conduct surveillance abroad or even of non-U.S. persons abroad. In your view, does

that inherent executive power operate alongside the Fourth Amendment, or irrespective of the Fourth Amendment, or does that create an exception to the Fourth Amendment?

MR. KU: Right, no, I don't think it creates an exception to the Fourth Amendment. It operates within the constraints, whatever they might be, of the Fourth Amendment.

But I would like to point out that historically this -- I mean so just to clarify. The reason I raise this, it goes to the point that historically the U.S. government as operated without statutory authority to conduct foreign surveillance. It's been, the power was granted, was thought of as coming from the Constitution.

So the statutory scheme has not been thought of as necessary to authorize the type of intelligence gathering that's going on.

Now the Fourth Amendment does apply, but as I also emphasized, it hasn't always applied. It didn't originally was thought of to apply at all, even to U.S. citizens overseas, but

I think we understand that the courts have come around to view that it does apply to U.S. citizens overseas. But I think it still has a limited impact compared to the way it applies for purely domestic searches. So that's how I would analyze that.

MS. BRAND: And how does it apply to purely domestic searches where there's a purpose of foreign intelligence gathering?

MR. KU: Well, I think that -- well, here I think that, you know, it does. The Fourth Amendment has been interpreted in recent cases to be a much more robust protection for searches domestically, although even in some of those cases, right, a warrant has not been required or the exception to the warrant requirement has been found for foreign intelligence purposes. So it still continues to exist within the domestic sphere.

I would say that for me, at least my understanding is a lot of this has been supplanted by the FISA system. The rise of the FISA system

has to some degree made the Fourth Amendment analysis a little bit less onerous because what's been happening is that everything's been funneled through the FISA system and the challenges to the FISA system has not been sort of as robust.

I think if we hadn't had FISA maybe we'd have had more cases that would have clarified exactly what the Fourth Amendment limits on domestic foreign intelligence searches would be. I do think that it applies more strongly to domestic searches and I think it has more significance.

But I do think that ultimately the foreign intelligence exception to the warrant requirement is a reasonable one that does need to be respected. It has a long tradition in history.

In my view, really FISA is sort of on top of that to add additional privacy protections that I think Congress has judged, and probably rightly so, we need. But I'm not sure the Fourth Amendment itself standing alone would necessarily require all of the sort of procedural limitations

and minimization protections that we have.

MS. BRAND: Okay. And Jameel, can you very briefly, because I have another question for you, you do not think there is any foreign intelligence exception to the Fourth Amendment? Is that what I heard you say earlier?

MR. JAFFER: I don't think that there's any foreign intelligence exception broad enough to justify 702, and no court has --

MS. BRAND: But there is -- I mean I guess what I'm trying to get at is, do you think that the Fourth Amendment applies equally to collection for the purpose of foreign intelligence gathering as it applies to collection when the purpose is to gather evidence of a bank robbery, for example?

MR. JAFFER: I think that there are certainly narrow circumstances in which the courts have held that there is a foreign intelligence exception.

Again, those cases predate FISA, and so you know, you have to evaluate whether those cases

survived the thirty-five years of experience under FISA.

MS. BRAND: Okay. And then you referred earlier to, I think you were referring to, well, you're referring to 702 generally as large scale collection. I'm not sure if you were including both upstream or PRISM in that assessment.

But if you were here for the first panel and if you take the government's facts as they stated them to be true, what about that program strikes you as large scale? What's your justification for that description?

MR. JAFFER: Well, so two responses to that. The first is I think it's important to draw a distinction between statutory restrictions and executive restraint. So there's a question of what the statute allows and then there's a question of how the government is implementing it.

Obviously I know much less about how the government is implementing it than I do about what the statute on its face allows because I can

read the statute and I have access to only a portion of the government's documents.

But then as to, you know, whether it's large scale collection or not, I think that the problem is that everybody is using these words in different ways. The panelists this morning said that they weren't drawing a distinction between acquisition, surveillance, and collection. But their own documents do draw a distinction.

If you look at USD 18, for example, which is the Defense Department's implementation of the executive order on intelligence collection, it draws a distinction between electronic surveillance and acquisition on the one hand and collection on the other.

And collection involves the tasking of that, or tasking of communications, whereas electronic surveillance and acquisition do not.

And so, you know, we have always thought of this, putting the vocabulary to the side for a second, we've always thought of this in two stages. There is a kind of, just to -- there

is a kind of, you might call it scanning, you might call it collection, but there's a kind of large scale acquisition of data, and then there's the government tasking that data, and then there is the government's tasking that data with selectors.

So to be a little more concrete, if the government installs on a switch somewhere installs a device that either diverts all of the communications or a large portion of the communications, or scans a large portion of the communications, we would call that bulk collection.

I'm not sure that anything turns on vocabulary but we should all make sure we're talking about the same concepts.

MR. MEDINE: Ms. Cook.

MS. COLLINS COOK: Actually that was right at the top of the last piece. I think we've used, and in this conversation alone we've used scan, inspect, acquire, collect, access.

And so I guess my question is, if you

have access, so in your hypothetical you've installed something that gives you access to this stream of communications, is that a seizure or a search for the purpose of Fourth Amendment analysis in your view?

MR. JAFFER: Well, I think it would depend what you were accessing. You know, the question would be have you invaded a reasonable expectation of privacy?

But we have taken the position that, for example, the bulk accessing of telephone metadata is an invasion of a reasonable expectation of privacy, and we would certainly take the same position with respect to the bulk acquisition of telephone calls or emails.

The MYSTIC program, again, just discussing it as a kind of hypothetical, that program in my view involves the bulk collection of telephone calls, voicemail messages, and telephone calls, even if the government doesn't access more than a small proportion of them.

MS. DONOHUE: May I add something to

that just very quickly? I was a little bit confused in the earlier panel because on the one hand they were saying this is a very limited program. On the other hand they say that this SIGAD is the most used NSA SIGAD.

The slides that have been released say it draws from Microsoft, Google, Yahoo, Facebook, Paltalk, YouTube, Skype, AOL and Apple, that it gets voice over Internet protocol, email, chats, all this information, and it's hard to square that.

And what they say is the value of the program, with its limited nature --

MS. COLLINS COOK: I'm sorry, can we talk about -- I appreciate your desire to talk about the previous panel but I had a specific question out that I'm really trying to understand the panelists' view on when the Fourth Amendment is implicated and how.

And so if it's under your hypothetical if you have the acquisition of all phone calls from a country with subsequent access, at what

point would the Fourth Amendment attach?

MR. JAFFER: I would say certainly the moment you put it in your databases, by that moment the Fourth Amendment has attached.

MS. COLLINS COOK: So flipping that, if it's access to a wide swath of communications but acquisition into the government's possession or control, when would the Fourth Amendment attach?

MR. JAFFER: I'm sorry, but I've lost track of the difference between access and acquisition.

MS. COLLINS COOK: And this is part of the, I think you've used scanned, but some ability to review a stream of communications and pull, filter, something to that effect.

MR. JAFFER: Right. The scanning or the filtering would implicate the Fourth Amendment in my view.

MS. COLLINS COOK: That's helpful. I wanted to follow up on a different set of questions and just close the loop.

If the determination was made that the

acquisition of the information pursuant to 702 was lawful, it's lawfully acquired information, would you still take the position that a subsequent search, and by that I mean a query using a U.S. person identifier, would need some sort of probable cause determination, that there would be a separate Fourth Amendment analysis?

And can you explain why? I guess is this because there's a view that there's a lack of particularity of the front-end and therefore you have to have subsequent some particularized finding?

MR. JAFFER: Yes.

MS. DONOHUE: That would be my position as well.

MS. COLLINS COOK: Okay. One question for Professor Ku, if I could. We've heard that 702 is silent, I think it's fair to say on the precise question of abouts. There are some structural arguments here and some purpose arguments that you can look to, but it's silent.

In view of the evolution of our

understanding of Article II of FISA, how would you as a constitutional matter assess a silence in 702? Because Title VII is both an authorization and a restriction on Article II authority, so.

MR. KU: Right. So I think, I don't know if I have any sort of grand insights on the purely textual analysis, although I do think that the constitutional background is what can help us here with respect to, if we understand where we're coming from can help us analyze this.

If we understand that constitutionally that the U.S. government was engaged in broad searches prior to the enactment of 702 then you have to sort of think about, well, to what degree.

This is not really about authorizing, this is really about restricting, imposing restrictions on what I think the U.S. government had the authority to do prior to the enactment of the statute.

And so if you look at it from that perspective then, if it doesn't, the silence or the lack of clarity or specificity would then I

think lead me from that perspective to suggest that the President retains that power.

I would analogize this a little bit to the point that was made in the earlier FISA statute, how they excluded radio completely from the original FISA, radio communications, they just said nothing about it.

And there are a lot of people that argue that was on the assumption that most of the foreign intelligence was radio in 1973 and that the President would continue going on gathering as much radio signals intelligence as he could. And then at a certain time, no one used radio anymore.

But the point is that if you add the restriction in the statute it doesn't -- the previous or the other authority the President has to conduct the surveillance should in theory continue, and I think would likely to continue here too, assuming he had the authority prior to the enactment.

MR. MEDINE: Mr. Dempsey.

MR. DEMPSEY: A quick comment and then

a question. Going to the definition of distinctions between collect, acquire, etcetera, my comment is we really have to take yes for yes and no for no and move on. The government has said, to my mind totally clearly, they are not relying upon the USD 18 concepts in implementing 702, so I think that we just have to move on from that. That's my comment.

My question is the following, and this is for Jameel or anybody, Rachel, in terms of the querying of data otherwise lawfully acquired, what is the best case law that would limit the proposition that data lawfully acquired can be subsequently queried without limitation?

MR. JAFFER: Well, so on your comment, I think you're certainly right that the government said on the panel earlier today that they were not relying on the distinction, any distinction between acquisition and collection.

But I think that the government also acknowledged that it was engaged in about surveillance, and to engage in about surveillance,

my understanding is that there is no way to engage in about surveillance without inspecting in some sense every communication within the universe of those that you are monitoring or surveilling. There's no way to do it.

Now you can call that bulk collection or you can call it something else, but that scanning of every communication in a particular universe raises constitutional issues, and if all you're saying, Mr. Dempsey, is we should just address those constitutional issues, then I entirely agree.

MR. DEMPSEY: So now as the querying of otherwise lawfully acquired communications, and let's take, you know, if I steal your computer, I think, and then I give it to the government, the government lawfully acquired it. I may have stolen it. Or certainly in the Title III context the government lawfully acquires, or in the normal search and seizure context, or in the voluntary disclosure context, where is there case law limiting the proposition that lawfully acquired

information cannot subsequently be queried essentially without prior authorization, without meeting any threshold? What is, is there any case law limiting that?

MS. DONOHUE: So we're starting to see cases come out of border security issues where computers -- border security issues, and I'd be happy to send you the names of the cases afterwards, where computers have been lawfully seized under customs laws but then they cannot be searched for all of the information on them because of the privacy implications that are involved and lack of a sufficient nexus to the suspected criminal activity.

So those cases might be one source that you would look to in a new age of data where so much information is available.

MR. JAFFER: You know, I think it's important to ask the question the other way around as well, which is, you know, where is there case law showing that the Constitution is indifferent to the government collecting huge

volumes of communications without any individualized suspicion or particularity, and then sort of bootstrapping its way into free rein or --

MR. DEMPSEY: Again, if we're in a situation, I'm just trying to pose the situation of let us assume, just let us assume that the collection was lawful.

MR. JAFFER: I'm not suggesting for these purposes that the collection was unlawful. What I'm saying is that the collection here is different in kind from the kind of collection that the courts have been concerned with in other cases involving the use of information lawfully acquired. You know, it was important to those cases not just --

MR. DEMPSEY: So then the license plate readers, the information collected by the license plate readers is lawfully acquired and then the government can subsequently query that license plate database. I mean that's standard procedure.

MR. JAFFER: I'm not sure that it's

established with any certainty that the bulk collection, that the querying of a database of bulk collected license plate reader information doesn't raise Fourth Amendment concerns, and I think that that's still an open question.

MR. DEMPSEY: Well, I'm looking for some cases. Professor Donohue has some border cases --

MS. DONOHUE: I'd be happy to send you the border doctrine cases.

MR. DEMPSEY: That may be relevant. I would welcome any other cases limiting that proposition.

MR. MEDINE: Judge Wald.

MS. WALD: This is probably an unfair question but I'll ask it anyway. Given the fact that the grievances about 702 as it operates today have included a whole series of things, one we didn't discuss here but it's been raised in written stuff is the lack of FISA review of particularized targeting designations. I know it's allowed by the statute, but nonetheless the

capture and use of incidental U.S. information to search database, the use and retention of the U.S. information.

But my question is, if you had to focus on one or maybe two important changes that you would like to see made now in 702, what would they be? Very quickly, anybody that wants to answer it.

MS. DONOHUE: I would say limiting the information to, or from, or held by the actual target and inserting a mechanism of judicial review if information is uncovered that would lead to subsequent criminal prosecution prior to analysis of the databases that are held.

MS. WALD: Okay, great. Down the line.

MR. JAFFER: The only thing that I would add to that is destruction of inadvertently acquired communications. Communications that the government itself acknowledges should not have been acquired in the first place should be destroyed immediately.

MS. WALD: Destruction, they say

they're purging them but you mean something --

MR. JAFFER: There are broad exceptions to the --

MS. WALD: I know there are exceptions, but you mean -- okay.

Do you have any, Professor Ku?

MR. KU: Actually, I mean this may be kind of not what you're looking for, but I do think that actually I would prefer the FISA section clarify the default that I've been arguing for, that it doesn't encroach, to clarify further that it doesn't encroach on, Section 702 doesn't encroach on the President's, you know, foreign intelligence authority. That would, I think, help our interpretation of the statute.

MS. LEVINSON-WALDMAN: And I just would mention three things. One is I agree more robust involvement by the FISC.

MS. WALD: I'm sorry, more?

MS. LEVINSON-WALD: More robust involvement by the FISC in terms of review. There's some review now that is sort of a

box-checking procedure, and have that review be more --

MS. WALD: Just the way they do what they do now, but more carefully?

MS. LEVINSON-WALDMAN: Well, I'd say not even, it's not so much that I think that they're not careful with it now, it's that the statute actually limits the scope of some of the review that they do, that they sort of don't get behind the curtain.

MS. WALD: Including the targeting.

MS. LEVINSON-WALDMAN: Right. I guess the second, thinking about, so if you think about Section 702 but having the minimization procedures be a natural part of that statute.

Certainly limiting and potentially eliminating the use of information for law enforcement purposes. And obviously this is something that the NSA, that the President's review group spoke to as well and made that recommendation.

And then the third quite honestly would

be to lift the standard back up to agent of a foreign power from the foreign intelligence requirement. And the foreign intelligence purpose is so loose and that that seems to be --

MS. WALD: For targeting?

MS. LEVINSON-WALDMAN: For targeting, yes, that's correct.

MS. WALD: Okay. I've got maybe one minute left so a quick question. Some of you, I don't remember now, all of you in a prior one, when we were doing 215, talked about the desirability/necessity of having an adversarial element in the FISA proceedings.

A very quick notion of how would you see an adversary, however appointed, in a 702 proceeding? In other words, what function could they serve, he or she serve in a 702?

215 was a little bit more evident. A novel technological case coming up to the court, what would you say, do they have any, would they have any function in a 702?

MS. DONOHUE: So I would imagine them

having a function absolutely, yes. The ACLU tried to do this and was not allowed to intervene on a motion on a First Amendment grounds and it was denied by the court in part on the grounds that they would never succeed on the First Amendment to actually intervene.

I think having an advocate there would allow them to more carefully review minimization procedures, to more carefully review targeting procedures. It would allow them to evaluate the role that they play with regard to targeting.

MS. WALD: In individual cases in 702?

MS. DONOHUE: And in individual cases, yes, but you would have to change to insert some sort of a warrant requirement equivalent for criminal prosecution or further examination of the records.

MR. JAFFER: And I think that our biggest concern is with judicial rulings that have far-reaching implications and not just implications in the individual cases. So I think that when you're talking about the individual

cases, I do think that, you know, in theory an adversarial process would be a useful thing.

On the other hand, I think that the closer you get to an individualized warrant application, or court order application, or surveillance application, the more it looks like traditional Title III or a search warrant context, which is ex parte.

But you know, when you get to judicial opinions that authorize about surveillance at some level of generality, that is something that ought to be argued in open court, you know, with a closed hearing to follow if there is legitimate, if there are legitimate sources and methods to be protected.

But if I can just use the process to add one answer to your previous question, I agree very strongly with what Rachel said that reforming or revising the standard, the targeting standard is crucial.

Right now there is, there's really no limit on who the government can target overseas.

The example that the government panelist kept coming back to is bad guy at Google.com or bad guy at Yahoo.com. But it could as easily be journalist at Yahoo.com, or human rights activist at Yahoo.com. And I think it's crucial that some limits be drawn around the category of people whom the government can legitimately target.

MS. WALD: And by the FISA court?

MR. MEDINE: We only have a couple of minutes. If there's any members of the Board who want to ask any additional questions.

MS. COLLINS COOK: Can I ask just one quick follow-up question on this point actually?

MR. MEDINE: Sure.

MS. COLLINS COOK: And this is to Ms. Levinson-Waldman. You had said lift the standard back to agent of a foreign power or a foreign power. What were you referring to when you said back to?

MS. LEVINSON-WALDMAN: Right, I mean I guess back to, we're sort of envisioning to some extent Section 702 is sui generis and when it came

into being it was a foreign intelligence requirement. But I guess thinking of FISA more broadly, narrowing that foreign intelligence standard in some way to match what is in other sections.

Obviously one option would be matching what's in other sections of FISA, agent of a foreign power, I think that would be our preference, but narrowing that in some way. Back was probably an imprecise way of referring to it.

And if I could add one other brief thing, I think our other, you know, if we have a wish list it would be, and again, I'll say restore, but thinking about other parts of FISA, having the collection be, and you know, these may be one or the other but having the collection, the foreign intelligence be the primary purpose rather than a significant purpose, that that has also allowed, you know, potentially a fair amount of slippage in terms of what the collection is for.

MR. MEDINE: Any other final questions? I want to thank the panelists very much for

joining us today. It was a very enlightening discussion. We're now going to take a lunch break and we will resume with our third panel at 1:45. Thank you.

(Off the record)

MR. MEDINE: Good afternoon, and thanks everyone for rejoining us. And I want to introduce our third panel, which will be on transnational and policy issues.

We are joined by John Bellinger, who is a partner at Arnold & Porter, Dean Garfield, who is the President and CEO of the Information Technology Industry Council, Laura Pitter, who is a Senior National Security Researcher at the Human Rights Watch, Ulrich Sieber, who is the Director at the Max Planck Institute for Foreign and International Criminal Law in Freiburg, Germany, and Chris Wolf, who is a partner at Hogan Lovells.

Each of the panelists will make a brief opening statement and then we will proceed with the Board questioning.

I guess we can start alphabetically

with Mr. Bellinger.

MR. BELLINGER: It's me first then. Well, thank you all very much for having me in, the members of the Board. I'm going to focus my comments on whether international law places any restrictions on electronic surveillance of foreign nationals outside the United States.

I think you know I served as the legal advisor for the Department of State from 2005 to 2009, as the legal advisor for the National Security Council from 2001 to 2005, and then I was the national security advisor to the head of the Criminal Division at Justice Department before that, so I have extensive experience, both in intelligence activities and international law.

So in recent months I think you know many scholars and human rights advocates have argued that NSA surveillance of foreign nationals violates a so-called universal right to privacy recognized in international law.

They base their argument on Article 17 of a human rights treaty called the International

Covenant on Civil and Political Rights, which the U.S. ratified in 1992.

Article 17 provides, and I quote, no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence, end quote.

The argument that NSA surveillance violates Article 17 of the ICCPR is incorrect for several reasons. And I will say in my view international law, neither the ICCPR or any other part of international law placed international legal restrictions on the NSA, any of the NSA programs.

With respect to the ICCPR, first, for the last sixty-four years the United States government has taken the consistent position that it does not apply outside the borders of the United States. The U.S. took this position when we negotiated the treaty in 1950, and we re-articulated it in 1995, when the Clinton administration submitted its first report to the U.N. Human Rights Committee, which is the group

that oversees compliance with the ICCPR.

My predecessor at the time, the then legal advisor Conrad Harper, explained to the committee that the ICCPR imposes obligations on the United States only inside the United States. And that's because Article 2 of the ICCPR, which defines its scope, says that a state party is bound to respect and ensure the rights in the ICCPR only to all individuals within its territory and subject to its jurisdiction.

And as my predecessor, Conrad Harper said at the time, this is a dual requirement that establishes that treaty obligations apply only if both conditions are satisfied. An individual must be under United States jurisdiction and within United States territory.

And now the negotiating position of the United States of the treaty confirms that interpretation. The phrase, within its territory, was added at the request of the head of the U.S. delegation, Eleanor Roosevelt at the time in 1950. And she explained that, quote, the purpose of the

proposed addition is to make it clear that the draft covenant would apply only to persons within the territory and subject to the jurisdiction of the contracting states.

There was a vote held on that addition and that addition was adopted 8 to 2 in 1950. Subsequent efforts to change that have failed.

And again, in his statement to the Human Rights Committee in 1995, Conrad Harper explained that the words were added, quote, with the clear understanding that such wording would limit the obligations to within a party's territory.

Now it's true, and I know that Laura Pitter is going to talk about this, that the Human Rights Committee and a lot of human rights groups in other countries don't agree with the long-standing U.S. interpretation, but the Human Rights Committee's statements don't have binding legal effect on the United States or to any other country. We give respect to them but they're not binding on us.

Both the Bush and the Obama administrations have confirmed the Clinton administration's position that the ICCPR does not apply extra-territorially.

In fact, just five days ago in Geneva we were making our periodic report to the Human Rights Committee and the acting legal advisor, Mary McLeod, told the committee, quote, the United States continues to believe that its interpretation that covenant applies only to individuals both within its territory and within its jurisdiction is the most consistent with the covenant's language and negotiating history.

So we really have fifty years of U.S. practice on this point recently reaffirmed by the Obama administration.

But even if the ICCPR did apply extra-territorially, the treaty would still not place limits on NSA surveillance because persons in other countries are not subject to U.S. jurisdiction.

The Human Rights Committee itself has

defined the phrase subject to a party's jurisdiction to include people within the power or effective control, or effective control of the forces of a state party acting outside its territory. So not even the Human Rights Committee is suggesting that everybody who may be subject to NSA surveillance is actually within the power or effective control of the United States.

And I would want to hear more from my colleague who I've met before, Professor Sieber, but even if they're unhappy with NSA surveillance, I am not aware of any foreign government that believes that the ICCPR or any other provision of international law imposes an obligation to respect the privacy rights of non-citizens.

In fact, candidly, most foreign governments spend lots of time spying on foreign citizens. So they may be unhappy with what we're doing as a policy matter, human rights groups may suggest that there are binding legal norms, but I'm actually not aware that foreign governments are suggesting that there is an actual violation

of international law.

And finally, just to close on my analysis of the ICCPR, and then I'll wind up, even if the ICCPR did impose certain obligations on United States extraterritorial conduct, even if people outside the United States were considered to be within the jurisdiction of the United States, Article 17 of the ICCPR still only bans, quote, arbitrary and unlawful interference with privacy.

Now we can certainly argue about constitutes arbitrary and unlawful interference but there is no international norm on that point. I'm sure lots of people can suggest that the NSA program is arbitrary, that it's unlawful, but when we're talking about international law there has to be actually a specific norm that people have agreed to, and there is no generally accepted framework under international law that defines what kind of surveillance is unlawful or arbitrary.

So the bottom line, despite statements

that we are violating the Article 17 of the ICCPR, it just simply does not apply, nor does any other provision of international law.

And so let me close by saying that just because international law doesn't actually create a universal right of privacy that's binding on the United States, I'm by no means saying that we ought to be insensitive to the rights of non-citizens. Certainly if I were still in the White House I would be saying, you know, we need to be respectful of concerns both of individuals or of leaders. That's why we make these policy decisions.

President Obama's recent presidential policy directive states that signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information.

So it's perfectly appropriate to take

into account privacy interests, but international law does not place binding legal obligations on us. Thank you.

MR. MEDINE: Thank you. Mr. Garfield.

MR. GARFIELD: Thank you. Thank you members of PCLOB on behalf of fifty-six of the most dynamic and innovative companies in the world, thank you for inviting us to testify today. And thank you as well for your efforts to advance both national security and civil liberties.

From our perspective we have the firm view that those two concepts are mutually reinforcing and in fact are not mutually exclusive and so we want to do whatever we can to support your efforts.

I'd like to focus my testimony on two areas. One, what we're experiencing in the marketplace as a result of the NSA disclosures and, then share some solutions that may help remediate some of the challenges that we're facing.

On the first, the economic impact from

the NSA disclosures are significant and ongoing. The folks in this room are very familiar with Section 215 and the distinction between that and Section 702, but for folks outside of this room much of what they experience and what we're experiencing is diminishing trust, particularly diminishing trust in U.S.-based technologies. So rather than made in the U.S.A. being a badge of honor, it's increasingly becoming a basis to question the integrity and security of technologies.

That has a real world economic impact. In fact, there are a number of analyses out there that put the numbers of the impact in the tens of billions of dollars.

As significant, perhaps even more significant than the economic loss is the broader societal impact and the implications for the Internet more generally. We're celebrating this year the 25th anniversary of the commercialization of the Internet and are all very familiar with the benefits and the way it's transformed all of our

lives.

Increasingly, what we're seeing though are policies aimed at changing the open, ubiquitous, globally-integrated Internet into one of walled silos. And so the legislation that's actually being debated today in Brazil would create walled gardens around their data.

And it's not simply limited to Brazil. We're seeing the same in Europe, as you all know, where the parliament is questioning the continuing viability of the safe harbor, or in particular territories within Europe where they're calling for country-specific clouds that would again create these islands of walled silos rather than an open, integrated Internet, which we all know the implications of that.

And so what do we do about it? I'll offer up three sets of solutions that build on global principles that we released earlier this year after working with our members to forge consensus on it.

And I place the emphasis on global

because we firmly believe that in order to address these issues and to address them effectively, high level, global communication and engagement around surveillance is critically important.

The first aspect or screed of solutions is around transparency. This body, the PCLOB in its January report made the point that transparency is the foundation for democratic principles. We firmly agree. We also think it's the foundation for separating fact from fable.

And so to the extent that there's a greater awareness, particularly around 702 where there are protections in place already, for there to be greater awareness about that would be quite helpful.

As it relates to our companies, the ability to share with the public more about 702 and 215 and the requests that come in pursuant to those, as well as the accounts, particularly the numbers, would be incredibly helpful. And so greater transparency is one element of what we would recommend.

The second relates to oversight. And as I've said in other places, including my testimony on the hill, our solutions are offered with a great deal of humility because we don't know what we don't know. I don't pretend to be able to offer the exact framework for making sure that there is a civil libertarian advocate or a civil liberties advocate within the FISA or FISC court process. But developing a framework for enabling that, we think is very important.

Finally, the last set of solutions are based on working to rebuild the trust that has been eroded, and there, a few unequivocal statements from our government would be quite helpful.

By way of example, there has been a lot of reporting around steps that may or may not have been taken to undermine encryption standards. NIST has been very firm in taking steps to make sure that they bolster the encryption standards that are being developed.

But a statement from our government

that they don't, do not intend to take steps to undermine the integrity of our cyber -- to undermine the integrity of those standards would be incredibly important.

Similarly, taking steps to affirm that data acquisition pursuant to 702 is not being done in an indiscriminate manner, I think would also be incredibly helpful. With that, I'll pause.

MR. MEDINE: Thank you. Ms. Pitter.

MS. PITTER: First, thank you very much for this opportunity. Thank you for having me. We've filed a more lengthy statement with the Board so I'm just going to be a little bit more brief here.

I was asked to talk about U.S. obligations under the International Covenant for Civil and Political Rights so I'll start with that.

And obviously, I'm going to disagree with Mr. Bellinger on this issue, as did Harold Koh's recently released memo where he disagreed as well and tried to get the Obama administration to

take a different position, arguing that it was not actually in the U.S. interests to continue to not apply the ICCPR in an extraterritorial manner.

There has been debate about whether or not this treaty applies outside of U.S. borders and it stems from, as Mr. Bellinger said, the operative jurisdictional clause in the covenant which says that states have an obligation to respect and ensure that those within its territory and subject to its jurisdiction, the rights under the covenant.

So the word jurisdiction in that clause has been interpreted to mean power and effective control. But the U.S. does not accept that. It takes a strictly territorial stance. And this essentially means that a state has to abide by the covenant within its territory but then it can willfully violate the covenant outside its territory, killing and pillaging at will outside its borders, which doesn't really make any sense.

Treaty law requires that the language of the treaty be interpreted in accordance with

its context, as well as its object and purpose. And the context in this case was post-World War Two when the treaty drafters were aiming at empowering people with rights universally and not diminishing them, and responding effectively to Nazi atrocities.

To interpret the treaty in that limited way would allow, for example, Nazi Germany to run a concentration camp in Poland, as Marco Milanovic, a prominent scholar on this issue has pointed out.

And the U.S. is the clear outlier on this. Only the U.S. and Israel take such a strict interpretation of the treaty.

So how does this apply to surveillance and the right to privacy? Some have argued that even if the ICCPR applies extra-territorially it should only be in the case where the government has physical control over the individual, like in the context of detention or torture. And that doesn't apply to surveillance simply because the individual is not within a state's effective

control.

But the problem is that their communications are. And so to not recognize even a duty to respect the right to privacy in this context creates a kind of absurd situation where the U.S. would be barred from going into someone's house in Germany and taking letters out of someone's drawer but not barred from reaching into their computer and doing the very same thing remotely.

These are novel questions, and I won't deny that. The Human Rights Committee, which is the main interpretive body of the ICCPR, has not adjudicated this matter.

And though there is a body of case law in other jurisdictions, particularly in the European Court of Human Rights, that have the issue and they do provide some guidance on a framework for how to analyze surveillance laws.

That said, those decisions, they came out before the Snowden revelations so they're not informed by a lot of the information that's come

in the public domain about the vastness of the collection that's going on.

But these issues are novel in the U.S. too. Just because there may not be necessarily a case en point does not mean the obligations or the rights don't exist. They are in the treaty.

Just as like many in the U.S. have argued that U.S. law has to catch up with technology and recognize a reasonable expectation of privacy in metadata, international law has to acknowledge that when it comes to surveillance, though an individual may not necessarily be in a state's physical control, their communications are, and the right to privacy can be violated remotely through technical means.

But just because the obligation applies extra-territorially does not mean that the surveillance has to stop. There is a framework within which surveillance can take place, but also be in accordance with human rights obligations. The surveillance has to be lawful and non-arbitrary and necessary to a legitimate cause

that's proportional to that legitimate aim.

By all accounts, that's not what 702 is. 702 may all be for the purpose of protecting U.S. national security, which would be a legitimate aim, but are there more narrowly tailored ways to achieve that aim?

And if the answer to that question is no, and I'm going to quote from the review group here, the question is not whether granting the government authority makes us incrementally safer but whether the additional safety is worth the sacrifice in terms of individual privacy, personal liberty, and public trust. And also, is it really worth the other harms that will result?

We're in a situation now in which countries are rushing to enact laws that would localize data collection and companies are rushing to offer alternatives to customer data being stored in the U.S.

And from a technological standpoint data flows are not necessarily based on geography but travel the cheapest, most efficient route.

This means a transfer to someone in the same country can mean data passing through many countries without the sender even knowing it. So a failure to respect the right to privacy extra-territorially imposes, exposes U.S. data to vulnerability when it's situated in other states.

The President has already essentially recognized all this. His presidential policy directive purports to bring the rules on retention and dissemination of data collection on foreigners closer to those that govern data on U.S. persons.

But it did not end bulk collection and specifically exempted data temporarily acquired to facilitate targeted collection.

Also, this was through an executive order not legislation, so it could be changed by future administrations.

The bottom line is that the U.S. is in a unique position because most of the world's data flows through its borders. And this confers an obligation to respect the privacy rights of those individuals whose communications fall within the

U.S. jurisdiction, but also to refrain from interfering with the ability of other countries to protect data, protect their own citizens' data. And a failure to recognize the value of this undermines U.S. business and long term national security interests.

The administration says it will make some changes but the law remains the same and that too has to change.

MR. MEDINE: Thank you. Mr. Sieber, Professor Sieber.

MR. SIEBER: Thank you very much for your kind invitation. It's a pleasure to be here.

International legal obligations for U.S. surveillance programs for which you are asking can be based on two different sources, interests of states and interests of persons. The two are interrelated since the protection of a state's territory also has effectual protective functions for its citizens.

Let me start therefore with a few remarks on this broader approach before turning to

specific human rights, which have been addressed here.

General international law and Article 2 of the U.N. Charter protects the sovereign equality and territorial integrity of all states.

A state therefore violates territorial sovereignty if it accesses, copies, or manipulates non-public data in computer systems located in a foreign state because such acts initiate in data processing on the servers located in a foreign territory.

There are no norms in public international law that permit violating other states' sovereignty by across the board world-wide surveillance.

There is also no customary rule of international law that permits the infringement of sovereignty resulting from acts of espionage.

In addition, espionage committed from the premises of embassies violates the obligations under Article 3 of the Vienna Convention on Diplomatic Relations.

These infringements of the territorial integrity of many states by large scale surveillance programs have two impacts for our topic. First, with respect to policy considerations, infringements of the territorial integrity of foreign states violate international law, plus in addition also national cyber crime statutes that are globally agreed upon in the Budapest Convention.

These violations pose serious threat to the continuing trust and the integrity of the U.S. and its IT industry. This infringement may be more serious than the violations of privacy rights, the scope of which are controversially in dispute in most countries.

Secondly, transnational surveillance programs on foreign territory take over the security functions of the affected states. This transnational control deprives citizens of protection by their own state and any other legal protective systems in these security measures, since their home state cannot protect them against

unknown foreign violations of their privacy and the intercepting foreign state often does not recognize any aliens' rights outside its territory where the interception is taking place.

In such a global system the citizens, including U.S. citizens, are deprived of any protection, especially if authorities of different countries exchange certain data.

Thus we are all losing a protective system which mankind has won in a long historical battle dating back to the Enlightenment. Thus, if we are engaging in transnational surveillance programs we must at least recognize certain basic human rights apply to all humans, regardless of nationality and place of residence. And if we want to create an effective global solution this must be supported by international human rights, to which I will now turn.

In the field of international human rights I will also concentrate on Article 17 of the International Covenant of Civil and Political Rights. The International Court of Justice, the

U.N. Human Rights Committee, both in its case law and in its General Comment 31, as well as many national courts and governments acknowledge the extraterritorial applicability of the ICCPR.

I also simply refer to the well-founded memorandum presented by Harold Koh, former legal advisor at the U.S. State Department in 2010 and 2013, with respect to the ICCPR. Koh is convincingly for the extraterritorial applicability of the conventions.

According to the prevailing opinion, the ICCPR is extra-territorially applicable to anybody within the power or effective control of the acting state party or its agents.

In the physical world, extraterritorial applicability of the ICCPR is thus limited to situations in which the government has total or special control, spatial control over a territory.

Since communications and privacy rights are by their very nature exercised in the virtual world and are prominently infringed upon there, the control of this virtual world by highly

extensive surveillance programs should be a decisive factor.

If we do not accept these conclusions we still must deal with an argument of the German Constitutional Court, which also might be relevant for the American discussion. The court argues that telecommunication interception not only infringes upon privacy rights by the first act of recording the telecommunication, it also infringes on these rights by the following data transmission to their home country, the analysis, the linking, the long-lasting storing, and by further transmissions to other recipients.

All these acts are repeating and deepening the infringements of privacy rights and they are undoubtedly committed on the territory of the surveilling states. Thus, even in cases of foreign intelligence gathering, we are not dealing only with actions outside the national territory.

Accepting the arguments for the transnational applicability of specific international human rights would promote then a

deeper discussion on the substantive scope of international human rights protection of privacy.

A first attempt to define the contours of the international concept of privacy can be seen in the already mentioned U.N. General Assembly Resolution 68167 of last December on the right to privacy in the digital age.

When this discussion proceeds, it will be most important to recognize that threats from abroad are different from internal threats. Thus the principle of proportionality as developed by international and national courts will lead to very different results in different circumstances, such as for data collection to homeland, in Afghanistan, or today in the Ukraine.

These necessary differentiations under the principle of proportionality can recognize many U.S. security concerns. Thus applying certain transnational privacy rights would not prevent a reasonable security policy, especially also since the ICCPR is self-executing in the U.S.A. and national foreign citizens could not

initiate judicial proceedings against the U.S.

In sum, I would advocate for an international solution and discussion in order to maintain or regain the leading role of the U.S. as an advocate for the rule of law and human rights in democratic societies, as well as for the trust in its IT industry and its clouds.

If time is not yet ripe for an international human rights solution, then more emphasis should be placed on national efforts to provide more guarantees for non-U.S. persons.

For that reason I welcome the respective U.S. Presidential Directive 28 of last January to applying certain safeguards for all individuals, regardless of the nationality of the individuals to whom the information pertains or where that individual resides.

This policy is also the position of the German constitutional law. In case of your interest it would be a pleasure for me to provide you with more details on these comparative legal aspects later on in the discussion. Thank you.

MR. MEDINE: Thank you. Mr. Wolf.

MR. WOLF: Thank you, Mr. Chairman. As Chairman Medine said at the outset, I'm the partner in the law firm of Hogan Lovells, where I lead the firm's global privacy practice.

And in 2013 Hogan Lovells published a white paper examining the similarities and differences among various legal regimes that authorize and limit governmental access to data.

And our work began before the Snowden NSA disclosures in response to the claims of certain EU cloud service providers that storage of data in the EU made it safer from surveillance than storage with a U.S.-based cloud provider.

Obviously following the Snowden revelations the argument in support of allegedly secure from surveillance regional clouds has been renewed loudly.

A previous white paper we did on governmental access to data internationally noted the availability of mutual legal assistance treaties and other forms of cross-border

governmental sharing addressing faulty claims of regional cloud service providers about the invulnerability to foreign government access that local cloud storage might provide.

Our 2013 white paper specifically looked at Section 702 surveillance and the frameworks in Australia, Canada, France, Germany, and the United Kingdom. My written and oral testimony today synthesizes the findings from this white paper and includes additional information on similar laws in Brazil, Italy, and Spain that we intend to publish soon.

I will note that our white paper foreshadowed last week's report of the European Parliament criticizing the practices of certain EU member states for the lack of transparency and controls on their surveillance activities.

My principle point today following our white paper is straightforward. While the policies and practices of the United States addressing surveillance and related privacy concerns obviously need to be and are being

reassessed, the U.S. has on its books greater due process and independent oversight of surveillance activities than many of our fellow democracies.

As you know, Section 702 surveillance requires court approval, surveillance is limited to foreign intelligence information, and oversight mechanisms exist for 702 surveillance.

As our white paper revealed those same limitations are not always found in the law of many of our counterparts. Australia, Canada, France, Germany, Italy, and the United Kingdom do not require court approval for national security surveillance.

In France, the intelligence agency is allowed to conduct surveillance to protect economic and scientific assets, even when national security interests are not at stake.

On the issue of intelligence agencies secretly and without any process at all asking companies for data, we have found that Australia, Canada, France, Germany, and the U.K. allow their governments to ask private entities voluntarily to

disclose data to the government.

In the U.S. the government is not allowed to seek voluntary transfers. A neutral judicial body must approve the government's request for data.

Last week's resolution by the European Parliament recognized extensive surveillance systems in EU member states, and the lack of control and effective oversight that some EU member states have over their intelligence community.

The resolution also questioned the compatibility of some member state's massive economic espionage activities within the EU, with the EU internal market and competition laws. The parliament did not go into the detail of our white paper, but its resolution reflected the baseline findings of our research, that there are substantial deficiencies in transparency about and controls over national security access to data in countries outside the U.S.

Thus when also considering the cross-

border sharing arrangements available to governments for information they collect through surveillance, it is misleading in the extreme to contend that so-called regional clouds provide individuals with security from government surveillance.

I commend this Board for engaging in an assessment of U.S. surveillance practices and looking at how these practices relate to our counterparts. There are no guarantees in the U.S. or elsewhere that agencies will abide by the laws restricting national security surveillance, but the degree of authorization required and the kind of review that occurs is obviously relevant to a determination of how well personal privacy and personal liberty are protected.

Thank you again for the opportunity to present the findings of our white paper and I'll look forward to your questions.

MR. MEDINE: Thank you very much.

I want to turn to the ICCPR for a moment, and as I understand it there are really

two issues here. One is the jurisdictional test, and if you pass that then the substantive test with regard to evaluating whether the 702 program affords appropriate protections or is arbitrary in some fashion.

I want to start with the jurisdictional issues, and that is, I guess there are three interpretations of the applicability of the treaty. One is that there has to be both territorial presence and jurisdiction. The other is there could be one or the other. And I guess the co-approach, which is they sort of split it, and that is there is a respect requirement across the board and an ensure requirement only subject to the territorial and jurisdictional issues.

I want to ask about the jurisdictional side. As we know from discussion earlier today and what's been made public is the information that's being collected under the 702 program is being collected in the United States, albeit about non-U.S. persons.

I guess my question is for the

panelists, how should we, how should one interpret jurisdiction? It's not going to be up to us to interpret it, but in terms of understanding jurisdiction, is it jurisdiction over the information, which may be here, is it jurisdiction over the person, who may be elsewhere? And how would that apply, both in sort of friendly and unfriendly countries, in terms of the scope of our responsibilities?

MR. BELLINGER: I'll take a stab at that. Let me say a couple of things. One, just to reiterate that the U.S. has in fact reaffirmed its position again that the ICCPR does not apply extra-territorially and the point that the individuals have to be under the power and control.

You know, I get sort of the novel suggestion that anybody who is subject to electronic surveillance is therefore under U.S. power and control. But I don't think that's actually a credible argument.

Even the Human Rights Committee I think

would not go so far as to say that if one can touch a foreign national through surveillance that that is someone who is under U.S. power and control.

The fact that the surveillance may be then collected ultimately inside the United States I think does not change the fact that the collection is being done of persons who are outside the United States. And so I think that does not change the, either the essential jurisdictional element that it does not apply extra-territorially outside the United States, and that those individuals are within the power and control of the United States.

Again, these are things that one might wish were so, and I'm not sure that there's as much of a disagreement between me and Laura Pitter as she suggests.

If one were writing a new treaty and could get people to agree to certain things one might agree that there might be, you know, policy limitations that one might accept.

But the way this particular treaty is written now, certainly the view of the United States government, and I frankly think I am not aware of any single government in the world, and I mean this is what I mean, governments who believe that their right to conduct electronic surveillance of people outside their territory is controlled by the ICCPR. I would be very surprised if we found any European government, as upset as they might be with electronic surveillance by the United States, who would say the Article 17 of the ICCPR limits our ability to collect outside our borders.

And in fact, the German government in a submission made to the European Court of Human Rights interpreting the European Convention on Human Rights argued that that convention did not limit its electronic surveillance of Uruguayans outside of Germany.

So again, the view of governments is that this does not have jurisdictional control over people who are outside their territory.

MR. MEDINE: I just wanted to follow up. What is the scenario where someone would be in our territory and not within our jurisdiction? Because the statute, the treaty says both territory and jurisdiction. Are there other situations where one would apply but not the other?

MR. BELLINGER: Well, certainly there would be people who would be, theoretically there could be people who are not in our territory and who could be subject to our jurisdiction. That was the problem that Eleanor Roosevelt was trying to solve at the time, to think about what the converse might create.

MR. MEDINE: Okay, thanks. Ms. Pitter.

MS. PITTER: Well, first of all, the German position was taken in 2008 before these revelations came forward and they've since sponsored a U.N. resolution which underscores the importance of respecting the right to privacy.

So I would say that, you know, Koh's interpretation is that there's on the one hand a

duty to ensure the rights in the covenant to those within a state's territory and jurisdiction, and then there's also a duty to respect the rights of individuals outside of the territory, the actual territory of the United States.

So there's the duty to respect is what's important here, and so there is an obligation under the ICCPR, even with the jurisdictional clause, to respect the rights to privacy of those outside the United States.

But this all, as you said, is happening in the United States. I mean the data is flowing through U.S. borders, although I'm not sure about the backbone upstream collection, where exactly that's taking place. So absolutely, yeah, absolutely, I mean I think that it would be the duty to respect the right to privacy is what's implicated here.

MR. MEDINE: Thank you. Judge Wald.

MS. WALD: I've got two questions I think for Mr. Bellinger. First is I think we recognize that the government has now reaffirmed

its earlier position about what the ICCPR means in relation to people abroad. But I wondered if you'd just say a word about how they dealt with the question of Article 31 of the Vienna Convention on the interpretation of treaties insofar as, as I remember it, you know, deference should be given to the official interpreters of the -- which in this case I believe, you know, have taken a much broader interpretation of that.

And I think a couple of our Supreme Court justices have said in several cases that when you're interpreting, when they're interpreting a treaty one should look to the interpretations, maybe for guidance, maybe not controlling, of other parties to the same treaty. Just a word or two on those two aspects of the reasoning which led to what is, is the reaffirmance of it.

MR. BELLINGER: Right, and I think what you're talking about is the General Comment 31 of the Human Rights Committee.

MS. WALD: Yeah, yeah.

MR. BELLINGER: Which certainly in the view of the United States, and again, I'm not aware of any government in the world who believes that the views of the Human Rights Committee actually are legally binding.

The Human Rights Committee was set up to monitor compliance and it makes statements which governments, including the United States, give respect to but we certainly don't, neither we nor other countries believe that that is the definitive interpretation of the treaty, nor do we believe that it's legally binding.

MS. WALD: Okay. My second question --

MS. PITTER: I was just going to add, sorry.

MS. WALD: Go ahead.

MS. PITTER: That it is, the Human Rights Committee is a very authoritative source regarding the interpretation of the covenant. And I mean the U.S. is under an obligation to give effect to the rights in the treaty in good faith. So what the Human Rights Committee has said in

that regard is very important.

MR. BELLINGER: And if I could just say, because these are important points right now, including for treaties, frankly the Human Rights Watch is extremely interested and having gotten through the senate the U.N. Convention on Disabilities.

So you know, Human Rights Watch can speak for itself, but certainly the view of the U.S. government and of most human rights organizations is that the statements made by these treaty compliance groups, while due great respect, are not binding on the United States.

If they were in fact considered to be binding on the United States, those would in fact fundamentally change U.S. obligations under the treaties and we would never get any treaties through the senate, including the treaty that both Laura and I would very much like to get through the senate, the U.N. Disabilities Convention.

MS. WALD: Okay. My second question very quickly is that acknowledging what

everybody's about, that this big debate in the international world will continue probably despite the most recent position we've taken, and given, you know, all of the people allied with it, the official interpreters, whatever they're called, Harold Koh, Sara Cleveland, Manfred Nowak, who's the U.N.'s leading expert on the ICCPR, my question to you deals with the last paragraph of your both oral and written testimony, and that is that you would see no problem with a policy which gave greater consideration to the rights of non-U.S. persons within the surveillance context, alluding to the fact that the President in his directive suggested that.

But I'm wondering if you, having served the position you did as counselor in the State Department, have any more specific ideas about in this context 701, or maybe even in other surveillance programs we could do just that?

MR. BELLINGER: Thank you, Judge. It is a great question. I have not actually given a lot of thought to that.

MS. WALD: Maybe a little.

MR. BELLINGER: My general sense from the surveillance that I saw was in fact that we are very targeted on specific intelligence requirements.

These are not broad dragnets of the surveillance of average individuals and so this is not a great violation of the rights of privacy of every single foreign national, that's very much focused on individuals who may pose a national security threat or for which the United States has a valid intelligence interest.

MS. WALD: Would you, for instance, think that taking national security, assuming you didn't have a national security risk, that basically non-U.S. persons we should try to approximate as much as we can within those restrictions the equal treatment in use, retention, that kind of thing of non-U.S. persons in our surveillance, or not?

MR. BELLINGER: I think that some of the things that the Obama administration,

President Obama has been focusing on to ensure that, particularly for the information that is collected, that we ensure that it is kept private.

I mean I would be personally, I haven't seen this happen, but I would be personally extremely concerned if we found that the United States had collected information about foreigners great or small, either a world leader or a lesser known person, and then we're not careful with that information and were to let it out. That would very much interfere with that individual's right to privacy.

I think, you know, as a national security official it's important for us to collect the information that we've collected, but we need to be extremely careful with it. So my sense is that as a policy matter these privacy concerns are important.

MR. MEDINE: Mr. Dempsey.

MR. DEMPSEY: My question I guess for Laura Pitter and maybe also for Mr. Sieber. Among the major, certainly the countries that Chris Wolf

looked at and cited, but among the other major democracies that do foreign intelligence surveillance, is there anyone that has a law which you would point to as a better model?

MR. SIEBER: Could you ask the question?

MR. MEDINE: Is there a country that has a better model of surveillance than ours? Is that --

MR. DEMPSEY: Yeah. In other words, what other country has a better model, a better law, more checks and balances, more controls, more limits?

MR. SIEBER: In general.

MR. MEDINE: In general, checks and controls balancing privacy and civil liberties and national security.

MR. SIEBER: It's a very broad question --

MR. DEMPSEY: Just pick one.

MR. SIEBER: Because you have to consider many, many aspects, not only the

extraterritorial implication. I just can give you some reliable differences a between the German system and the U.S. American, that's what I can witness on.

If you have a look at the German system you have to see that Germany has a very strong constitutional court and is very much attached to fundamental rights. This is a reaction to the Nazi cruelties and any steps towards this direction should be prevented. This is the reason for some very basic differences between the U.S. and Germany.

The first one, for example, is that intelligence agencies in Germany have no executive powers. So they cannot execute arrest warrants or anything like that. They just can collect the information. This is based on the idea that the lack of control which we have in this area of intelligence agencies must be balanced by lesser constrained measures.

Secondly, Germany has constitutionally founded strong separation of powers and separation

between the police and the intelligence agencies. This has been changed a little bit after 9/11 but still there is a fundamental separation.

Information exchange is only possible in a very limited way for very, very serious, serious crimes.

So I would say the differentiation between the institutions is stricter. We don't have multipurpose institutions like the FBI.

On the institutional side there is an absolute strong separation between these institutions, despite certain common datas and things which we have done after 9/11.

You could go further, if I compare it and look around at the control agencies which you have. In Germany it's separated. For internal surveillance we have a special commission appointed by the parliament, G-10 Commission who is doing the job. It's not called a court but the functions are similar.

And for foreign intelligence agency, the BND, there is a parliamentary commission who

does these things.

Maybe one last point, if you look at the aspect of protection of foreigners' rights and applicability of the constitution abroad, the German attitude is more in favor of applying the national constitutional guarantees.

With respect to the first question, which is foreign territoriality, section 1 of the basic law says that the basic law binds all public authority. And this is in general irrespective of whether it's in the country or outside the country.

There are differences of course, but they have more to do with the different circumstances, because the risks coming from abroad might be bigger than coming from within the countries, and for that reason I absolutely agree that the systems might be different for internal intelligence and external.

But it's not based on the fact that we do not apply the constitutional guarantees abroad, and it's definitely not based on the fact that we

are giving different rights to foreigners and to citizens, at least in this area of dignity rights, of human rights, and especially in the privacy rights.

So for example, there was a German decision of the court which was controlling intelligence gathering for abroad and which checked these systems.

So with respect to this question which we are dealing here, if I generalize it I would say we are more open to applying these fundamental rules. We do not reject it as it's not applicable. We don't go into these (inaudible) stay out of it. We would apply it, but then we have a proportionality principle and we check whether the things are justified.

And for example, in this decision I mentioned, the court said, yes, dangers coming from abroad are bigger, bigger dangers, and with balances and this law was in general justified with one exception.

It was applied also by law to internal

conflicts, and the constitutional court said it cannot apply just like that.

So I think these are the main interests which I could tell you. It's impossible to say better or worse. I would never, never do that.

MR. MEDINE: Thank you. Ms. Cook.

MR. DEMPSEY: We'll come back around.

MR. SIEBER: And if you permit afterwards I would like to say a few words with these International Convention 17, the applicability, but I don't want to --

MR. MEDINE: We'll come around at the end.

MS. COLLINS COOK: So I wanted to thank you all for coming and to congratulate you for being the panel that has come the farthest set of distances to participate today. I think it's very helpful to have this type of discussion in an open forum.

We've talked a fair amount today and all through the day about skepticism about U.S. law and U.S. practices. I think it's fair to say

there is also a high degree of skepticism about the contours -- let me get closer here.

I think it's fair to say that there's a high degree of -- if I can get through this question without hurting someone, this is really going to be my goal for the day.

(Laughter)

MS. COLLINS COOK: There's a high degree of skepticism about the contours and applicability of international law as well. So having experts who are able to speak to these issues is critical, I think, to us.

And I wanted to draw off of something, Professor Sieber, that you had mentioned and I have to confess it was not a focus of mine coming into today. I had been focused on the ICCPR and the potential applicability of Article 17.

But you talked about the interests of states, and if I understood what you said correctly, that the interest of a state in its own sovereignty is inviolate, that surveillance by one country in another country is a violation of that

sovereignty, there is no exception under customary international law that would make that any less of a violation of the state's sovereign status or rights.

So that's the academic point. That would lead me to think that no one was conducting surveillance on anyone else, that no country is doing surveillance.

But as a practical matter I think it's fair to say that every country is either engaging in foreign intelligence collection or attempting to engage in foreign intelligence collection.

So if you can explain to me how you can have a principle of customary international law, here the absence of an exception that is honored by not one country in the world, as I understand it.

MR. SIEBER: Yes, I remain with the saying that there is no permission of espionage under international law because the principle of self-defense, that needs an armed conflict for it. It's not there for the ordinary case.

And customary law would require an opinio juris, the conviction of the people that espionage is right.

But our estimations, that are split. If we are considering our own law, we say, yes, we do it and we give them a medal if they are successful. If we are considering the other, we say it's illegal.

So there are two regimes of law which come to different results. We live with that but we cannot say that international law has a general view that we can, that we can do it.

We have this problem in a very interesting case with the German reunification because when the two parts of Germany came together, there have been people doing espionage in East Germany and they are now under our jurisdiction.

This question came up and here again the Constitutional Court said there is no general violation of international law, and I think you agree with that. We have to live with this

conflict.

And in the global world that's normal. The world is getting so diverse that we have many conflicting regimes today now, so we can stand with that.

MS. COLLINS COOK: So I guess my question, perhaps Mr. Bellinger, you can speak to this, is it a violation of international law in terms of infringing the interests of another state to engage in sort of foreign surveillance?

MR. BELLINGER: I was going to jump on that as well. And the answer to that I think is clearly no. I am not aware of any country who believes that the U.N. Charter's statement on the protection of territorial integrity and sovereign equality of states actually prohibits electronic surveillance of another country.

Certainly if that were the understanding of our senate that in becoming party to the U.N. Charter that prohibited us from spying on another country because it would violate their sovereign equality or territorial integrity, then

we would get out of the U.N. Charter immediately. But I am not aware that any other country believes that as well.

So there is not, the principle of territorial integrity and sovereignty would apply to, say, for example, use of force. International law does not prohibit electronic surveillance or spying. Domestic law may.

And so that's really, you know, when we talk about international law, that basically means that there is a compact between countries. Judge Wald knows this very well, you know. Countries have to have agreed that they are not going to do these things to each other.

And in the U.N. Charter, the U.N. Charter was not saying we promise not to spy upon one another, we were saying we promise not to use force against one another.

U.S. surveillance in another country might violate the other country's law, but it is not a violation of international law.

MR. MEDINE: Let's go on to another

question. We'll give Ms. Brand a chance and then we'll come back.

MR. SIEBER: Because I think I have to contradict.

MS. BRAND: All right. Let's see if this microphone will work now.

Thank you all for being here today. One of the things I find frustrating about this discussion, not here specifically but in general is that there is a tendency to not distinguish between what is law and what is -- it's not working is it?

And what is either what people would like to be the law or what is a matter of policy.

And John, thank you for making that distinction very clearly in your remarks.

I was having a little bit of a harder time, Laura, following where you were moving from what you think is actually binding law to what is not.

And so I wanted to know if we are looking, setting aside policy, aspirational policy

for a moment, if we were trying to determine whether what the government is doing under 702 is legal, do you think there is some binding international law instrument that affects that questions?

MS. PITTER: Yes. I mean from my position it is a violation of Article 17 of the International Covenant on Civil and Political Rights. The United States does not recognize that, and that's part of the problem.

MS. BRAND: So let me just ask a question then. If the U.S. government doesn't recognize that, what is the body, what is the document, what is it that then makes that law binding on the U.S., on the agencies implementing 702?

MS. PITTER: It's the treaty itself. As Mr. Bellinger said, you know, a treaty is something that governments have agreed to abide by and to honor the commitments in the treaty in good faith.

MS. BRAND: And what is the body that

has the last say on the interpretation of the treaty, right? Because obviously the U.S. government interprets the treaty differently from the way you interpret the treaty.

Is there some other body besides the U.S. government itself whose interpretation of the treaty is then binding on the way the U.S. agencies implement it?

MS. PITTER: Well, the Human Rights Committee is one of the most authoritative sources on this, but --

MS. BRAND: But is it legally binding, right? That's my question, not is it persuasive, is it binding?

MS. PITTER: I mean from the opinion of many other governments it is. The treaty is binding upon them. The United States does not recognize the extraterritorial application of it.

MS. BRAND: And this is an honest question, give me an example of a country that views the ICCPR to have extraterritorial application with respect to surveillance of

foreigners abroad that itself that takes its own advice or heeds its own interpretation.

MS. PITTER: So this surveillance, as I said, is a novel issue. It's not something that's been addressed by the case law, and especially not since the revelations from Snowden which have disclosed, I think even to policy makers in many countries, the degree to which the law, the domestic law on the books is actually being applied, and the vastness of the programs, how much data is actually being collected.

So it's a novel interpretation, I mean it's a novel question, as it is in the United States --

MS. BRAND: I'm sorry to cut you off but we have a strict timekeeper here, the Chairman, and I want one last question.

I'm interested in your interpretation of what constitutes control and how being surveilled essentially would put someone within the control.

My concern about that interpretation in

part is that I'm not sure what meaning is left in the phrase, under its jurisdiction. If the statute talks about territory and jurisdiction, if jurisdiction means something in addition to territory, it seems like a meaningless phrase if it can include surveillance.

MS. PITTER: Well, it is meaningless in the sense that the United States has taken up, used the technology to conduct surveillance on a very mass scale. So it affects an enormous number of people.

The, you know, jurisdictional clause has been interpreted extra-territorially in the context of detention and torture, in which a smaller number of people have been affected. But when you're talking about surveillance --

MS. BRAND: But detention, I mean someone being detained or tortured is, I would say, much more clearly within the control of the government who has detained or is torturing them, right?

So my question is when you get into

surveillance and the person is clearly not within the physical custody of the government in question, what is it within the ambit of the treaty?

MS. PITTER: So you can look at it two ways there. You know, their communications are within the effective control of the government and so that's one way to look at the obligation.

But in addition, they have an obligation to ensure the rights within the covenant territorially, but also to respect the rights in the covenant extra-territorially.

So although they are not necessarily bound, you know, to enact legislation domestically regarding, you know -- well, they're not necessarily bound to ensure the rights of individuals with regards to privacy extra-territorially, they are bound to respect those rights extra-territorially.

MS. BRAND: I see my time is up.

MR. MEDINE: Mr. Garfield, in your statement earlier you indicated that the

revelations about the surveillance programs, particularly 702, has had significant international impact with regard to business dealings with U.S. firms, and you proposed a number of steps to ameliorate that, and I wanted to ask you about some of them.

And you also mentioned one of them, namely transparency in your remarks earlier. Do you have thoughts about what level of transparency would be helpful to companies, but taking into account national security concerns?

As you know, our first report on 215 did recommend greater transparency, but in terms of disclosures that a company can make about surveillance requests from the U.S. government, so long as that took into account national security.

And I guess in particular if you have comments on the agreement that was reached between the Department of Justice and a number of firms, whether that agreement goes far enough and provides sufficient detail to give comfort to business partners of those firms overseas.

MR. GARFIELD: Thank you for the question, first of all. The agreement with the Justice Department is viewed as a significant step forward. There are additional steps that can be taken that would be helpful as well.

One is the level of detail that the companies are able to share, including disaggregation of data between Section 215 and 702, or whether it's a national security letter. So a greater level of granularity would be helpful.

The second part of that is it is not only important that the companies be able to share out information but that the government share information as well and provide greater transparency, which is often lost in these discussions.

The debate that's been taking place today speaks to the importance of greater transparency because 702 already includes a number of protections that are not generally known, particularly internationally.

To Christopher Wolf's point, if they were more well-known it would be clearer the extent to which steps are being taken in the United States that are not necessarily being taken in other countries.

MR. MEDINE: And you also recommended, made a couple of other recommendations that you put forward were oversight, the importance of oversight and in discriminant collection.

And I guess the question is in the 702 program isn't there already oversight through the Foreign Intelligence Surveillance Court and some of the internal government processes?

And with regard to indiscriminate collection, I think as we heard earlier there has to be a foreign intelligence purpose, and so it's somewhat constrained. Do you think that with regard to this program it meets those requirements?

MR. GARFIELD: Correct. My recommendations there weren't intended to suggest that it in fact was indiscriminate. It was

suggested, it was a suggestion that taking steps to be clear about the protections that are in place and to the extent it is not, it is in fact not indiscriminate, to reaffirm that would be helpful as we go about doing our business internationally.

MR. MEDINE: And Mr. Wolf, you analyzed other country's laws and shown that they're not only not better but maybe not even as good as our laws by some criteria. What lessons should we draw from that in terms of how countries should conduct their surveillance programs?

MR. WOLF: So the purpose of our white paper and our research was really to be expository than to reach judgements and to pick winners and losers or to decide whose was better or best.

But we thought it was important in light of the claims that were being made, particularly by the cloud industry in Europe that there is national security access obviously that goes on in the EU and elsewhere around the world, and often without the controls and safeguards and

transparency that we have here.

So the overall conclusion that we reached is that this is a global problem. Obviously it's one that has been focused on intensively here in the United States because of the Snowden revelations, but it is an international issue that needs to be resolved internationally, particularly with the sharing that goes on among intelligence authorities.

It is heartening that the European Parliament in its resolution last week adopted the draft report that came out in January that focused on the European intelligence gathering practices.

We hope that the data protection authorities in Europe who've been vigorous critics of the NSA practices will comment on their own country's practices. They've been relatively silent on that, and we think the debate that has to be made should be among all those interested in privacy protection, and obviously that would include the privacy commissioners abroad.

MR. MEDINE: Obviously countries have a

lot of self-interest in conducting surveillance programs. Do you see a forum in which countries can or even should agree with the methods by which they conduct surveillance?

MR. WOLF: So that's well above my pay grade. I really don't have a view on that.

I do have, if I can just mention on the transparency point, we did a white paper in August that then general counsel of the Commerce Department Kerry cited in his speech at the German Marshall Fund that actually showed on a per capita basis access by national security and law enforcement on a per capita basis is larger outside the United States in many instances.

MR. MEDINE: Judge Wald.

MS. WALD: I have two questions for Ms. Pitter. Given what most or many observers concede are widely varying practices in different countries about surveilling their own and other country's citizens, would you advocate, as we sitting here have to make some observations, maybe recommendations on 702, would you advocate that we

unilaterally, we recommend unilaterally putting in place one and the same protections for non-U.S. person surveillance that we have for U.S. citizens? Or two, raising the non-U.S. citizen person protections to the level that the official bodies of these international organizations that we've talked about say they should be?

If you come out on the second, what specific criteria do we have to go on as to what those practices would be?

In other words, there's a slightly cynical end to the question, what would be the additional protections in real time to privacy interests of non-U.S. persons if the U.S. took a position that the ICCPR does apply to our activities outside territorial U.S., but that we've already met those standards, such as seems to be the case with some of the other countries who espouse the official broader interpretation of ICCPR but then go on their way, as Mr. Wolf suggested, and don't really raise those?

MS. PITTER: This is to me?

MS. WALD: Yes, this is to you.

MS. PITTER: So, I mean I think one clear change that needs to be made is the purpose of the surveillance needs to be much more targeted. The definition of foreign intelligence information is just much too broad. It encompasses, you know, things that, conversations that could be just about generally the foreign affairs of the United States.

And I know we heard in the panel testimony earlier that that is somewhat reined in by certifications but those are not public and we've not seen them.

There should be a lot more transparency in the law. I think the difference in the German law is that there is a lot more transparency. The capacity also is less in Germany. I mean the U.S. has vast capacity, so you know it affects a lot more people.

But definitely a more narrow, a more targeted approach, and applying, you know, necessary and proportionate principles to the

surveillance as well, I think would go a long way.

There's probably plenty of room for recommendations. I probably can't get into all of them here but that would be --

MS. WALD: In general would your standard be that there should be a presumption that we treat non-U.S. persons like U.S. persons in our surveillance activities, or rather that we go to the best practices we can pull from that people who endorse the ICCPR, even if we don't actually endorse that application?

MS. PITTER: So I think that there can be differences in the law itself but it has to, the differences have to be ones that don't impair the impact of the right itself.

So the right to privacy has to be part of, it has to be made part and parcel of the assurances, but they can be different for practical reasons when it comes to --

MS. WALD: Can you give us, in my remaining few seconds, some application of what you've just said to 702?

MS. PITTER: Well, I'd like to go into, you know, a more detailed analysis here but right now there's --

MS. WALD: Well, just quickly.

MS. PITTER: There's not a warrant requirement, for example, under 702 for individuals, but there should be -- it may be that it's not a practical requirement to have a warrant for individuals outside of the United States.

And it's not just individuals under 702, it's also facilities and about targeting as well.

But the procedures that are in place to protect against sort of suspicionless, you know, there's no standard for what authority has to find before it can target an individual. The main distinguishing principle is that it's a foreigner, and that that information is going to be acquired for foreign intelligence purpose, for foreign intelligence purpose, so that is too broad.

MS. WALD: Okay.

MS. PITTER: Does that make sense?

MS. WALD: Yes. All right, very quickly I guess, Mr. Wolf, your testimony, you know, recited the report about the lesser, basically the lesser protections most other countries including our close allies give to privacy, at least despite some of their countries adherence to the ICCPR's broader definition of privacy, yet you also note that the economic risks to U.S.-based telecommunication companies from threats both from competing companies inside those countries and from the governments themselves that they may balkanize and insist on collection and storage activities being conducted in-country poses a real risk.

Is it above your pay grade to give us some indication of what line or policies the U.S. should follow given those two competing concerns?

MR. WOLF: Well, I think our concern in doing the work that we did on the white paper was the misperception that was arising --

MS. WALD: Let's assume you've done those and that they are real, but also are real

the threats to the competitiveness of U.S. companies if foreign governments and peoples get very excited and want to keep everything inside their own countries.

MR. WOLF: So our position is that they're deceiving themselves if they think that when they keep data presumably within the four borders, four corners of their own country that it's safer from surveillance, not only from their own surveillance authorities, but of course through the sharing arrangements from surveillance authorities from elsewhere around the world, and that the Balkanization of data is not a useful global phenomenon at all.

MS. WALD: Well, what can the U.S., or what could we recommend they bring them together?

MR. MEDINE: Judge, your time has expired. Mr. Dempsey.

MS. WALD: Right. You can think about it.

(Laughter)

MR. DEMPSEY: On my last round we were

talking about what were, if any country's laws that did a better job here, and Mr. Garfield, you were ready to jump in. Do you remember what you wanted to jump in on? I wanted to give you a chance to make the point, if you still remember what it was.

MR. GARFIELD: It really was the point that was made in response, which is that in fact our experience in carrying out our business is that there aren't many, if any, other countries that have as many safeguards in place.

The lack of open discussion through multinational engagement as well as transparency here in the U.S. furthers that false perception that somehow other nations are doing more than we are. And that is certainly something that whether through legislation or recommendations from the PCLOB, we can do something about.

MR. DEMPSEY: The question for Laura Pitter, a couple of other witnesses have raised this and a couple of times I grabbed for the book in order to raise it and didn't get a chance to,

the definition of foreign intelligence, as I read it, it means information that relates to the ability of the United States to protect against actual or potential attack, grave hostile acts of a foreign power, sabotage, international terrorism, international proliferation of weapons of mass destruction, or clandestine intelligence activities. None of those are too broad, I would think.

And then it says, information with respect to a foreign power or foreign territory that relates to the conduct of the foreign affairs of the United States.

I mean isn't that precisely what foreign intelligence is supposed to be about, information with respect to what foreign countries are doing that might affect our foreign affairs? Why is that too broad?

MS. PITTER: I think that the first category of information that you said could, it would be permissible. But the general foreign affairs of the United States allows for the

collection of a vast amount of information that does not necessarily have any national security purpose.

MR. DEMPSEY: No, but it has foreign affairs purpose. It is by definition about the intent of foreign governments, and are you saying that other countries self-restrain themselves from trying to understand what their adversaries are doing, even in matters that don't involve attack and so on?

MS. PITTER: I mean if other country's laws are overbroad and vague then they're in violation of, you know, the International Covenant on Civil and Political Rights as well.

MR. DEMPSEY: Well, I think John would say that if everybody is doing it, it probably isn't a violation of the treaty. Everybody didn't bind themselves not to do what they all were doing at the time they bound themselves to the treaty.

MS. PITTER: Well, you know, the revelations about how this is applied are just coming out now and there are going to be

challenges and there already are challenges to the law.

And I think we're going to find that there is room certainly for reining in the overbroadness of some of the statutes as they exist right now.

I think that because it allows for the communications of things that don't necessarily have to do with national security, that it just, it's overbroad and it's impacting, you know, the United States in other ways.

MR. DEMPSEY: In what way is the collection of information about foreign affairs overbroad?

MS. PITTER: Because it could be, you know, someone talking about, you know, their opinions about the foreign affairs of the United States --

MR. DEMPSEY: Not someone talking about their opinions, it's the information with respect to a foreign power. So this is not Joe Schmoe in Germany saying I like or don't like the United

States, this is about what Germany thinks about the United States.

MS. PITTER: It merely has to relate to the foreign affairs of the United States --

MR. DEMPSEY: Yes.

MS. PITTER: In my opinion it's too broad. It allows in for much too broad a type of communication.

MR. DEMPSEY: No, I'll yield. I'd like to have another round, a third round if we could, but I'll yield for now.

MS. COLLINS COOK: Mr. Bellinger, I think you had put your finger up midway through that and I'd like to follow on this conversation as well because it struck me.

First, where would you draw the line? And I'm struggling to determine what precisely is impermissible about collecting foreign intelligence in the category of foreign affairs as set forth in FISA.

MR. BELLINGER: Yeah, so thanks for that question. And I think this is a very

important point, and Judge Wald started it and you have continued it.

We have to be really very clear about what international law is. International law is not principles that we think would be fine, policy principles that you and I might agree.

International law, if we are serious about international law, and this actually is the definition of international law, are things that nations agree to, to be bound by, by treaty or that is customary internationally, meaning that countries do it so often that everybody does it and they do it by a sense of binding legal obligation.

So two points here, and Judge Wald, I heard you say that while it is true that other countries actually take a broader definition of whether the ICCPR applies extra-territorially, I'm not aware of any country in the world that believes that the ICCPR actually binds them with respect to electronic surveillance, that that right to privacy in Article 17 actually limits

their ability to conduct electronic surveillance of foreign nationals. So that is just not a treaty obligation that countries have accepted, even under the ICCPR.

It might be something that human rights groups wish were the case, but it is not something that governments have accepted, and certainly not something the United States government has accepted.

And then just one more round on the Human Rights Committee. Again, the treaty itself does not say that the decisions of the Human Rights Committee, which is basically a group of academic experts, are binding. Governments who write treaties know how to write language.

For example, the U.N. Charter says that we undertake to comply with rulings of the ICJ. But the human rights monitoring groups, countries have not said that we undertake to comply with their decisions.

And in fact, the senate, and all of you know this, the senate would never agree to cede

responsibility for the future interpretation of a treaty to a group of academic experts. That would take completely out of the hands of the shared understanding between the executive and senate, the interpretation of a treaty.

So you know, the United States, and this is the view of the Obama administration as well, you know, recognizes that other people may not agree on the extraterritorial application of the ICCPR, but you know, no country believes that the ICCPR actually limits electronic surveillance.

MS. COLLINS COOK: So I just wanted to as a follow-up question to Ms. Pitter. Thank you. I know we've aimed a lot of our questions at you.

I think there's a sense within the United States government, a little bit of exasperation, the concern is that our surveillance lacks transparency or that we are somehow outside the mainstream of what other countries are doing.

And I look at 702 in particular and I see something where our legislative branch has specifically said exactly what our executive

branch can do. The executive branch, which is headed by democratically accountable individuals then oversees the execution of that authority, it is subject to the oversight of the judicial branch and it is subject to the oversight of our legislative branch.

So I guess my question is systemically what else could the United States be doing to help build the confidence and trust of other countries?

MS. PITTER: So the oversight so far has all been in secret. I think that's one problem. I mean even the first panel today said they were in the process of declassifying a large number of documents and they were looking at doing that because they recognize the importance of transparency.

The oversight has not, I mean if you look at what happened with 215, even --

MS. COLLINS COOK: I was talking about Section 702, which is the focus of our --

MS. PITTER: We don't know the details of the oversight regarding 702, so the only

information I have about oversight would be regarding 215. And we saw that the judicial oversight in that context, you know, would up, there was an opinion that had an impact on the vast number of communications of Americans that was kept secret from the Americans, so --

MS. COLLINS COOK: Well, let me push back a little bit on this notion that the oversight is not transparent.

So again, we have a statute that tells the world exactly what the executive branch must present to the judiciary, what findings the judiciary must make, what authority judiciary has vis-a-vis that application, and the framework for this surveillance.

We have a public statute that also tells you exactly what the executive branch is obligated to share with Congress. So where's the lack of transparency in that?

MS. PITTER: Well, the judicial oversight for the 702 program is annual. They look at just the procedures. They don't actually

look at the individual targeting requirements. That's done by an NSA analyst at his computer desk.

MS. COLLINS COOK: Actually I think if you were here for the first panel the testimony by the first panel was that that is not in fact the case, that it is an ongoing process of oversight. There are regular reporting requirements, both to the court and to the Congress, so.

MS. PITTER: I was, I did hear the first panel, and I believe he said that those targeting decisions by the analysts are reviewed eventually, but it's not something that's done at the beginning. So the --

MS. COLLINS COOK: So if there's not public review of specific targeting decisions, so this, the United States government saying we would like to collect foreign intelligence information about this specific selector, that's a lack of transparency that is problematic for you?

MS. PITTER: Well, the transparency, even the certifications that the FISC court gets,

there's no, they don't even see the identifiers or the selectors, they just approve the procedures. So you know, that's a problem with the oversight. In terms of --

MR. MEDINE: I'm going to let Ms. Brand pick up since we're at time. So thank you.

MS. BRAND: Okay. I guess maybe this question is directed at John but if anyone wants to jump in, that's fine.

If the ICCPR did have application to the U.S. government surveillance of non-U.S. persons abroad, setting aside the territorial issue for a minute, what does privacy mean in that context?

I have found the lack of a universally accepted definition of privacy very frustrating writ large across everything that we do, and I mean the same issue pertains here. So I guess is there a universally accepted definition of privacy? Is there a definition of privacy that is binding on the U.S. government? If not, how would we find, who would supply such a definition? If

you can sort of help us understand that.

MR. BELLINGER: Yeah, so that's a great question. And that's really the third prong. I mean the reason that the ICCPR doesn't apply is, one, there's the within its territory and subject to its jurisdiction. Then even if it were subject to our jurisdiction, then it has to be within the power and control.

And you know, no one is really going to legitimately argue that, as I think you said earlier, power and control in the view of those who take that interpretation of power and control is someone that you actually physically have in your custody, not electronic surveillance.

And then there's the issue, even if those applied, is something unlawful or arbitrary violation of privacy? And there are not definitions that are universally accepted.

You know, people can argue about these things but for it to be law that a country actually violates, there has to be an agreed definition on privacy and there has to be an

agreed definition on what is arbitrary, and there just are not those definitions.

You know, again, someone can say that someone has an absolute right not to have any country pry into anything that they're doing and that that's a violation of their privacy, but there's not an accepted definition of that.

I mean I could frankly imagine if one were to accept the first part of your premise, which is that it were to apply extra-territorially, and let's also say that it were someone within the U.S. jurisdiction, let's say someone, the United States is actually holding a terrorist in another country and we agreed that the ICCPR applied, we agreed the person was within our power and control, and then we were to do extensive interviews of that person about the person's private life, and then we just publish it willy-nilly, not as part of a criminal proceeding but essentially just as a leak, well, you know, there might be an argument that that might be an arbitrary intervention with that person's right to

privacy.

But I think that's -- there's not a definition of privacy, or of arbitrary, or unlawful that is binding as a matter of international law.

MS. BRAND: Chris or Laura, any thoughts on that question?

MS. PITTER: Would you repeat that question again?

MS. BRAND: Just what does privacy mean in the ICCPR context? Where does the definition come from? How would you find the definition?

MS. PITTER: Well, it guards against unlawful and arbitrary interference with an individual's privacy, so there has to be a respect for correspondence, for example, and a respect for an individual's personal space, and there has to be an ability to have personal space to communicate.

MS. BRAND: Where are you getting that definition?

MS. PITTER: Well, that's, I mean

that's coming from the interpretation of, the right to privacy is connected to freedom of expression, freedom of association. It impacts that. And you know, the right to correspondence comes from that as well. So I mean it's defined in the treaty itself, and --

MS. BRAND: What is the definition? Humor me.

MS. PITTER: I mean --

MS. BRAND: I can look it up, never mind. But it sounds like what you're giving me is sort of your sense of what privacy entails, not a sort of legally defined or legally articulated definition. Chris?

MR. WOLF: So a privacy lawyer's answer goes back to Brandeis and Warren who said the right to privacy is the right to be left alone. But they recognized and I think it's been recognized ever since, that was 1890, that there are exceptions for the good of society, for law and order, for social good.

And that's really where the rubber hits

the road. What are the permissible exceptions for national security surveillance? And you know, that's the discussion that needs to be had globally.

You know, Judge Wald asked what should the U.S. government do? I think it should promote that discussion as a global matter, and at the same time I think it should promote the decoupling of national security surveillance from cross-border data flows for commercial purposes.

The threat to withdraw safe harbor, for example, the declaration that the transatlantic trade and investment partnership shouldn't address data because of what happened with national security surveillance is a non sequitur.

Those issues need to be dealt with between governments, but that shouldn't interfere with cross-border data flows, which have to have privacy protections built-in, no question. But those are not something, that isn't something, the surveillance issue is not something that the companies themselves can really address and

they've done about as much as they can in pushing for transparency, pushing very hard.

MR. MEDINE: Dean, did you want to add something?

MR. GARFIELD: The question was asked earlier about what the appropriate venue is and I would say a reminder that the strategic and economic dialogue didn't exist beyond five years ago, and so this is one issue that's getting left behind in the discussion, the importance of creating a framework and a venue for greater multinational dialogue around the surveillance issue. And I think the PCLOB in its recommendations can have a dramatic effect in this area.

MR. SIEBER: It's clear that we have not an international definition because the countries are too different. However, in the countries and national law, and European law and in other legal bodies these definitions are emerging. And of course they have to develop.

What is sure is that there is a core

area of privacy where we all would agree that privacy is infringed. For example, if you directly do intelligence gathering on the sexual life of somebody who is not a suspect, there's no reason, that's a clear core area infringement of privacy.

Now if you go further, it's becoming of course a difficult, mass surveillance of people against which there is no suspicion would be one aspect where we'd have to investigate.

Another one is to create a complete picture of the private life of somebody going back to his birth, whatever did he do, did he demonstrate in school? So collecting enormous mass of data on one person would be another aspect, just illustrating. There are cases which fall under something like that.

And we should work on this definition and the fact that we do not have something like that would not lead me to the conclusion we shouldn't go in these things.

It's the same with this attitude on

extraterritorial application and things like that. These questions are so new that you cannot find any government's position here. So for me, that's not a valid argument. If you are pioneers on these questions, we cannot say the governments are not yet there.

I agree with you it's a political question on this issue.

One final point where I do not agree what was said is the question with respect to territoriality. If you are collecting data in a foreign country from (inaudible) it's clear that's legal. You are not infringing the foreign territory.

But if you go to a foreign territory and you switch on servers, you download countries -- the electronic pulses, you are changing and you do a function that usually the police does, this is a clear infringement of territoriality.

And you can see this especially in the cyber crime convention where we are fighting about these questions. We have Article 32 B with a big

struggle between the U.S. and Russia, which is bringing down the complete process of the cyber crime convention. We all agree that except these cases mentioned in Article 32 of the cyber crime convention ratified by the U.S., any police activities doing access to foreign countries are of course infringements of privacy. Nobody would claim that this is legal. We could stop the process of the cyber crime convention if your statement would be, all right, like that in this generality.

So I would say that we have to remain -- these surveillance activities do not in any case infringe territoriality but there are many cases, especially looking at the cyber crime convention, our agreements which we have on this committee, we all would say that's a clear infringement of the sovereign territoriality of a country. And it is also undisputed that the protection of territoriality is guaranteed, not only by Article 2 of the U.N. Charter, but also by customary law. It's one of the basic principles

since the Westphalia Peace Accord.

MR. MEDINE: Let's give John a chance to respond.

MR. BELLINGER: I'll be brief. On the second point, again I would say that I don't think any country in the world would say that the Article 2 of the U.N. Charter's protection of the territorial integrity and sovereignty of states would mean that they cannot conduct essentially espionage activities from anywhere. I just don't think that's what the U.N. Charter says.

But more importantly, the first thing you said really goes to the heart of our discussion here, where you said this is an evolving national dialogue about privacy and it is a dialogue that is going on nationally in different countries, and it therefore is going on internationally.

But the question at least that was put to several of us, to me and Laura in particular is, is there a binding international law standard right now? And the answer to that is clearly no.

Germany may have laws inside Germany, given its particular past. Other countries may have particular national laws. Sooner or later countries may get together and agree on things, but right now there is not an international legal standard, either in the ICCPR or anywhere else that limits electronic surveillance from the United States, or again, from any other country.

Other countries would not agree that there's not an international legal standard -- or that there is an international legal standard.

MR. MEDINE: We have time for just a quick round that Jim had requested. Let me just ask just to clarify one point, John, the treaty ICCPR is not self-executing. What does that mean and is there any forum in which enforcement action could take place?

MR. BELLINGER: That means that it would require implementing legislation for it to be, so it's binding as a matter of international law and we have implemented it already and are in compliance with it in certain ways because of laws

that we already had on our books, or might thereby have our Congress pass. But it does not have automatic legal effect merely by the United States becoming party to it.

MR. MEDINE: And is there any forum in the world where we could be held accountable for compliance with the ICCPR?

MR. BELLINGER: The U.N. Human Rights Committee monitors our compliance and comments upon things that we are doing. That's what happened last week when we presented our report. And the United States commented on or responded to these comments, but that's not judicially or legally enforceable.

MR. MEDINE: Thanks. Judge Wald.

MS. WALD: Just a quick comment. Am I not right, John, that not in this context of surveillance, but hasn't England at times relied in some of its judicial decisions on the ICCPR for the, to disallow, I think in dealing with some detainees or asylum people, etcetera?

So my impression was there are courts

who have actually relied upon the ICCPR, not in the surveillance context but in other contexts.

MR. BELLINGER: You and I would have to look at those together. It may have been the European Convention on Human Rights. There has been a fair amount of jurisprudence recently on the extent to which the European Convention on Human Rights creates obligations on British and European forces who actually do have someone within their control of their military outside of Britain, or Germany, or elsewhere.

MS. WALD: Okay. I'll let you off. Very quickly I have one question, quickly, for Mr. Garfield, and that is that the statement that your organization provided to us spoke of the need for meaningful oversight by an independent body in government as to the surveillance programs, including access to collected data.

Just wondered very quickly, who you had in mind, was it the IGs, us, FISA, Congress? Did you have particular independent bodies who would provide the meaningful insight, which included in

your statement oversight of collected, access to the collected data?

MR. GARFIELD: We did not.

MS. WALD: Okay, that's a succinct answer.

MR. MEDINE: Gives you a concise answer.

MR. DEMPSEY: Rather than a question I'll just offer an invitation, which is if any of the witnesses could provide us with guidance on the question I posed, what would be a better way of structuring a foreign intelligence system.

I think at the end of the day any concept of law, any set of rules is going to recognize that different countries are going to have somewhat different structures. So the German structure is robust but different from the United States. The United States believes it has a robust system with different elements than Germany has, etcetera.

Has anybody put together or could anybody put together a list of the elements of a

system and then some sense of how you come up with what is the minimum?

We talked a lot about judicial oversight but Germany does not have. The court reviews the statutory structure but not the individual implementation, does not do individual targeting on the strategic surveillance in Germany. In the U.K. it's all administerial, not judicial.

Secondly, if any further thoughts on how we get from here to there. So several witnesses have said it's an evolving situation. We have new questions, questions which to my view are not answered in the existing documents. Let's just say that it's not answered. They don't apply. No one thought about this. It hasn't been answered. How do we move forward, we, the world, or maybe the U.S. and Europe, which have more shared values than we sometimes admit, how do we move forward in getting that kind of commitment?

And the industry in Garfield's paper is that a global, I think implicitly recognizes we

need global understanding, even if not all of the laws are the same.

So any thoughts that you can offer us. Not right now because we want to move along, but any further follow-up thoughts you could offer us in writing, please, it would be very helpful on both of those points.

MS. COLLINS COOK: I just wanted to thank you all for coming. As I said at the beginning I think it's important to have these discussions. I won't assign homework or request any follow-up, but it's an education process for us, as well as for the American people, particularly on these issues.

So if there is information you think should be a part of the public record, which will remain open, I'm sure David will explain, it is welcomed.

MS. BRAND: I won't take up anymore of your time since we are at the end of our schedule here. But I want to thank all of you for coming. It was very helpful to me, so thank you for taking

the time to prepare and to be here.

MR. MEDINE: Thanks again to all the speakers and the Board staff that made this hearing possible. The Board's activities for today are now complete.

The Board encourages all those who are interested to submit, panelists and members of the public, to submit written comments on this topic at our website of www.regulations.gov. And the deadline for submitting comments is March 28th. All comments submitted will be available for review by the public. A transcript of today's hearing will be posted on PCLOB.gov.

And I will now move to adjourn the hearing. All in favor of adjourning the hearing please say aye.

(Aye)

MR. MEDINE: Upon receiving unanimous consent to adjourn, we will now adjourn. The time is 3:40. Thank you.

(Whereupon, at 3:40 p.m., the hearing was adjourned.)

CERTIFICATION

I, LYNNE LIVINGSTON, A Notary Public of the State of Maryland, Baltimore County, do hereby certify that the proceedings contained herein were recorded by me stenographically; that this transcript is a true record of the proceedings.

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 10, 2014