PRIVACY & CIVIL LIBERTIES

OVERSIGHT BOARD

- - -

PUBLIC MEETING ON

EXECUTIVE ORDER 12333

- - -

May 13, 2015

- - -

Transcript of the Privacy & Civil Liberties Oversight Board's public meeting on Executive Order 12333 held at the National Constitution Center, F.M. Kirby Auditorium, 525 Arch Street, Philadelphia, Pennsylvania, commencing at 10:30 a.m. on the above date, before Loretta J. Clark, a Professional Shorthand Reporter and a Commissioner of the Commonwealth of Pennsylvania.

A P P E A R A N C E S:

BOARD MEMBERS:

David Medine, Chairman
Rachel Brand
Elisebeth Collins
James Dempsey
Patricia Wald

PANELISTS:

Session 1:

Robert Chesney
Aziz Huq
Deborah Pearlstein
Stephen Slick

Session 2:

Orin Kerr
Katherine Strandburg
Stephen Vladeck

Session 3:

Michael Allen
Timothy Edgar
Mieke Eoyang
Matthew Olsen

- - -

P R O C E E D I N G S

- - -

MR. ROSEN: Ladies and gentlemen, welcome to the National Constitution Center. I'm Jeffrey Rosen, the president of this wonderful institution. We're so glad that you were able to make it here in light of the terrible train accident that occurred last night and our thoughts and prayers are with the victims and their families.

Let me say just a brief word about the National Constitution Center and how thrilled and honored we are to host this meeting of the Privacy and Civil Liberties Oversight Board. The National Constitution Center is a very unique and wonderful institution. We are a private nonprofit but we have a Congressional charter to disseminate information about the U.S. Constitution on a nonpartisan basis and we are the only place in these polarized times that can bring together people of very different perspectives to debate, celebrate and learn about the U.S.

Constitution. We do that as the Museum of We, the People here in this beautiful building on Independence Mall in Philadelphia where we have rare copies of the Declaration of Independence, the Constitution and one of the 12 original copies of the Bill of Rights and I hope all of you will go see it during the breaks of this great panel.

But we're also America's Town Hall and a Center for Civic Education and we sponsor debates and pod casts and symposia about Constitutional issues on every media platform. I've just come from Boston, where we had a wonderful debate co-hosted by the Federalist Society and the American Constitution Society about the Citizens United decision. And during this meeting I'm going to enlist some members of this great body to have a pod cast discussion as well. So, this is the place to come and hear the best arguments on all sides of Constitutional issues so that you can make up your own minds. That is why it is so appropriate and fitting that we have the honor of hosting this meeting of the Privacy

and Civil Liberties Board.

I want to read from PCLOB's great charter as well. The Privacy and Civil Liberties Board is an independent bipartisan agency within the Executive Branch established by the implementing recommendations of the 9/11 Commission Act and it has two primary responsibilities -- to analyze and review actions the Executive Branch takes to protect the nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties. And second, to ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations and policies related to efforts to protect the nation against terrorism.

That is why it is so appropriate that the Privacy and Civil Liberties Oversight Board's consideration of constitutional issues related to Executive Order 12333 is held here at the National Constitution Center. You are going to hear about separation of powers, First Amendment issues and Fourth Amendment issues

and there could not be a more appropriate place for this important discussion that you are about to hear.

And with that, it's my great honor to introduce my friend and the great leader of the Privacy and Civil Liberties Oversight Board, David Medine. David, welcome.

MR. MEDINE: Thank you, Jeff, and thank you for hosting us at this perfect place for holding this meeting. On behalf of the Board, our thoughts go out to the victims of the train accident yesterday and their families and hope everyone recovers as quickly as possible.

Good morning and welcome. This is a public meeting of the Privacy and Civil Liberties Oversight Board, in which we will be addressing Executive Order 12333 and the foreign intelligence activities that are conducted under it. It is 10:35 a.m. on May 13, 2015 and we're meeting in the F.M. Kirby Auditorium at the National Constitution Center in Philadelphia, Pennsylvania. This meeting was announced in the Federal Register on April

29, 2015 and 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, James Dempsey and Patricia Wald. I now call the meeting to order. All in favor of opening the meeting please say aye.

VOICES: Aye.

MR. MEDINE: Upon receiving unanimous consent, we will now proceed. We're meeting today to examine the history, Constitutional implications and practice of intelligence that ae conducted under Executive Order 12333 as part of the Privacy and Civil Liberties Oversight Board's oversight function. Executive Order 12333 has governed the intelligence activities of the United States since it was issued by President Reagan in 1981.

The purpose of today's event is twofold: To inform the Board as we conduct our oversight work and to inform the public about our activities and about some of the questions

raised by Executive Order 12333 with respect to privacy and civil liberties. Oversight of counterterrorism activities conducted under E.O. 12333 presents some new challenges.

First, our earlier reports on Section 215 and 702 examined discreet individual surveillance programs governed by specific rules that were unique to those programs. But E.O. 12333 does not provide the authority for any one intelligence gathering program. Instead the Executive Order is a high level delegation of authority from the President to 17 agencies and offices that make up the United States intelligence community. The Executive Order provides direction on which intelligence community elements are supposed to conduct which activities and it sets the ground rules for activities that have a United States person A fact, a category that includes citizens and legal permanent residents.

In essence, Executive Order 12333 establishes the overarching framework under which the entire intelligence community operates and it provides broad rules under

which individual intelligence activities are developed and conducted. For oversight bodies like PCLOB, this raises the question of how to learn about and understand the wide range of counterterrorism activities under Executive Order 2333 in order to focus oversight efforts on those activities that may have the greatest impact on privacy and civil liberties.

Second, individual activities conducted under E.O. 12333 are authorized and reviewed in a manner different from activities undertaken pursuant to statutory authorization such as the way the 702 program operates under the Foreign Intelligence Surveillance Act. Instead, these activities are developed within the Executive Branch by intelligence agencies that conduct them. This raises questions about how these intelligence activities are initiated and vetted. Who proposes these activities? Who approves them? Who evaluates their effect on privacy and civil liberties? Who monitors how they're conducted?

Third, the Section 215 and 702 surveillance programs that the Board previously

examined are both conducted here at home in the United States. By contrast, E.O. 12333 governs intelligence activities conducted anywhere in the world and many of those activities take place outside the United States. When E.O. 12333 was issued over three decades ago, the global communications landscape was quite different than it is today. Widespread use of the internet, e-mail, cell phones, smart devices and social media had not yet developed nor had the capacity that we have available today for large scale digital processing analysis of data.

This raises the question of how technological revolutions that have occurred over the past three decades have effected E.O. 12333 intelligence activities from a Constitutional perspective and from a policy perspective. In the global digital age, information or communications acquired in a foreign country may be more likely than ever to involve those in the United States. Should the rules governing overseas collection change to reflect this new reality? And if so, how?

Finally, intelligence activities that are conducted under the Foreign Intelligence Surveillance Act are subject to oversight by the court that approves those activities, the FISA court. This means that a second branch of government plays a role in reviewing the Executive Branch's intelligence activities. And FISA surveillance is specifically authorized by Federal legislation, it's subject to oversight from Congress as well, thus bringing three branches of government into the picture.

By contrast, courts play no role in E.O. 12333 activities. They do not approve those activities, review them or oversee them. And while the Congress has oversight responsibility with respect to E.O. 12333 activities, primarily in the form of oversight from the House and Senate Intelligence Committees, it's unclear how closely Congress has traditionally reviewed these activities. This raises questions about the oversight measures that take place exclusively within the Executive Branch and not Congress and the

courts and how they protect privacy and civil liberties of U.S. persons. And a necessary part of that inquiry is the question of how big Congress' role is even allowed to be under the Constitution under the Separation of Powers Doctrine.

Another important question is what constraints the First and Fourth Amendments impose on the exercise of presidential power in this area. Now to examine these difficult questions, the Board has brought together a wide range of outstanding experts today to discuss three topics. We will have panels on -- and of course, it's fitting as Jeff said that we're here at the Constitution Center to discuss those topics.

The first panel will address separation of powers raised by E.O. 12333 as well as the history of the Executive Order. After lunch our second panel will consider First and Fourth Amendment implications of E.O. 12333 activities. And our final panel will focus on E.O. 12333 in practice, including

oversight mechanisms.

Thank you. With that, I turn it to Rachel Brand.

MS. BRAND: Thank you, Mr. Chairman. I should turn on my mike. Thank you and thank you to the Constitution Center for hosting us here. It's good to be back on this stage. I'm going to be very brief in my opening remarks. I'd first like to thank our witnesses for being here, especially considering the very unfortunate circumstances of last night and this morning. I'm glad you could make it. I look forward to hearing your presentations, and I look forward to the opportunity to ask questions. And if I should do something different with my mike, please let me know. Is it working? Okay. Thank you.

When we announced last year that we intended to review Executive Order 12333, we didn't articulate any limits on that review. We mistakenly, I think, gave some in the public and the agencies the impression that we planned to review every aspect of E.O. 12333 and its implementation. This may have exacerbated a

common misimpression that E.O. 12333 is a discrete intelligence program. But, of course, as David said, it is not. It is a document that first outlines a construct for all the intelligence community's activities, assigning particular roles to particular agencies, and also imposes a number of privacy focused limitations on those agencies' actions.

Reviewing every activity conducted under 12333 would be impossible for us to do as a practical matter and would go far beyond our statutory mandate of counterterrorism. Fortunately, we have since clarified that we intend to limit our inquiry into 12333 to selected individual programs that fall within our statutory jurisdiction. So, with all of that in mind and in light of the many public misimpressions about 12333, I'd ask the witnesses today to be precise in identifying what you are talking about. If you are talking about a particular aspect of 12333 or its implementation, please say so. And I may ask you questions along those lines to help me better understand your testimony. So thank

you again for being here.

MS. COLLINS: I'd like to first welcome and thank our panelists, who I know are all busy folks and the logistics were particularly challenging today. Second, I want to thank the staff of the PCLOB. We are small but mighty. The dedication of the staff allows us to put together really tremendous events like this, so I thank them for that. And finally, I want to thank the Constitution Center and our hosts here today.

For an intelligence oversight body such as ours, understanding the history, parameters and contours of Executive Order 12333 is a necessity. As you can see from the titles of the three panels we have planned for today, Executive Order 12333 touches upon a broad range of issues, including and especially suited to our setting today, the balance and separation of Constitutional powers. But the practical questions about the operation of government programs and the oversight mechanisms that are designed to ensure that these programs stay within bounds set by

controlling statutes, regulations and policies are equally important.

Like other policy directives or orders issued by past and current presidents, E.O. 12333 is a product of the legal, political and historical events that preceded its existence. But as of today, the Executive Order has been utilized by numerous presidents to organize and divide responsibility amongst the components of America's intelligence infrastructure. This order also limits the government's foreign intelligence activities and restricts the intelligence community's use and dissemination of U.S. person information.

To the extent that I am aware, the United States is unique in having such an intelligence policy framework that expressly recognizes the privacy interests of its citizens in matters of national security. I hope that the discussion we have today and the considerable knowledge and expertise of our panelists will aid the Board as it begins to review specific counterterrorism activities governed by the Executive Order. I also hope

this event will help to correct and demystify much of the popular discussion surrounding this misunderstood and oftentimes mischaracterized order.

MR. DEMPSEY: Good morning. I'd like to thank Jeff Rosen for hosting us and the National Constitution Center for generously hosting us today, all the panelists for sharing their expertise on these timely and important questions and the PCLOB staff for planning our agenda today. Actually, speaking of staff, I managed to get on the stage here without a pen, so if someone could give me a pen, I'd be grateful. Thank you.

For me, the consideration of Executive Order 12333 is dominated by the technological realities that drive legal and policy debates in so many spheres today. The route that evolution of technology since the advent of the internet has fundamentally changed the way we communicate, keep records, do business. These changes are forcing every organization that deals with data, which is virtually every organization, public and

private, to develop and update rules for collecting and using data. The challenges of the digital age are acute for U.S. intelligence agencies, which handle huge volumes of data and must of necessity do much of their work in secret.

So, I'm particularly interested in how we can move forward to design rules that are suited to the current threat and technology environment in which the intelligence agencies operate are as transparent as possible and are coherent and consistent, starting with the Constitution at the top of the pyramid down through Executive Orders and Attorney General guidelines to the very detailed guidance that must be given to collection targeters and analysts.

The Board has already expressed its concern that some of the Attorney General guidelines in the middle of the protocol stack are seriously outdated and some cases predating the internet. I hope that today's meeting will help to better inform both the Board and the public about the origins of Executive Order

12333 in the context of debates about separation of powers and oversight, about how changes in technology and surveillance capabilities are challenging, if not leaving behind the traditional rules and understandings, and finally, how we can design 21st century legal rules and oversight systems that respond to the realities of 21sst century technology.

So again, thank you to all who had a role in this. I look forward to all the panels.

MS. WALD: I, too, look forward to this forum as an opportunity for PCLOB to learn from experts in law, technology and intelligence policy as we embark on what may be the most ambitious of our inquiries thus far. Executive Order 12333 is not, I believe, well understood outside of the intelligence community. The operations it authorizes are conducted in great part outside of the United States, a great many of them are classified and, except for Congressional oversight, not subject to any regularized independent review

outside the Executive.

Our inquiry is designed to clarify the scope of E.O. 12333, the limitations that are contained in it and in the regulations of the several departments which conduct operations under its ambit and the ways in which the Executive Order activities may affect Americans. We begin modestly by looking deeply at two projects conducted pursuant to its authority. That approach, however, must take appropriate account of the broader legal and Constitutional framework in which all intelligence operations must be conducted. And it is in that realm that we are hopeful and confident that our speakers today will inform our future activities.

We are thankful to Jeff Rosen, the National Constitution Center, the panelists today and to our able staff for doing the backstage logistical work that undergirds this kind of important intellectual exchange.

I do have one other point to make briefly. Our panelists today deal with the Constitutional framework of separation of

powers as it may affect Executive Order 12333, the First and Fourth Amendments and their implications for such activities, especially as new technologies for conducting surveillance emerge with relentless certainty and, finally, the real world considerations of the intelligence community and Congress, in which E.O. 12333 operates.

In my view, the focus of all three panels is essential to our work. It has sometimes been suggested that PCLOB should stick to policy analysis and leave legal and Constitutional issues to the courts and Congress. My experience, both inside the judicial branch and at PCLOB, convinces me that that should not and can not be. Because we are a government of laws and PCLOB specifically operates under statutory mandate to assure that laws are implemented in a way that appropriately balances privacy and national security and counterterrorism programs, we must understand and examine the legal and Constitutional framework within which the intelligence community operates.

I cannot candidly think how we could conscientiously pursue policy analysis outside of that framework. So, our friends in the legal academy, those who have worked in the intelligence community and in Congress have valuable and often different perspectives on these issues and we're very grateful to them for sharing those views with us and the public today.

MS. COLLINS: Thank you, David. So, again, welcome and the hour is nigh we finish what we need to be doing and now we get to actually listen to the experts. So, thank you, guys for joining us today. This first panel will examine the legal, historical and policy considerations that led to the development and implementation of Executive Order 12333 as well as Constitutional separation of powers issues implicated by its implementation.

Each of our distinguished panelists will have five to seven minutes of opening remarks. Rebecca, I believe, if you could, here we go -- will hold up a yellow card

to let the panelists know that two minutes remain. And once the first panelist's time is up, I will introduce the next speaker. When all the speakers have given opening comments, each Board member will have ten minutes to ask questions and I understand we will be subject also to the yellow flag rule. All right.

So, turning to our first panelist, Robert Chesney is the Charles I. Francis Professor in Law and the Associate Dean for Academic Affairs at the University of Texas Law School -- School of Law -- excuse me. In addition, he is the Director of the Robert S. Strauss Center for International Security and Law, a university wide research unit bridging across disciplines to improve understanding of international security issues. So, if you could kick us off.

MR. CHESNEY: Thank you. Chairman Medine and members of the Board, I appreciate the opportunity to appear before you today. I will use my time to help frame our discussion of 12333 foreign intelligence collection and the Constitution separation of

powers. Mindful that your charge is specific to counterterrorism, but at the high level of generality I plan to talk about, I'm not going to be very specifically focused on that constraint in these remarks.

I want to start within the central point and that is that foreign intelligence collection raises two distinct types of separation of powers questions and it's critical that we be clear in distinguishing those two and avoid confuting them. One concerns the power of the President considered in isolation. That is, does the President have inherent Constitutional authority to collect foreign intelligence without need of a statutory grant of power to do so? A distinct second question concerns the power of Congress in relation to that of the President. That is, would it be Constitutional for Congress to legislate various kinds of constraints on the collection of foreign intelligence information?

I'll talk about these in that order. First, does the President have inherent

Constitutional authority to collect foreign intelligence information? I believe this is an easy question that the answer is yes. It's true that the text of Article Two does not specifically address the point, but the case for inherent collection authority is nonetheless overwhelming. It flows from the President's role as Commander in Chief, as the sole organ of United States in foreign affairs, as the Supreme Court put it in Curtis Wright, and as the officer vested with the executive power. Functionally, the President's comparative institutional competence advantages with respect to secrecy, dispatch and energy all favored this conclusion, and most notably, the course of actual practice over time strongly favors this conclusion.

For nearly two centuries the Executive Branch in various forms of foreign intelligence collection with little, if any, hint of statutory authorization beyond the provision of generalized funding. Diplomats performed the function, private representatives of the President performed the function,

Army/Navy performed the function, eventually including signals intelligence of an electronic variety. Things changed only slightly with the National Security Act of 1947 with its brief references, affirmative references, to collection. But absolutely no one thought at the time that what the National Security Act was accomplishing was a grant of a novel heretofore unavailable form of authority for the Executive Branch to use.

Simply put, the course of practice throughout our history establishes that the President has this authority as an inherent matter. Of course, it also follows that all things being equal, the President, in using this authority, is at liberty to adopt the rules he sees fit with respect to which subordinate Executive Branch entities or officials shall have which particular sub-functions under the general collection domain and, likewise, if the President wishes to impose substantive constraints on those entities and individuals. This is what 12333 and its predecessor Executive Orders do. It's

a manifestation of the President exercising these Article Two functions.

But this isn't really the interesting question. The interesting question isn't whether the President, all things being equal and in the absence of legislation, has these sorts of authorities. The interesting question is the second one I mentioned at the outset. What constraints, if any, are Constitutional for Congress to impose on the exercise of this function? Another way to frame that is whether the President's Article Two authorities are to any extent preclusive of statutory regulation. This is a much trickier, more fraught question, more nuanced question and I don't believe it allows for a one-size-fits-all answer in one direction or the other.

I think that the most useful thing I can do at this point is to identify some of the variables that help distinguish different types of existing or potential constraints in this area. For example, one variable concerns the nature of the potential

constraint. Is Congress attempting to manage or control the internal Executive Branch decision making process related to collection? For example, with a requirement that certain officials or entities have a voice in decisions to collect in certain ways. Is it instead an attempt to compel the sharing of information with Congress? Or is it instead a substantive prohibition of some kind, perhaps barring collection on certain topics or in certain places or for certain reasons?

Another potentially relevant variable concerns the nature of the Article One authority that Congress might be employing. Is Congress exercising the spending power where its capacity to regulate indirectly is arguably at its maximum? Or is it instead a stand alone regulatory measure that might be said to depend on, say, the necessary and proper cause in some fashion or perhaps the power of Congress to make rules for the Armed Forces?

And critically, we might also consider whether the legislation that either exists that we might consider or might

hypothetically exist pertains to a Constitutionally protected right, particularly the First and Fourth Amendments. Now, there's no doubt we can expand on this list, highlighting potentially relevant variables, but I think this is enough to illustrate my point that the nature of potential legislative constraints can very widely and that, in turn, can greatly complicate the Constitutional separation of powers analysis, particularly insofar as in this realm the course of practice over time may loom very large. We have the example of some forms of legislative regulation already. We have procedural regulations and information sharing regulations.

In the covert action sphere we have the Hughes Ryan Amendments and, of course, we have FISA for collection of a certain kind with Fourth Amendment equally strongly implicated, both from the 1970's. And in those cases, whatever arguments might have been made in the 1970's -- and certainly some arguments were made challenging the constitutionality -- the course of the practice of the Executive

Branch acquiescing in these measures over time weighs heavily in the balance today and that, in turn, helps to bolster the case for similar measures in the future.

Where the same variables are not present, it's not nearly as clear. Now, I won't go so far as to suggest that we can draw a clear line here. I think any amount of time spent thinking about separation of powers in the foreign affairs and national defense realm teaches you quickly that although we often talk in terms of bright lines, it's very hard to actually draw them. And so, I would instead simply suggest that consideration of these sorts of factors can be a useful guide in making claims -- not so much about what is clearly constitutional or clearly unconstitutional, but rather that which is going to be relatively troubling and problematic and that which will be relatively acceptable and likely to prove constitutional on close inspection.

And my time having expired, I'll end there and I look forward to your questions.

MS. COLLINS: Perfectly timed. A great way to start us off. Thank you. Deborah Pearlstein is an Assistant Professor of Law at the Benjamin N. Cardozo School of Law. Her research focuses on national security law and the separation of powers. Previously, Professor Pearlstein served as the founding Director of the law and security program at Human Rights First.

MS. PEARLSTEIN: Thank you. Thank you very much to the Board and Chairman Medine for the opportunity to testify on 12333 today. As you know, 12333 establishes procedures for, among other things, the bulk collection of human and technical foreign intelligence information outside U.S. borders. While 12333 prohibits directly targeting U.S. persons for collection, it expressly contemplates, as the administration has acknowledged, that an unidentifiably large quantity of Americans' electronic communications may be incidentally captured through the process of bulk data collection.

Because other witnesses will

address the constitutionality of this collection and the adequacy of associated minimization procedures under the First and Fourth Amendments, it was here on the separation of powers significance of this particular practice. The President has maintained the power to engage in bulk data collection like this flows neither from 12333 nor from any necessary Congressional authority, but, as Bobby tells us, from the President's constitutional authority to conduct U.S. foreign relations and to fulfill his constitutional responsibilities as Commander in Chief and Chief Executive.

What does the Constitution's commitment to the separation of powers tell us about the wisdom of the 12333 scheme? I'd like to make four brief points. First, in the service of his duty to act in defense of the nation, the President no doubt has some inherent Article Two authority to engage in electronic surveillance to obtain information, particularly about those who plot unlawful acts against the government, as the Supreme Court

has recognized. But as the Court has also repeatedly reminded us, no governmental power is unlimited. The conclusion that the President's power in this context, as all others, must be limited flows from the enumerated structure of the Constitution itself, from the existence of external limits on executive power in the Bill of Rights and elsewhere and from the reality that Congress is also given a substantial role in national security affairs. Congress has the power not only, for example, to define and punish offenses against nations and make rules governing the regulation of our Armed Forces, and also, of course, the spending power, but to regulate commerce with foreign nations and among the several states.

Telecommunications and the internet are today channels of commerce in just the same way waterways were in the 19th century and there is no serious dispute that Congress can make rules regarding their use by commercial and domestic governmental actors. Indeed, as I believe this administration

agrees, when Congress legislates in the field of surveillance, that legislation controls executive operations, at least so long as it doesn't fundamentally impair inherent or what Bobby calls preclusive executive authority -- that is, this preclusive core of power that not even Congress can regulate to engage in foreign intelligence surveillance.

So, what is the scope of that inherent preclusive Congressional authorization or prohibition to the existence of a systematic unbroken executive practice long pursued to the knowledge of Congress and never before questioned that might be treated as a gloss on the executive power. This is the Supreme Court's words. But while presidents have long engaged in foreign intelligence collection in retail in this individual targeted way, never in human history has there been the kind of computing power required to engage in the kind of wholesale collection and subsequent searching the executive undertakes today.

Worse, as multiple actors have suggested, executive practice under 12333 was

and remains little understood even to members of Congress. When some of its contours were revealed, legislative questioning seems to have begun in earnest. More, Congress has in a closely related context in FISA, of course, regulated to constrain executive authority and foreign intelligence surveillance for nearly 40 years, primarily by the executive unchallenged years. History in this sense offers little basis for recognizing the breadth of preclusive power asserted here.

Third point: The functional interests that the allocation of power between the branches was designed to advance -- first and foremost, protecting individual liberty, but also promoting political accountability and facilitating effective government remain indisputably salient today as a matter of policy and constitutional law. But substantial questions exist as to the success of 12333 by any of these metrics. The activities regulated by 12333 generally avoid the structure of multi branch participation the Constitution presumes is best suited to protecting individual rights.

For example, here executive agencies make the rules, the Attorney General approves them, agencies then implement them with no legislative authorization or other politically transparent rule making process in the first instance and no judicial review or other rigorous independent check after the fact.

It's not that liberty and accountability interests can never be protected in an intrabranch scheme. Many administrative agencies protect rights and ensure their operations are politically accountable through substitute mechanisms. Notice and comment rule making is one of many examples. But 12333 offers little in the way of alternative processes to correct for the absence of multi branch participation. Indeed, executive rule making processes relating to any military or foreign affairs function remain broadly exempted from the Administrative Procedure Act requirements governing rule making otherwise. Collecting massive amounts of data is one of the most potentially intrusive things a government can do. It is also in this context

the least subject to independent checks.

Finally, what of the need for effectiveness in government, equally one of Hamilton's interests in structuring each branch of government to feature different institutional competencies. While Hamilton's notion retained substantial influence, the unitary executive is the most competent branch in security matters, given its characteristic advantages of secrecy and dispatch, here it's useful to recall the lessons organization theorists have taught us since Hamilton's time. Namely, that unitary secretive structures have significant and predictable disadvantages as well.

Political scientists, sociologists and others have studied elements of structural design to identify how organizations best manage, for example, chronic or acute kinds of risks. They found insular institutional cultures, career incentives in professional norms, all these can be advantages but can also contribute to disincentives, to adaptation and self-correction, features

essential for the maintenance of effective intelligence collection in the face of rapidly changing technology.

That there had been no comprehensive revision to 12333 guidelines to protect information concerning U.S. persons for nearly 30 years is in this respect an unsurprising sign of a predictable organizational pathology. The greater outside participation could help remedy going forward. Engaging in applying these lessons of institutional competence and design can allow us to do intelligence collection better.

MS. COLLINS: Thank you. We turn now to Aziz Huq, who is the Professor of Law and the Herbert and Marjorie Freed Teaching Scholar at the University of Chicago Law School. His research focuses on constitutional law, criminal procedure and Federal Courts. Previously Professor Huq was the Director of the Liberty and National Security Project of the Brennan Center for Justice.

MR. HUQ: Chairman Medine, Board members, thank you very many for the

opportunity to address you this morning. My testimony today will address two questions at the request of your staff. First, what is the origin of Executive Order 12333 and, second, what inference we draw from that origin about the relationship between the separation of powers privacy rights. In brief, I shall answer first that 12333 illustrates how the separation of powers can fail under those political circumstances that are perhaps most propitious to its success. And second, I shall argue that advocates of robust Privacy Protection should use a diversified range of institutional safeguards rather than leaning upon our entirely non self executing separation of powers.

History first. In 1976 the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities or the Church Committee published a comprehensive record of decades long illegality involving several security agencies. The committee, acting with a bipartisan concord that is rare today, pointed to the absence of

comprehensive organic statutes for the NSA, the CIA and the FBI. It urged that this gap be filled. With one exception, the 1978 FISA statute, the committee's statutory recommendations failed. A central reason was the Ford administration's timely promulgation of executive orders. These divided and sunk the legislative coalition for reform. One was Attorney General Levy's FBI guidelines, another was the February 18, 1976 Executive Order 11905, the precursor to 12333. Like many executive orders, both 11905 and 12333 rested upon diaphanous and gauzy imputations of statutory authority. Rather than instantiating Congress's will, 11905 and 12333 are best understood as executive instruments to thwart legislative will.

Why does the resulting statutory gap matter? It matters here because the 1978 FISA was never intended to be field covering. To the contrary, its regulatory reach is mapped by the definition of electronic surveillance in 50U.S.C.1801(f), which largely encompasses domestic wire communications. The Wiretap

Act's parallel boundary provision in 18U.S.C.2511 evinces similar limits. FISA's intended complements, however, were never enacted. And it is within that gap that those surveillance programs that have been identified in the media as operating pursuant to 12333 unfold.

Members of the Church Committee worried that non statutory constraints would prove evanescent. So it was. President Reagan campaigned for office on the promise to deregulate the CIA and he adhered faithfully to his word. On December 4, 1981 he issued Executive Order 12333. This abrogated a Carter-era revision of 11905. The December 1981 revision did many things. It expanded the CIA's authority to engage in both foreign and domestic surveillance. It enlarged the scope for covert actions. And particularly relevant here, it eased and enabled the dissemination of incidentally obtained information concerning U.S. persons.

Now, this trajectory of regulation matters because the late 1970's were

perhaps one of the most fruitful opportunities over the last several decades for Congressional regulation of the National Security Agencies. Legislators then, unlike now, did not want for information. The White House's luster stood at a post Watergate idea. One party also commanded significant majorities in both houses. Yet comprehensive regulation floundered in large measure, as I said, because the executive employed executive orders to divide and dilute Congressional opposition.

Subsequent trends have only deepened Congressional emasculation. Growing party polarization has raised the enactment cost of any legislation. The increasing technological sophistication of surveillance has widened the knowledge gap between the branches. And when specific statutory language can be mustered, such as in the operative provisions of the Stored Communications Act, the text rapidly yields to obsolescence.

We know what happens when Congress cannot agree or when it faces technical uncertainties. Canonical work by

political scientists such as O'Halloran and Epstein finds that it delegates. Delegation, which is the legislative panacea in other parts of the regulatory state, however, may well just be another way of stating the problem in the national security context.

So, what did we learn? First, my co-panelists have debated the legal question of the distribution of authority between Article One and Article Two. I would add caution. This legal question must be understood in light of if they observe dynamics between the branches. What Congress can do as a matter of law in short is quite different from what it is likely to do in fact.

Second, the history of interbranch dynamics suggests that the Congress will not reliably provide comprehensive regulation in this domain or that it will be able to update such regulation in the face of technological change. Congressional involvement may be necessary under some circumstances, but it alone cannot be sufficient.

Third, and finally, if constraints upon aggregate collection and analysis are desirable, they must be established in a more creative fashion. We can draw some insight from a tragedy that was roughly contemporaneous with the promulgation of Executive Order 12333. We might say with some glibness that one doesn't rest the success of an entire mission to space on a single O-ring. Preventing catastrophic outcomes, we've learned from the Challenger and like disasters, means having multiple often redundant safeguards in place. In the privacy context, it requires a plurality of institutional platforms to prevent the misuse of aggregated telecommunications data.

This Board is an important start. We could talk more about other robust internal checks, such as inspector generals, other kinds of privacy officers as well as external checks like support for and sanction of self help in the privacy domain as well as enlarge private rights of action. And we should further recognize the fruitful interaction between the

branches. Hence, when the Second Circuit Court of Appeals last week drew upon this Board's report to rule on Section 215 collection, it provided a small but useful example of how multiplicity of institutional platforms can interact to generate meaningful constraint that no one branch alone can provide.

Thank you for the opportunity to speak to you today

MS. COLLINS: Excellent. Three for three on time. So, for our last panelist challenge, Stephen Slick is the Director of the Intelligence Studies Project at the University of Texas at Austin. Before moving to Austin, Professor Slick acted as Station Chief and DNI representative in the Middle East. He has also served as a special assistant to the President and Senior Director for Intelligence Programs and Reform on the staff of the National Security Council.

MR. SLICK: Thank you, Beth. I appreciate the opportunity to be here today. I appreciate the invitation from the Board. I left Philadelphia 29 years ago, a law practice

up the street, to join CIA's clandestine service and I have never regretted that decision, but I always welcome the chance to come back to Philadelphia. So, with the chairman's permission, I'll move very quickly through a prepared statement and then welcome your questions.

This statement will address the circumstances surrounding the 2008 amendments to Executive Order 12333, the treatment of privacy and civil liberties issues that arose during that process as well as the limited separation of powers issues that we discussed while making those amendments several years ago now. There's a more detailed account of the interagency process that led to the amendments in 2008. It's captured in a Studies in Intelligence article from June 2014. I left several copies back on the desk and I'm sure there will be a scuffle breakout after we finish here over who gets the three copies I carried with me. But anyway, you're welcome to those. And then I'll conclude with a short comment on the practical application of the

Executive Order from the perspective of a CIA field operations officer. And for the record, because of my long association with CIA, these remarks were approved by CIA's Publication Review Board.

Although Executive Order 12333 was a near constant reference point during my career in the clandestine service, I was most intensely focused with the order while serving on the staff of the National Security Council in 2008 when the order was significantly amended by President Bush. My colleague, the NSC's legal advisor, Mike Scudder, and I were responsible for interagency coordination of draft amendments to the order before the President approved them.

President Bush chose to update the order late in his administration, in part based on the consensus recommendation of his Director of National Intelligence, Mike McConnell, the President's Intelligence Advisory Board and his senior staff advisors. After the Intelligence Reform and Terrorism Prevention Act was passed in 2004, creating the

position of the DNI, establishing the National Counterterrorism Center and mandating greater information sharing between intelligence agencies, the original Executive Order on intelligence signed by President Reagan in 1981 was clearly obsolete. With the benefit of two years' experience operating under the IRTPA, DNI McConnell proposed a series of amendments to the order that would clarify ambiguous provisions in the law, accelerate the process of integrating the intelligence community and also reinforce the DNI's role as the leader of that community. For example, Admiral McConnell sought a stronger hand in selecting and removing senior intelligence officials. He sought the authority to determine what data constituted national intelligence and therefore needed to be shared with him as well as with other agencies. And also the ability to implement more efficiently certain policies at intelligence agencies housed within other cabinet departments.

This latter objective grew from mounting frustration with agencies that would

repeatedly invoke Section 1018 of the IRTPA, a provision in the law that was intended to prevent the DNI from interfering in departmental chains of command. The President and his senior staff and members of the NSC Principles Committee were extensively engaged during the first half of 2008 resolving a series of thorny issues that arose while updating the order. The final text of the order was approved in late July after passage of the FISA Amendment Act and before Board Member Collins and her colleagues at the Department of Justice completed the Attorney General guidelines for domestic FBI operations that are described in the Executive Order.

With respect to the privacy and civil liberties protections in the 1981 Order -- or excuse me -- the 2008 Order, President Bush provided unequivocal guidance. He directed that the process of updating the Executive Order was to be privacy neutral. If an opportunity arose to strengthen the privacy and civil liberties protections of the new order, we were to do so, but in no instance

were safeguards in the original order to be weakened. In practice, this meant that relatively few changes were made to Section Two of the order.

One example of how civil liberties matters were addressed involved the DNI's authority to determine when information was of interest to more than one IC agency and therefore subject to the procedures for access sharing and retention that would be approved by the Attorney General. The amended order made clear that whenever such information pertained to American citizens or law enforcement investigations, the relevant procedures promulgated by the DNI had to be reviewed and approved in advance by the Attorney General.

Turning to the panel's assigned topic, separation of powers, I would note only that there was full agreement that amending Executive Order 12333 was the preferred means to achieve the goals of the DNI and the administration in 2007 and 2008. Between 2004 and 2007 there have been periodic discussions about whether to pursue formal amendments to

the IRTPA, but this option was never seriously entertained. There had been little appetite for reopening highly charged intelligence reform questions that were exhaustibly debated in the summer of 2004 within the administration and later that year by the Congress.

Indeed, the NSC principals agreed at one of the first meetings called to consider these amendments that one objective for the process would be to avoid taking any actions that were likely to provoke a legislative response. The overall goal was to establish a durable model for effective intelligence activity but within the framework of the IRTPA. We were aware that the intelligence orders issued decades earlier by Presidents Ford and Carter had been prepared with extensive consultation with the Congress. In 2008, however, the decision was taken to provide Congress with notice and explanation of planned amendments to the Executive Order. Requests from the Intelligence Oversight Committees for a draft of the order were declined. That decision was later criticized by the leaders of

these committees. Because of the many contentious issues addressed in the revised order and delicate compromises that were reached among Executive Branch principals, it's unlikely, in my view, that the process of updating Executive Order 12333 could possibly have been completed before the end of the administration if substantive consultations with Congressional leaders had been attempted.

Despite the criticism at the time, I'm not aware of any instance where the Congress has subsequently acted to reverse or modify any of the changes made in 2008. And notwithstanding the considerable attention paid to oversight of intelligence activities in recent years, the current administration has also not further amended Executive Order 12333.

Later today the Board will hear from distinguished panelists, several of whom are close friends of mine, about the practical application of Executive Order 12333. I would add to that only the following: Based on my several decades of service with the CIA, including multiple assignments overseas, it's

difficult to overstate the seriousness with which field collectors of intelligence treat the provisions of the Executive Order. As a young operations officer serving overseas under cover, my colleagues and I received annual in-person refresher briefings from CIA's Office of General Counsel about the provisions of the Executive Order. Years later while I was leading a large field station, I encountered Executive Order 12333 issues almost every day. For example, field managers are required to assign lanes in the road between different U.S. collection agencies that may be present in a foreign country. They have to apply minimization procedures to U.S. person information that's collected and they have to determine when it's necessary to disclose an intelligence affiliation to American citizens.

The Board should be assured that intelligence officers and managers serving overseas are trained to identify issues like these when they arise and seek guidance from more senior managers and their attorneys in Washington.

Thank you. Sorry for getting the red card.

MS. COLLINS: I think that means that you can't participate in the rest of this panel and possibly the next panel, if I remember soccer correctly.

MR. MEDINE: Thank you all for your very helpful comments. Two of the -- I guess I'm talking about separation of powers, we're talking about some strong powers of the president under Article Two and I'd like to focus on the Congress' spending power, which two of the panelists have addressed. I think we tend to think of legislative restrictions imposed on the President in terms of exercising foreign intelligence powers, but I'd like you to discuss spending power because that seems almost an exclusive grant of authority to Congress whereas, as was mentioned earlier, the President's power to conduct intelligence is inferred from some of the President's constitutional authorities.

So, what happens in the event of a conflict where the Congress in an

appropriations bill writes in a provision that says the President cannot conduct any foreign intelligence gathering in Country X? Is that constitutional? And doesn't Congress have exclusive spending authority to control the President's use of the budget or does the President say under Article Two I have exclusive authority and I'm going to spend money that I wasn't appropriated to engage in those activities? Any thoughts on how those two powers, separation of powers -- not the legislative, but the spending -- interrelate? And I guess we can start here.

MR. CHESNEY: Well, that's a great example to raise and it calls to mind the analogy here to the Commander in Chief authority of the President in Article Two where in our classrooms -- I suspect Deborah has the same experience -- we routinely are talking with students various hypotheticals about where the Commander in Chief authority might run up against various legislative powers and, of course, the history of Vietnam and the role that Congress played in compelling the military

withdrawal from Vietnam. Ultimately it was the spending power that did the trick, as we all know. Does that mean that there's no limits to the conditions that could be imposed by leveraging the power of the purse? At some point there has to be. So, in class when this comes up under the Commander in Chief clause heading, I'll pose a hypothetical about the use of the spending power to require that the military chain of command be disrupted in some obviously unconstitutional manner such as making the Speaker of the House the Commander in Chief because the spending power is being used in that way.

And this usually leads to what I think is the right answer, which is that bridge is too far. So, the question is how close to the constitutional bone can you cut in leveraging the spending power? And there is a substantial gray area in which reasonable lawyers are going to disagree about which bridge is too far. I think the Commander in Chief example I just gave you is sort of the paradine for what would be too far. But we

have the example of the funding constraints for Southeast Asia and Vietnam in the early 1970's to suggest some historical practice in which the Executive Branch acquiesced, allowing a cut pretty close to that bone. Perhaps the same set of considerations apply by analogy here in the foreign intelligence collection realm, which I see is actually quite analogous.

MS. PEARLSTEIN: So, I agree it's a great question. I think I'd say two things or make two points in response. The first is to keep in mind the conclusion that was detailed really wonderfully in the article by Marty Leiderman and David Barron several years ago about the scope -- entirely focused on the scope of the President's preclusive constitutional authority. And the conclusion of that rather lengthy historical study was that there's got to be some but not much. And the reason they concluded that was the case -- that is, not much that Congress couldn't constrain about what the President did was primarily historical -- that is, in the past 200-plus years, Congress has regulated,

including in the military context, but not only in that context, almost everything that the President has done. And today we have the really historically unprecedented example over the last several years of Congress regulating essentially who can and can't be released from a particular prison facility held in a particular wartime, which is one might have imagined was at that preclusive core and is nonetheless happening. So, I guess the first point I'd make is there's something there, but, you know, it's a narrow piece.

The second point I'd make on constraints surrounding Congress' spending clause power, which I otherwise agree, are -- you know, Congress has an enormous amount of power to say we're going to give you this money but only on the following conditions. And that is that Congress operates under a set of, as we've discussed, weighty and enormously effective political checks, which is to say that even when in Vietnam or otherwise a majority of Congress might have otherwise said we want the President to stop doing this, it

has felt constrained from exercising its spending clause power for political reasons. Now that may be and, in fact, often is exactly the way we want the system to operate. Among other things it means or it puts a check on Congress' exercise of its spending clause powers, it's unlikely to do something that's really extreme or really beyond the pail in pulling in the powers of the executive because it has, you know, all over it the desire and the political incentives to expand executive power generally.

MR. CHESNEY: Mr. Chairman, can I add a quick follow-up thought?

MR. MEDINE: Sure.

MR. CHESNEY: It occurs to me to emphasize that, of course, not all collection names are of equal stature in this regard. And so, going back to my opening theme of being mindful of these distinctions, if we imagine the distinction between collection undertaken to inform trade policy versus collection undertaken in the context of an armed conflict in which national self defense authority of the

President has been implicated, I think that's a salient distinction and I'm thinking of the prize cases in which the Supreme Court in the American Civil War specified that when it comes to national self defense, the President in that capacity when acting unilaterally, it's not just the President having the authority to do so, but as the court put it, it's the duty of the President to act in that circumstance.

And this suggests that to the extent there is a preclusive core into which even the spending power can't intrude, that core is going to be more strongly implicated in the national self defense scenario.

MR. MEDINE: So, I guess talking about the war powers that the President has, we also heard earlier both from my colleagues and from the panelists that as part of 12333 authorities, more and more U.S. person information is being incidentally collected. I guess the question I'd like to pose is what is Congress' authority to legislate protections for U.S. persons in the context of 12333 collections? Could Congress impose a probable

cause requirement, a warrant requirement, other restrictions that would limit or protect further incidental collections of U.S. persons in light of the fact that a lot of the activities we currently engage in are in war theaters or against terrorist activities? Does Congress have the necessary and proper authority to vindicate Americans' constitutional rights by imposing restrictions on the President's exercise of Article Two powers together and engage in national security matters?

MS. PEARLSTEIN: So, does Congress have the power to enact legislation protecting its civil liberties? Yes. And in a way I view this as a species of the discussion we've been having. As long as Congress has an affirmative authority that's applicable under the spending clause, which is centrally relevant here, under the commerce clause, which I think we shouldn't overlook the importance of, particularly in the context of regulations about the government's access to and use of channels of communications. I think there's no

barrier to that and, you know, with reference to my earlier remarks about attending to the nature of a preclusive core, one might logically reason it can't be within the scope of the President's preclusive power to do something that might otherwise violate the First or Fourth Amendments' right of the Constitution. These external limits exist on the President's power regardless. So, it seems a reasonable constitutional expectation that assuming Congress already has the affirmative authority to do it, that's certainly a realm within which it can act.

MR. CHESNEY: I'll just add that as I mentioned in my opening remarks, I think that the authority of Congress and the corresponding analysis of what the preclusive zone may be, Congress is in a very strong position when there are clear connections or clear nexus with First and Fourth Amendment equities. As a strictly technical matter, it gets a little bit tricky explaining precisely what the affirmative legislative authority is if you're not talking about leveraging of the

spending power. I understand the Foreign Commerce Clause argument. I'm not as drawn to it as I think my colleague is. And if we were talking about regulation of state government activity, you could simply point to the enforcement powers under Section Five of the Fourteenth Amendment and you could get enforcement legislation for any number of rights through that way.

We don't have identical language for the Fifth Amendment in regulation of the Federal government's activities and so, it might require a bit of fancy footwork. I think that the spending power is a critical piece to get around that.

MR. MEDINE: Can I have maybe a minute -- just a quick question and maybe a really quick answer, which is Congress not that long ago -- I guess in Section 309 of the Intelligence Authorization Act -- limited 12333 record retention to five years subject to a number of exceptions. You can say yes or no -- constitutional or not?

MS. PEARLSTEIN: Oh, I don't

know. I'd have to ask other questions. I'm sorry.

MR. MEDINE: Okay. I'll defer to my colleague since my time has expired.

MS. COLLINS: Although I think it's a great question, so if I have some time I might go back to that. I actually wanted to follow-up Professor Huq, if I could, with you on this notion of the separation of powers being non self executing. And the reason I ask your basis for that is it strikes me and another source of authority for a congressional power is, of course, their ability to make criminal statutes and criminal penalties. And so, to the extent that there is a statutory prohibition or restriction, there are individual agents within the Executive Branch who face potential criminal prosection for violating those types of legislative enactments. So I just want to press a little bit on what you meant by non self executing.

MR. HUQ: What I'm thinking of here is the mechanism that according to Madison would motivate the branches to act in their

self and trust in a way that produced the kind of equilibrium that the frame is anticipated. In the Federalist papers, Madison pointed to an identity between the interests of the officials who inhabited the different branches and the interests of the institution itself. There's a large literature in political science that legal scholars have recently rediscovered to the effect that individuals within the branches do not always or necessarily act in the interest of the branches. The point probably has the most force with respect to Congress, where incentives that are party framed are often more powerful than interests that are institutional in their grounding.

The consequence of the insight that the interest of the person is not always aligned with the interest of the institution is that the mechanism whereby the framers perceived the balance or the mechanism that the framers perceived as producing healthy equilibrium between the branches is one that is unevenly operative between the branches. So, in using the phrase non self executing that's

what I meant.

You are entirely correct to say that Congress has authority to enact criminal statutes. At the same time there is Supreme Court case law -- most importantly, the Armstrong case -- that recognizes the discretion on the part of the Executive Branch to determine when and how prosecutions proceed under statutes that Congress has enacted. And at least at the extreme, there are constraints that one might tie back to the Bill of Attainment Clause on Congress' authority to require a direct the use of criminal penalties, at least in the absence of the use of the impeachment procedures.

MS. COLLINS: Thank you. I don't know if it's Director Slick, Professor Slick, Steve, however --

MR. SLICK: Steve is fine.

MS. COLLINS: Excellent. This is a little bit of a combination of some of the panels we'll have later and what you talked a little bit about. With the 2008 changes to E.O. 12333, was some of the intention there

also to deal with technological changes? If not, why not and should there be a subsequent change to E.O. 12333?

MR. SLICK: Well, I'll answer the second half of your question first. When I mentioned at the end of my remarks that the current administration had not amended the 2008 version of the Executive Order, I welcomed that. It was an extremely complex undertaking. The range and scope of issues that were addressed in the four or five months we spent at a very high level working on this were truly daunting and there are second and third order consequences to change issue making in something that's been as durable and as pervasive as that. So, I would not undertake further amendments to that Executive Order lightly at all.

And to answer your question about technical change, I think we believed at the time in the spring of 2008 that those issues were largely being addressed through the FISA Amendments Act that was then under debate in Congress and Admiral McConnell spent a good bit

of time lobbying on the Hill, explaining to members how new technologies had changed the capacity of our intelligence community to collect and analyze information and they frankly did the best they could in that piece of legislation to reflect technologies that didn't exist in 1978. We did not have a broader discussion around the revisions to the Executive Order about new technologies and how they should be represented in that text.

MS. COLLINS: Well, since we do have the experts here and we have a recent piece of legislation signed into law, I'm going to ask David's question. I think it's a great one and I've got plenty of time on the clock for folks to answer, so legislatively imposed, although with some exceptions, restriction of five years on retention or materials collected pursuant to 12333? Professor Chesney?

MR. CHESNEY: If I'm not mistaken -- I haven't looked at this recently, but I believe there are some caveats to it; is that right?

MS. COLLINS: There are some

exceptions.

MR. CHESNEY: Yeah. I think that those are critical in enabling me to say yes.

MS. COLLINS: What were the types of factors that need to be reflected in that type of legislation in order to maintain its constitutionality?

MR. CHESNEY: Right. So I think you need to be mindful of the prospect that -- to go back to my example of, you know, a national defense relevant scenario or there's something that gets close to the bone of the President's duties relating to the national defense. Insofar as we can hypothesize arguments about the need to retain information for a longer term than the statute might otherwise allow, there's not an exception and you could have as-applied examples where it would be problematic to have such legislation. I think that by anticipating those types of categories, as I think this legislation does, I think you avoid those constitutional difficulties and that may be a good guide to how to -- if there's to be further legislation

in this area in containing those sorts of waivers and caveats, I think is critical.

MS. COLLINS: So, if the exceptions are capable of swallowing the rule, then it might be constitutional?

MR. CHESNEY: One can put it that way to make it sound a certain way, but I wouldn't put it that way myself. I think that they enable the rule to function in the vast majority of cases and with sensible carefully tailored exceptions, it can ensure its constitutionality.

MS. COLLINS: David?

MR. MEDINE: I'm not familiar with the changes.

MS. COLLINS: All right. Professor Huq?

MR. HUQ: I'm also not familiar with the exceptions that Professor Chesney described.

MS. COLLINS: You guys have not spent enough time inside the Beltway recently. This was the hottest topic for a while.

MR. HUQ: That explains so much.

You make us glad to not live in the Beltway. I think that the hard question is one of the question of who decides -- that is, the question of who has the discretion or who has the authority to make the determination on some kind of a categorical basis of when and how a matter of retention is critical to the national defense. The law and the case law, I think, does not provide us with even a framework for approaching that question or thinking about it. In part because much of the law and the Vietnam era examples, the price cases are all instances that are quite dissimilar from the retention context.

And to be frank, the closest that I can think of with respect to Presidential retention issues and Congress executive interactions is the second Nixon case, which concerns the Presidential Records Act and that's an instance in which notwithstanding what might have perhaps in the hands of another President been a more compelling set of claims received a fairly cold welcome on the part of the Supreme Court. So, if one is engaged in

the exercise of trying to fit this legislation within the different categories that the case law seems to give us for species of Congressional regulation, I think the closest fit is Nixon and I think that that lists in favor of broader rather than narrower discretion on the part of Congress to make judgments about what is as, as they say, necessary and proper.

MS. COLLINS: And with no offense intended to my fellow Board member, Judge Wald, what is your view of the institutional competence of the courts to be revisiting or looking at determinations by the Executive Branch or perhaps Congress, but more likely the Executive Branch as to what does implicate national security?

MR. HUQ: The question of institutional competence, first, is always a relative one. One doesn't just ask what the error rate with respect to courts is going to be, but what is the error rate of courts in relation to the error rate of some other institution -- for example, the Executive. One

also cares about whether the proportion that of false negatives and false positives is going to be different with respect to courts and with respect to Executive. So, if one believed, for example, that the Executive erred on, let's say, in terms of retention and disclosure in retaining too much and disclosing too little, and one thought that the court's word err on the side of retaining too little and disclosing too much, it may well be that one thinks that an error prone court is actually a desirable offsetting institutional check upon an error prone Executive.

MS. COLLINS: I think I actually should probably stop you here as I'm getting the red flag as well.

MR. DEMPSEY: Thanks again to the witnesses. Beth Collins has asked almost all of my questions, so thank you. So, all I'll try to do is a little bit of follow-up. One for Professor Slick: On this question of technology and the 2008 changes that followed the 2005, of course, revelations in the New York Times about warrantless surveillance,

domestic surveillance, which then translated into the FISA Amendments Act to Protect America, FISA Amendments Act debate which was ongoing simultaneous with the internal discussions about amending 12333. Was there at the time -- the legislative debate mainly focused on activities occurring inside the United States and it was only a tiny bit of FISA Amendments Acts that addressed surveillance outside the United States. But the disclosure and sort of some -- was there an effort to go through 12333 and say, well, whatever we're doing outside United States, there is some clause here or some framework everything we do fits inside the framework well enough so it's okay that Congress resolved the issues posed and raised in the Protect America Act and everything else is basically already covered by the general terms of 12333. In other words, was there an effort to sort of say, okay, let's look at what we're doing overseas and make sure that there is at least a clause or a phrase or a provision that it fits under?

MR. SLICK: I would first caveat my reply by saying I didn't have full visibility into every discussion that took place surrounding the 2008 amendments to the order. As I mentioned earlier, I was not aware of the kind of deliberate thought process that you described. That doesn't mean it didn't happen in the NSC lawyers group or it didn't happen in the Justice Department forum and legality review, but I'm not familiar with the kind of discussion and the kind of deliberative process that you describe. We were doing a lot of other things in connection with these amendments, trying to ensure we had a stable long term footing for the functioning of U.S. intelligence going forward.

Our hope was that this order would be durable, last several decades. The DNI was interested in enhancing his authorities in certain ways. This was not particularly popular with a number of department heads and so there was a lot of heavy lifting, but it had to do with the roles and responsibilities, the daily functioning of the intelligence community

rather than the issue you describe.

MR. DEMPSEY: Right, right. Okay. That's fair enough. But am I right in thinking about 12333 that somehow everything that's happening does fit within it? In other words, when you were in the CIA and when you had responsibilities for overseeing the activities and operations and personnel, you would always find comfort that, okay, that fits here or that is prohibited here and you would look at -- you said that 12333 issues arose frequently and if the issue came up of can we do this, why are we doing this, would you go to 12333 and say, well, that Section 1.8(b) or that Section 2.6(c) at least we've got that provision that lets us go forward. Is that the way the people look at it?

MR. SLICK: That's not the way that the field headquarters' relationship operates. We rely on our field managers, even our very senior and experienced field managers to issue spot. They review hundreds and hundreds of incoming and outgoing telegrams in a day. They're dealing with large numbers of

operations officers who are busy trying to build relationships and gather information. The role of the field manager is to issue spot on 12333 issues and refer them to headquarters.

And to answer the first part of your question, no, I never encountered a field operational decision that led me to doubt whether there was authority under 12333 or under a statute to go forward. And in any case, there's a chain of command and those sorts of issues are referred to Washington for more senior officers as well as for the general counsels to get involved.

MR. DEMPSEY: Different question entirely: Again, going to the question of the role the judiciary, maybe for all of the witnesses maybe starting with Professor Chesney, it seems to me that we do ask judges to make lots of fine-grained decisions, including technology decisions. You think about the Aereo case, the Supreme Court recent Fourth Amendment cases that involve technology, the Riley cell phone search case and other momentous issues, some of them quite

technologically sophisticated and other judgment calls, like the form of oversight the judiciary provides to law enforcement involving examination of very, you know, split second decisions obviously. In thinking about sort of all three branches and not only Congress, but the judiciary, could there be, should there be more of a role, particularly now in the era of programmatic surveillance, the FISA court has been given programmatic responsibility under the 702 statute -- what really constitutionally would limit, other than State Secrets Doctrine, which is not just a small thing, I appreciate, but what are your -- I mean, at some level I'm asking isn't it time that we begin to define a role for the judiciary in at least collection, national security collection activities, including those perhaps outside the United States?

MR. CHESNEY: So, it seems to me that first and foremost challenge for an expanded role for the judiciary is the case in controversy requirement, Article Three, standing and elements like that. And we're

seeing this now in the currently pending --

MR. DEMPSEY: I think that would drag down all of Title Three and FISA entirely.

MR. CHESNEY: Obviously, with respect to Title Three and for FISA Title One we've considered that question and decided to allow the court to have that role. I'm simply saying that if we're talking about less -- about still more complicated roles for the court in the nature of general oversight of programmatic surveillance, there are some questions surrounding the 702 rule and we're seeing the bite of these types of questions with proposals to add an adversarial component to FISK. And I think those to a substantial extent can be overcome, but that's the biggest check right there from a strictly legal perspective.

Then there's the policy perspective of, depending on -- and we've been generic here about what that role might be, so we might not even be thinking of the same thing. But depending on what the expanded judicial role might be, it may get beyond the

bounds of judicial competence, which is indeed broad and wide and expected to be able to move across many domains of expertise. You know, thinking about antitrust, for example, is an area where judges have to make all sorts of high stakes, complicated decisions. It's like they can do all sorts of things, but whether it's the right move to -- in our legal culture there is a tendency to want to look to the judges to save us and sometimes for very good reason, but maybe not always in every case is that the appropriate solution.

MR. DEMPSEY: Professor Pearlstein?

MS. PEARLSTEIN: So, I guess I'd make just a few points. One is it depends a lot exactly what it is we're asking the courts to do; right? So, obviously there are formal constraints that the Constitution imposes the case and controversy requirement. But there are some things the courts are enormously good at and experienced in -- interpretation, for example. So, if what we're asking is not for the court to recapitulate a first order

decision that the Executive Branch makes -- is this a good idea, is this not a good idea, do we need this information, do we not, but simply do you have the power to do what you're doing; right? That's an entirely different kind of inquiry than the inquiry we depend on the Executive as an expert agency, whatever, to make and that's the kind of inquiry that the courts are good at and very experienced with and so forth.

And you wouldn't want the court to simply recapitulate the first order decision that the Executive makes. And the reason for that flows from organization theory as well -- that is to say, it creates the so-called problem of redundancy problem. If you have a first decision maker saying, oh, I'm responsible or -- but I know somebody's going to check my work later, they're less likely to make a careful first order evaluation because they know somebody down the road's going to check their work, like my kid doing his homework; right? You want the courts to have a value added impact and it's entirely possible

to structure their world in a way that they do.

MR. DEMPSEY: Okay. Thank you.

MS. WALD: I have one sort of basic question which is going to take a minute to articulate and I just invite the answers, comments of all of the panelists. And that is I start out with the notion, which we all accept, we have a checks and balances Constitution which incorporates some notion -- the Federalist papers are full of it -- of how the Executive balances Congress, how Congress balances Executive, how the court comes in in cases of controversies. I'm wondering what you think -- I think Ms. Pearlstein said -- and I copied the quote -- "12333 offers little in the way of alternative processes that might correct for the absence of multi branch participation in ensuring an interest in liberty, accountability and effectiveness are otherwise served". Now, a couple of suggestions and they come, I think, from you and from other people in academia, who have suggested that in some situations -- and I think 12333 is one -- where there is no judicial and at least in practice

so far a fairly limited Congressional oversight. One suggestion from Professor Metzger up at Columbia is that Article Two's mandate to the Executive to, quote, "take care that the laws be faithfully executed" requires recognition of what she calls a duty to supervise defined as setting up a system and structure of internal supervision adequate to reserve the overall hierarchical control and accountability of governmental power.

Now, other people have suggested -- and I think Ms. Pearlstein alluded to some of them -- that perhaps there are ways to build into the Executive itself controls that feel a little bit like independence. I mean, whether they're ALJ's or people who are outside the Executive that review certain parts of the Executive's decisions, but some form of independence. And the third part that we've encountered and you mentioned in the FISA court is that even when you set up a court as a control, a form of multi branch accountability of it, we found -- and I think a large part of audience agreed with us -- that it really

doesn't work so well unless you have some adversariness in it.

So, I'm really looking for your suggestions about how to build on that kind of control. I think I'm being realistic to suggest we're not going to end up with FISA looking at every E.O. 12333 decision. We don't want that to happen. And maybe we can reform Congress, but having been, as Mr. Slick knows, in one of these former presidential commissions which made every possible kind of suggestion for reform of how you could make Congress be much more attentive to its duties. So has every subsequent one, including the 9/11 Commission, made the same suggestions. Some may come into being indeed, but one has to be, you know, a bit skeptical about it.

How do we try to in an E.O. 12333 situation duplicate the basic notions why you have checks and balances in the government? I think Professor Shlanger has talked about offices of goodness in which she included us very nicely as one inside the Executive. But how do you try to replicate in as important a

function as E.O. 12333 operations entities to perform the kind of independence accountability that we have overall in the Constitution and in many of the other parts of the government? It's a big question and go at it.

MS. PEARLSTEIN: So, I'll start and obviously welcome the others. I think there are a variety of ways of going at this, so let me try to categorize different ways. One is to go after this in a kind of enhancing expert, enhancing the role of expertise in this; right? So, if you think of the courts as one way of adopting a check and what they don't bring is expertise, but they bring different skills to the table. Another way is to try to sort of further depoliticize and/or systematize what's done and how the decisions are made. So, what do I mean by that?

One is -- and I think PCLOB, in its current iteration is a wonderful, right, example of this as well --

MS. WALD: Necessary but maybe not sufficient.

MS. PEARLSTEIN: Yes, yes. So,

in the human rights context we talk about now this universal periodic review system; right? Everybody, every nation submits to it. You know, how are we doing in the human rights by various human rights metrics. And it's periodic so that you don't have any -- you don't require a particular political event to trigger it, you don't require any independent action. It just automatically takes effect essentially by terms of statute in essence. This prevents things like counterproductive agency competition or feeling like, oh, we're the NSA, we're about to have our acts scored, right, it's required kind of across the intelligence community, it's systematized so that there is a regular expectation that not every 30 years, but every year, every two years or whatever this sort of review of how we're doing as technology changes, the privacy protections will be addressed.

In terms of expertise, there are also things like recordkeeping and sort of systematized metrics. Is this program effective at all; right? So, the NSA's Section

215 program, the Board's conclusion was -- not this Board's conclusion, but the Commission's conclusion was, look, it really didn't actually essentially contribute to any particular discovery in the counterterrorism context. That kind of discovery is important and a regular in the nature of Congressional research service body that's responsible for assessing sort of effectiveness, just raw effectiveness, I think is useful.

But there are also ways of constructing, I would say and then I'll stop -- professional incentives that remove appointment and removal authority over particular Executive Branch officials from any body that has -- any agency that has control over these intelligence operations. And just the independence of the actor, institutional and otherwise, I think --

MS. WALD: But how do you get -- I'm sorry to interrupt you, but very interesting -- how do you get independence within the institution? And are their mechanisms?

MS. PEARLSTEIN: So, here's an

interesting -- so, one way, for example, is developing an institution with separate professional commitments. And I'll give an example. The JAG Corps inside the Pentagon, right -- these are people who are uniformed military who absolutely report within the same chain of command to some extent, right? They have a somewhat different reporting authority than others do, but they're absolutely within the military and certainly within the Executive Branch. JAG lawyers played enormously important role in pushing back against efforts to, for example, carry out enhanced interrogation techniques to design military commissions in a way that was otherwise offensive. Why was it that the JAGS were able to operate at all effectively in this context; right? To some extent it's because they had separate professional ethics obligations in their role as lawyers, right, that other members of the branch didn't necessarily have. So, that's one example I'd give.

MS. WALD: Anybody else?

MR. HUQ: So, in thinking about

separation of powers, I find it useful to look back at the inspiration that Madison had, which was the writings of Montesquieu. And Montesquieu thought that you got restraint upon power -- not by necessarily chopping up government into executive, legislative and judicial, which is something that was unimaginable in pre revolutionary France. You got it by having many intermediate institutions, many what you might think of as platforms for dissent, difference and division within an outside government.

And it, I think, would be -- I think it is productive to use the terms that Montesquieu used to think about the ways in which we already have a plethora of institutions to serve the role that Judge Wald described. Perhaps not enough, depending upon your normative preferences of privacy, but arranged nonetheless. So, a couple of examples: Within the Executive Branch we have institutions like NIST, the National Institute of Science and Technology, that has played a very important role in promoting the private

use of technologies that enable people to use communications, media with privacy. Indeed, even the NSA has played that role by helping to promote certain encryption standards in periods of time. So, there's a diversity within the Executive branch above and beyond the offices of goodness that Professor Shlanger has talked about.

Moreover, courts, I think, play an important role. Perhaps not in terms of awarding remedies, but as Professor Pearlstein suggested, as what you might think of as catalysts for clarification. Again, the Second Circuit ruling from last week is an example.

And then the third and I think the hardest quality that one might think about is in what way does one create institutional cultures where the participants in the institution have an eye not just to the goal of the primary mission of the agency, but have an eye to other normative commitments.

MS. WALD: Okay. I notice the time is up. However, can I have one minute off of panel two? I'll take them off of panel two

just so the other two panelists can

MS. BRAND: You can have one of my minutes.

MS. WALD: Oh, thank you, Rachel.

MR. SLICK: Thank you. I'll try to be brief. I just would like to add a very practical consideration in response to your question. And I would encourage you -- nobody here -- to be quick to assume that there isn't extensive and exhaustive oversight and review already within the Executive Branch. Frankly, it's anything I have encountered. In a foreign environment we are leading the world in terms of scrutinizing and applying skepticism to our intelligence programs.

In that regard, having spent some time at a pretty busy intersection of this oversight and review at the National Security Council, we have chains of command. And at the chain of command is very often a person who's appointed by the President and confirmed by the Senate. We have the National Security Counsel, an intelligence programs director that I led where every covert action program is reviewed

on an annual basis and findings and recommendations presented to the President. The same thing for other sensitive intelligence collection programs. There is the President's Intelligence Advisory Board, which in recent years has always been bipartisan -- members of both parties there that provide discreet advice to the President. There's the Intelligence Oversight Board, a subordinate element of the PIAB that reviews the legality of actions. There are general counsels, there are inspectors general. Each of them have a relationship with Congress and they operate, as Professor Pearlstein was saying, very much like the JAG Corps. They're highly skeptical. They're officers of the court. A lot of hard questions are asked at every stage of a new or ongoing intelligence operation.

MS. WALD: You think that message really gets out to the public or even to the academia?

MR. SLICK: I think we should be more clear about it because a number of colleagues and I spent 80 hours a week for four

or five years doing exactly this -- asking hard questions to protect the administration and the President's interest and nobody should presume that a sensitive intelligence operation that places at risk the U.S. diplomatic interest or the interest of U.S. persons, U.S. citizens is lightly undertaken.

There are multiple reviews. I haven't even talked about the Office of Management and Budge, the White House Counsel, Department of Justice. There are extensive and overlapping layers of review and if everybody's doing their job, they weed out bad ideas and ineffective operations,

MS. WALD: Okay. All right. I just wanted to make sure. Mr. Chesney, in 60 seconds or less --

MR. CHESNEY: I can do it quicker than that. I concur with what my colleague, Steve, just said. I do think it's important to take care to specify the problem that we're talking about trying to address through institutional design. Are we talking about internal control failures where people are not

obeying the extant rules or even there's abuse taking place? Are we talking instead about the quality of the legal interpretations that are being adopted? Are we talking about the quality of the policy judgment? If it's the policy judgment, I'm not sure that you need to hear from law professors about that or at least you don't need to hear from me.

If it's the internal controls, I don't think the record suggests we have the sorts of abuses or failure to follow the rules that call for serious engagement, although that's something you always want to watch for.

I think that the issue deep is uncertainly about the legal interpretations and whether we understand sufficiently in the public domain at a high level of altitude what the authorities being claimed are. And of course, the dilemma there, as you know, is how do you cure that transparency problem without revealing sources and methods? And I think we have yet to figure out quite how to walk that tightrope.

MS. BRAND: Professor Chesney, I

wanted to ask you a question to begin with, and if someone else asked you this while I stepped out, humor me. You gave four or five considerations that you thought were relevant to whether Congress could constitutionally legislate limits, but you didn't take a position on which way any of them cut and didn't give any examples of where something might fall on one side of the lines. So I wonder if you could give an example of where legislative action might go too far or might not be permissible under one of your criteria. I was particularly interested in one that you mentioned -- substantive prohibitions. Can the government collect something at all? What would not be a permissible limitation?

MR. CHESNEY: I think it would be unconstitutional for Congress to forbid the Executive Branch from collecting information pertaining to nuclear proliferation or to forbid collection involving Iran or any sort of flat prohibition like that. I think that would be akin to --

MS. BRAND: Why is that?

MR. CHESNEY: I think that would cut not just to the bone, but would break through the bone of the core preclusive authority of the President. To the extent that he has any, it surely contains some amount of discretion in the deep duty to collect intelligence vital to the national defense.

MS. BRAND: You're familiar with the NIPF, the National Intelligence Priorities Framework?

MR. CHESNEY: Yes.

MS. BRAND: Do you think with something like that, which is sort of what you're talking about -- it's the topics on which the President and his administration want intelligence. Do you think that there is any role for the other branches of government before the fact? I mean, there might be oversight after the fact in some way, but is there any role before the fact or not?

MR. CHESNEY: By saying before the fact, do you mean --

MS. BRAND: Can Congress say, look, I think you should add this to the list

or I think you should take this off the list, that sort of thing?

MR. CHESNEY: Interesting. Right. Because, you know, my hypotheticals are sort of cartoonish and the more interesting questions get down into the granular level. Could Congress, for example, require elevation to a higher tier of a particular topic? This will sound like a dodge and I suppose it is, but here it comes. You get very quickly into the gray area of what -- reasonable people are going to disagree about whether this goes too far. The more granular, more modest the intrusion, the easier it is to say, gosh, that touches on the President's, you know, core responsibilities and duties, but it's such a modest intrusion that it's hard to say it's clearly unconstitutional. You certainly can't say it's clearly unconstitutional. What you can say is that it gets into a fraught area and then we throw up our hands and don't give a clear answer, or at least I do.

MS. BRAND: Okay. Mr. Slick, did you have --

MR. SLICK: Yeah. I would just add to that I have no professional view to rival my colleagues on whether legislation in this regard in terms of intelligence priorities would be constitutional or not, but I would encourage you and defer to a later panel when you have Michael Allen up here to ask him and I think Michael will tell you that the Congress already participates in the priority setting process. For many years now the intelligence community has recognized Congress as a perfectly legitimate consumer of intelligence. They, too, need information that's often secret information to play their constitutional role and therefore the NIPF or their subordinate priority setting mechanisms are briefed extensively of Congress. And if an influential member of Congress had a specific topical interest in intelligence, conveyed that to the intelligence community, that requirement would be satisfied.

MS. BRAND: Okay. Thank you. Are there any other examples, Professor Chesney, of something that might be

impermissible based on one of your criteria?

MR. CHESNEY: With the criteria, what I was really trying to do is gesture towards the relative stronger ground Congress is on when, in particular, it's working in an area that looks a lot like something Congress has done in the past, the Executive Branch has acquiesced in. For example, the requirement that Congress be, or at least the committees, the intel committees, be notified at some level of generality about certain types of activities or situations where there are Fourth and maybe First Amendment equities strongly implicated.

But I want to avoid any claim that there's a template or a cookie cutter approach where we can say, well, here are the type of fact patterns that are in and here are those that will be out. I just don't think it really works that way -- in part because as Steve just suggested, the practical reality is that there are a host of considerations having nothing to do with the separation of powers that actually inform much of the day-to-day give and take between the intelligence

agencies, the Executive Branch more generally and Congress.

MS. BRAND: Something occurred to me during the previous discussion -- I didn't think we'd be going here, but since you've opened the door -- when the subject of FISA's constitutionality came up a couple times, I think, in response to Jim's questioning and in your initial statement, you suggested that it's constitutional because it's become practice and the Executive Branch sort of acquiesced to it. Is that what you meant or do you think that it would be constitutional in the first instance? As you know, there was some controversy about that at the time FISA was enacted.

MR. CHESNEY: I think it was -- my own opinion is it's constitutional in the first instance because it was so directly tied in with Fourth Amendment equities in particular and the whole design of it is to try to capture these electronic surveillance situations where those equities are implicated while leaving untouched those that are involving non U.S. persons located abroad, the collections abroad

and those equities aren't there.

My point in emphasizing the practical precedent, as I would call it, is that it undermines the -- as you know, there were many and to this day some who still think it's unconstitutional. I think that position has been eroded over time by Executive Branch acquiescence very severely. But I wasn't persuaded by that position originally.

MS. BRAND: Okay. Mr. Slick, you raised the PIAB and I wondered if you could elaborate on the extent to which that's a -- how they exercise their oversight and what they do. That's not an agency we've had a lot of interaction with yet, although we've had a little bit. Can you elaborate on that?

MR. SLICK: I would offer by design the point of the PIAB and now the President's Intelligence Advisory Board was originally and when it's functioned effectively, it's been extremely discreet and operating outside public view within the confidence of the President. I would only say that the leadership and the members of the

Board during the five years that I served at the White House were extremely diligent, extremely bipartisan, extremely effective in their oversight and extremely influential in terms of the President seeking and taking seriously their views. And I can assure you from the intelligence community standpoint, if you're the director of a large agency and you're invited to come speak to the PIAB about any topic, you will be there and you will be prepared because they have this reputation for seriousness and influence.

And I think it's a very little known but highly important and effective check and balance on the function of the intelligence community, in particular because presidents in recent years have appointed people affiliated with both parties to the Board and treated them seriously. So, I can't help you better understand the functioning of the Board because I frankly think it operates best when it's not scrutinized particularly diligently from the outside. And if a president uses it and takes advantage of it, it can be a highly effective

tool in keeping his programs effective and lawful.

MS. BRAND: Can you give us a sense of the types of matters that come before it, whether it's programmatic or --

MR. SLICK: Everything.

MS. BRAND: Okay. I understand that IOB would look at more --

MR. SLICK: The IOB would look at reports of potential violations of law that are required under the Executive Board to be sent there for review. But there are few, if any, limits on the scope of the PIAB. If they ask for information or ask to speak to somebody, they'll get access to that. It can be regarding a specific incident, something that went well or something that went poorly that they wish to look back on and learn lessons from or it can be broad and programmatic or it can be, frankly, how effective is this leader of the intelligence community of a given agency. And that advice is conveyed in a highly confidential way to the President.

MS. BRAND: One last question for

Professor Huq: In your remarks I couldn't tell whether you were averse to the notion of extra statutory collection, if that makes sense -- collection that's conducted under some inherent presidential authority -- or not. I mean, your critique of 12333 seemed fairly far ranging. I'm wondering if there's some specific aspect of the Executive Order that you would improve or, if you could start from scratch, if there was some specific provision that you think should be included in it. So, go from generalities down to specifics.

MR. HUQ: I apologize if I conveyed a substantive view. I was trying to make descriptive points about the behavior of Congress and the Executive Branch rather than make a claim about what the law is or ought to be. With respect to extra statutory authority, my suspicion is as a practical matter. Most collection will occur in the number of statutes that have been enacted from the 1947 National Security Act onwards. And the treatment of penumbral activities executed under an Executive order raises what one might best call

complex legal questions which when they arise in the courts have been treated in a highly erratic way. So, the DC Circuit, for example, has confronted questions of this kind in a number of cases under the national security domain recently in cases like Wright, Chamber of Commerce v. Wright, Raskin v. Halder. And it's taken very, very different approaches to this sort of inference of penumbral Executive Branch authority.

From that I would conclude that it's very hard to predict and it's very hard to even know what the right framework for legal analysis is of such penumbral activities.

MS. BRAND: Thank you. My time is up.

MR. MEDINE: Okay. Thanks very much to the panelists for a very enlightening and interesting discussion. We're now going to break for lunch on your own.

- - -

(Whereupon, a luncheon recess was held at this time.)

- - -

MR. MEDINE: Good afternoon. We are resuming our discussion of Executive Order 12333 and we're going to begin our second panel, which is on First and Fourth Amendment implications of E.O. 12333 activities, the impact of new technologies. And Pat Wald will start that off.

MS. WALD: Thank you. Well, welcome back to our participants and to any new people that are joining us. Technological advances have changed the ways in which we communicate and obtain information. The rise of the internet, e-mail, cell phones and social media have transformed the modes of communication, not only used by the terrorist organizations but the public while also reshaping opportunities for the government to surveil. So, this second panel will address the First and Fourth Amendment implications of this new technological landscape as it pertains to foreign intelligence activities.

Now, once again, each of our three distinguished panelists will have eight minutes of remarks since we lost one of our

panelists. So, you get his time. Our aide in the front row will hold up a yellow card to let the panelist know that a minute remains. And once the first panelist's time is up, I'll introduce the next speaker. When all the speakers have given opening comments, each Board member will have ten minutes to ask questions and we'll begin with Professor Kerr.

Orin Kerr is the Fred Stevenson Research Professor of Law at George Washington University School of Law where his research and writing focuses on criminal procedure and computer crime law. Before joining the faculty in 2001, Professor Kerr was a trial attorney in the Computer Crime and Intellectual Property Section of the U.S. Department of Justice. He's also been a Special Assistant United States Attorney in the Eastern District of Virginia and he clerked on the Supreme Court for Justice Kennedy. Okay, Professor Kerr.

MR. KERR: Thank you. It's a pleasure to be here. I want to talk about the Fourth Amendment limits on evidence collection around the world and I want to start with an

overview of how the law applies based on what we know and then I want to talk about some of the ways that the law may apply based on things we don't know but would need to answer to really get a sense of how the Fourth Amendment applies to evidence collection all around the world.

So, the first thing I think we know based on current law -- and I'm just going to focus for now on existing doctrine -- if you're a lower court judge applying the Fourth Amendment looking at the Supreme Court's cases and lower court cases, what does the state of the law seem to be now. The first and most important thing you would see is that most people around the world don't have any Fourth Amendment rights. And that is because of a Supreme Court decision from 1990 called United States versus Verdugo-Urquidez in which the Supreme Court in a majority opinion by Chief Justice Rehnquist says that the Fourth Amendment only gives -- only grants any rights at all to those who have a significant voluntary connection to the United States and

does not give rights to people outside the United States who have no significant voluntary connections to the U.S. In the Verdugo-Urquidez case, the case involved a search of a man in Mexico who was a Mexican citizen who had been brought to the United States on trial and his house had been searched in Mexico and the Supreme Court says he has no Fourth Amendment rights to speak of. The thought being that the Fourth Amendment gives rights to the people and that implies some sort of political community and that people outside the U.S. who aren't U.S. citizens or a permanent resident alien traveling abroad would have no Fourth Amendment rights.

So that's the first step and that immediately says that there's a lot of surveillance around the world which won't implicate the Fourth Amendment at all to the extent that the people monitored are not those with voluntary substantial connections to the United States. That doesn't mean that if you're a U.S. citizen and you go abroad, you have no Fourth Amendment rights. The lower

courts have addressed some of the standard for how the Fourth Amendment does apply when a U.S. citizen or any kind of U.S. person travels around the world.

And most courts have said -- this is really an issue of Circuit Court decisions -- that the law imposes a standard of reasonableness rather than the warrant requirement. So, the Second Circuit and the Seventh Circuit have expressly held that there is no warrant requirement abroad and that instead the Fourth Amendment requires reasonableness -- the big question being what does reasonableness mean in that setting? And courts are not exactly clear on how to figure out what is a reasonable search, a reasonable warrantless search, although the courts so far have applied kind of a balancing idea of looking at the significance of the search, looking at the government's cause and sort of looking at the totality of the circumstances.

So, that's a broad overview which tells us that, first, the government can conduct essentially unlimited monitoring for

Fourth Amendment purposes of foreigners, those without a U.S. voluntary connection, and then has to satisfy the reasonableness standard for U.S. citizens, permanent resident aliens abroad.

Things get much more complicated when you try applying that rule for the reason that in the context of internet communications, you have people that could be in different locations, monitoring that could occur in different locations, you could have a U.S. person communicating with a non U.S. person, you could have the monitoring in the U.S., the actual point of interception, the point of collection occurring inside the U.S., occurring outside the U.S., occurring in a particular country, occurring in an overseas cable. And the difficulty is that if the reasonableness standard hinges on where the monitoring occurs, you need to come up with some sort of idea as to which reasonableness standard applies. Is it where the person monitored is? Is it where the interception occurs? Is it where the data is analyzed subsequently? And right now we

just don't have answers to that question. It's a really important set of questions.

I think normatively the best answer is that the reasonableness standard should follow the point of data collection rather than data analysis or the location of the person. And I think that's the most consistent rule with other areas of Fourth Amendment law and probably the easiest standard to apply. But I should be clear that that's just my normative sense of what probably the best rule is. And the answer from current case law is really we don't know. It's just an area that the courts have not yet reached.

And I also want to stress the relative degree of uncertainty, even on the first question of who has Fourth Amendment rights. I think the best reading of Verdugo-Urquidez is that the majority opinion from Chief Justice Rehnquist is the binding opinion, it is controlling. At the same time, that's a curious opinion in that Justice Kennedy wrote a concurring opinion. He joined the majority but then wrote a concurrence in

which he offers a very different rationale, a rationale rooted in a prior decision called Reid versus Covert and concurring opinions in that case, which seemed to say that rather than applying a sort of contractarian notion of the people get Fourth Amendment rights, non people don't. Instead that the scope of the Fourth Amendment, as a practical matter, you look at sort of legitimate government interests and what kind of rules, Fourth Amendment rules, would implicate or be inconsistent with those interests. And it's much more of a pragmatic standard in that case, leading Justice Kennedy to say that, at the very least, the exclusionary rule or the warrant requirement, rather, would not apply.

And it's difficult then to say in looking at Verdugo, do you look just at the majority opinion, do you look at the concurring opinions. And then to make it a little more complicated, there's a line in the recent decision, Boumediene versus Bush from 2008, authored by Justice Kennedy in which he cites his Verdugo-Urquidez concurrence in support of

the interpretation of the suspension clause abroad.

And I think the difficulty is that there's sort of two ways of thinking about how the Fourth Amendment applies abroad. One is to say that the Fourth Amendment is its own part of the Constitution. And the rules for the Fourth Amendment are specific to that amendment and you shouldn't say this is how the Fifth Amendment applies or this is how the suspension clause applies, therefore it means how the Fourth Amendment applies. In other words, sort of an amendment specific approach.

The other is to say that there's some sort of broad answer to how the Constitution applied and the Fourth Amendment is just one piece of that puzzle. And what makes it complicated, I think, is that the Verdugo majority opinion seems to take the former approach. Justice Kennedy and his concurring opinion and then in Boumediene seems to hint at the latter approach. And you have to figure out, well, which do you follow. Do you sort of follow the likely swing vote in a

future case or do you follow the binding rule as it exists now?

I think doctrinally the answer is you follow the binding rule from Verdugo-Urquidez, the five Justice majority opinion. The rationale being that Justice Kennedy had a choice in Verdugo -- either join the majority opinion or not. If Kennedy joins the majority opinion, he gives up the ability to control under a Marks Analysis to have the controlling opinion for lower courts. And he made that decision and, therefore, the majority opinion is binding.

It's entirely possible that that won't be the case in the future, that the future Supreme Court would look at these issues differently. At the same time, we really have no idea what the Supreme Court would do with these issues in the future. We don't know who would be on that court, for example. It may be that Justice Kennedy would be the swing vote, it may be that the issue doesn't get to the Supreme Court for 25 years and Justice Kennedy is retired at that point. We just don't know.

So, I think from a lower court perspective and just for purposes of understanding what is the law right now, the Verdugo-Urquidez majority opinion and its significant voluntary connections test is the one to follow.

So, that's a basic overview and I look forward to the questions.

MS. WALD: Thank you. Professor Strandburg is the Alfred Engelberg Professor of Law at NYU, New York University School of Law where she teaches, among other things, innovation policy and information privacy law. She's also in her own right a research physicist with qualifying degrees from Cornell and Carnegie Mellon. So, I think you might qualify as our technologist.

MS. STRANDBURG: I don't know about that. But thank you very much and it's a pleasure to be here. I'm going to speak about the First Amendment, potential First Amendment constraints on government collection under Executive Order 12333. So, this is an area where there really is very little directly on

point case law, so I'm going to try to go through my analysis briefly and then we can discuss it in the questions.

So, the first point I want to make, which I think is pretty clear, is that the First Amendment protects U.S. persons, communications and associations with each other and with foreigners, and that that's the case even in the national security context. And I think that's clear from the Supreme Court's discussion. Whatever one thinks of the holding in Holder versus Humanitarian Law Project, where the court applied a strict scrutiny test under the First Amendment.

The second point is that surveillance of communication content implicates First Amendment rights, again, even in the national security context. And there are many courts that have made statements to that effect. One well known one is the one from the Keith case where the court said though the investigative duty of the Executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected

speech, and the price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power.

So I think those two points are fairly clear. I also have argued in some of my writing that surveillance of communication metadata, particularly when that metadata is collected in bulk, implicates freedom of association. And in situations where it is -- which it is if it's collected in bulk -- where it's equivalent to government compelled disclosure of protected associations. And this is based on a variety of case law, but most importantly on Supreme Court case law holding that government demands for associational information that are sweeping and indiscriminate violate First Amendment because of the chilling effects that such collection can produce and because they are not sufficiently tailored to the compelling government interest.

Okay. So then the next point to make is that, in fact, the courts have applied strict or heightened, almost strict scrutiny to

data collection, which is bulk and indiscriminate, as I just mentioned, and also when collection is based on the content of the speech. And I think that that would have to apply to when collection is based on an individual's association with a particular other individual. And that's also suggested by the Holder versus Humanitarian Law Project case.

So, next I have argued elsewhere -- and I think the best way to understand what First Amendment scrutiny would mean in this kind of context -- is that in cases involving surveillance where there almost always is a compelling government interest, either in law enforcement or in national security, the primary implication of First Amendment scrutiny is that the surveillance must meet requirements of specificity. And in particular, there has to be a specific compelling government interest, which has to have a sufficiently close nexus to the specific -- and the surveillance has to have a sufficiently close nexus to that specific

interest. And there have to be no substantially less burdensome means to achieve that interest. And so, I've argued that at greater length in some of my writing.

So, how does this apply to the context of E.O. 12333? Well, I'm going to focus on the collection of U.S. persons' communications or communication metadata that is collected abroad and where one is not targeting a U.S. person. So, under that circumstance, there are two kinds of situations where you would collect U.S. persons' communications. One is when they are communicating with a target that is not a U.S. person. And the second is when there is some sort of bulk collection going on that is not targeting a U.S. person.

So, first, I would argue that First Amendment applicability, unlike perhaps Fourth Amendment applicability, shouldn't depend on the location of the collection point because it is a protection of the speech rights and association rights of the individuals, the U.S. persons, that are involved.

Second, I would just emphasize again that specificity and tailoring are the key factors that come out of the First Amendment's requirements. So, I would argue that in general, activities that result in bulk collection of a U.S. person are highly suspect under the First Amendment and that is whether or not the U.S. persons are targeted or the collection of U.S. person information is only incidental. If the result is bulk collection, then I think there is a need to be worried about specificity and tailoring.

And finally, that collection of U.S. person data that is simply incidental to collection that's targeting a non U.S. person or either communication or associational information, I think whether or not that would pass muster under the First Amendment depends on how well the targeting is done and how substantial the incidental collection of U.S. person information is. I don't believe, though, that the mere presence of a foreign intelligence purpose or a mere relevance to national security is necessarily sufficient if

the result is significant collection of U.S. person information.

Finally, because we're talking about the First Amendment and not the Fourth Amendment, though, we aren't necessarily just looking at the collection of communications. It's the overall government imposition on First Amendment protected communication or association that matters, the overall chilling effect were all negative implications. So, I think one has to look at the whole thing, the entire thing of what the government is doing. And in particular, I want to suggest that one should be concerned about querying of any sort of bulk or incidentally collected content or associational information in order to pull up with the purpose of pulling up U.S. person information. I would argue that that kind of querying also has to meet the specificity requirements and that in order to do that, would require some kind of standard, something akin to a warrant standard. And similar kinds of concerns, although not with quite the same First Amendment gloss to them, have been raised

in the 702 Report of this Board and also the President's Review Group.

So, I will -- is that the red one coming out? Okay. I'll stop there.

MS. WALD: Okay. Thank you very much. Our last speaker is Stephen Vladeck, who's a professor of law at American University Washington College of Law. His teaching and research focus on Federal jurisdiction, constitutional law and national security law. He, like the other members of the panel, is published widely in law reviews and popular commentaries and he clerked for Judge -- on the Eleventh Circuit for Judge Barkett and Judge Berzon on the Ninth Circuit.

MR. VLADECK: Thank you, Judge Wald. Thank you to all the members of the Board for the invitation to participate in today's meeting. You know, it's a common assumption, as Professor Kerr's statement suggests, that surveillance conducted pursuant to Executive Order 12333 doesn't implicate the Fourth Amendment for four different reasons. And I think we heard two of them from my

friend, Professor Kerr. First, that insofar as it's targeted at non U.S. persons, they are categorically outside the Fourth Amendment thanks to Verdugo. And second, insofar as it's sweeping in communications by U.S. persons who are outside the United States, that there are at least two Circuit level decisions holding that the warrant clause doesn't apply, they just need to be reasonable.

I think there are two other arguments that are often heard for why the Fourth Amendment isn't a problem. The third is that any collection of U.S. persons' communications pursuant to 12333 is merely incidental and so it doesn't implicate the Fourth Amendment rights of those individuals under the I think correctly but badly named Incidental Overhearers Doctrine.

And then, fourth, in any event, even if the Fourth Amendment did apply to 12333 surveillance, the foreign intelligence surveillance exception to the warrant clause would mean that such surveillance need only be reasonable, even as applied to U.S. persons in

the United States to pass constitutional muster.

And what I'd like to do in my brief remarks today is offer a more circumspect view of the Fourth Amendment status quo and offer four specific reasons why in my view this assumption may be challengeable and contestable at least going forward. Orin already did some of this work in talking about the relationship between Verdugo and Boumediene. I'll just jump right to what a panel of the Fifth Circuit suggested last summer, which is that the Boumediene court appears to repudiate the formalistic reasoning of Verdugo-Urquidez as a sufficient connections test. That panel opinion has since been vacated so it's not exactly precedent, but it does suggest that there are at least some judges who are beginning to think that the formality of Verdugo-Urquidez needs to be reassessed after and in light of Boumediene. And the mere fact that that conversation is happening, to me is a very important development.

Second, and in any event, it

seems increasingly awkward, as Orin suggested, to try to shoehorn electronic surveillance in the constitutional doctrines grounded in what a really Westphalian conceptions of territoriality and sovereignty. As my colleague, Jennifer Daskal, explains in a forthcoming law journal article entitled The Unterritoriality of Data, the ease and speed with which data travels across borders, the seemingly arbitrary paths it takes and the physical disconnect between where data is stored and where it is accessed critically tests these foundational premises of our current Territoriality Doctrine.

In this regard, consider the pending Second Circuit appeal in the case involving whether the District Court can demand production of e-mails stored by Microsoft on servers located in Ireland. There at least the government takes a strongly anti territoriality position or at least one based on where the data can be accessed -- not where the data is stored. At bottom, Verdugo-Urquidez increasingly appears to be an analog decision

that we're struggling to apply to digital world, even if the Supreme Court hasn't said so yet.

Third, even if 12333 surveillance of non U.S. persons remains categorically outside the Fourth Amendment, we know now that the government has collected and will inevitably collect communications of U.S. persons under the same authorities. The typical response is that such collection lies outside the Fourth Amendment insofar as it is incidental, much the same way as if a wire tap obtained to produce evidence of one crime incidentally revealed evidence of another. But there is, in my view, a marked difference between accidental incidental collection as in the wire tap example and intentional incidental collection where the government knows that the surveillance method at issue will result in the collection of non targeted communications to which the Fourth Amendment would otherwise apply and does it anyway.

As Judge Sand explained in his 2000 decision in the Bin Laden case, applying

the incidental collection doctrine to this lateral class of cases is, quote, significantly more problematic, unquote, from a Fourth Amendment perspective. Again, no Circuit level or Supreme Court precedent, but just reason to wonder if these same doctrines are going to apply as categorically.

Fourth and finally, if the Fourth Amendment does apply to any of the surveillance that the government conducts pursuant to 12333, it's not at all clear to me that the foreign intelligence surveillance exception to the warrant clause would cover the whole range of 12333 activities. Although the court of review in the Directives case has held that foreign intelligence surveillance need only be a significant purpose of government surveillance activities for the exception to apply. Every other Circuit level court to reach the question has held that the Constitution requires that foreign intelligence surveillance be the primary purpose of the government surveillance activities. Note the distinction between this Fourth Amendment interpretation and the

statutory primary purpose doctrine that Congress abolished in the U.S.A. Patriot Act.

And there are any number of reasons -- I don't mean to belabor the point -- unless we're willing to accept that all foreign surveillance is foreign intelligence surveillance and there are lots of reasons why we should resist that, then it stands to reason that at least some 12333 activities would not fall within this exception to the warrant clause and would therefore raise serious constitutional concerns.

Now let me close with a caveat. The circumspection I've offered this afternoon is grounded as much in questions that haven't been answered as it is in existing rules and doctrines. I agree entirely with Professor Kerr that Verdugo-Urquidez is still the law even though Justice Kennedy may not be sure what law it is. And my goal has not been to take a specific position on the merits of the relationship between 12333 and the Fourth Amendment, but rather just to suggest to you that the relationship is far more nuanced and

potentially more troubling than we typically assumed and that going forward, because of new technologies, because of the increasing interoperability of data and because of these doctrinal questions I've raised today, these questions might be more troubling than we've typically assumed.

Thank you for your time and I look forward to your questions.

MS. WALD: Okay. Thank you. I'll start off on the questioning. Professor Kerr, I believe you said that the reasonableness should follow the law of the place where the data is actually seized or collected. And combining that with your and others' observations on Verdugo, does that mean in effect that foreign law has no input into the question of reasonableness as to the place where the data was seized? I mean, let me be a little bit more specific on that. Apart from whether it's the law of Germany -- let's use Germany as the place where the data was seized -- and taking into account the President's directives on PPD 28, does that

suggest that there's any role for either international law, some of the basic concepts in international law which are supposed to and perhaps are embodied in some treaties kind of go across the whole universe or do we just decide about the reasonableness following American law precedent?

MR. KERR: So I think we don't really know.

MS. WALD: Yes, I know, but I'd love your ideas.

MR. KERR: In terms of what the law should be, I think -- you know, it's hard to say because there's so many different situations where the issue can arise. So, one context in which the cases have come up is joint investigations. Say it's a criminal case, U.S. authorities working with authorities in Belgium monitoring a U.S. citizen who's in Belgium and they want to search the apartment in Belgium and they get a search warrant in Belgium and the Ninth Circuit has said in that context that the reasonableness standard is based on foreign law -- that is, Belgian law.

And as long as the U.S. officials were acting in good faith compliance with that law, that seems reasonable. And I think that sort of has a common sense quality of well, what else do you expect them to do. I mean, they can't go to a U.S. judge and get a search warrant in Belgium and the piece of paper of a U.S. warrant doesn't have any meaning in Belgium.

So, that's almost kind of a common sense idea and interestingly goes back to Justice Kennedy's opinion for the Ninth Circuit in the 1980's in the Peterson case. Other cases are going to be more unilateral U.S. action and then you have to come up with a sort of conceptual answer to what replaces the warrant if there's no warrant requirement and is that case by case reasonableness? Is that categorical reasonableness? Is that a probable cause requirement? I can think of lots of different ways that the law could be construed. For example, one idea would be there's no warrant requirement, you don't have to get the paper, but the government does have to satisfy probable cause, for example. Or maybe they

have to satisfy reasonable suspicion, a lower requirement. So, some threshold that doesn't require judicial review ex-ante but does require a kind of sense of cause to justify that. That maybe makes sense in the unilateral context where the U.S. is acting without another country's officials involved.

It's not totally obvious that it makes that much of a difference in practice because you could see all of the reasonableness standards to the extent you want to say, well, we're going to factor in foreign law, we're going to look to foreign law, which itself is probably premised on similar kinds of reasonableness considerations that the Fourth Amendment reflects. It may be that all roads kind of lead to the same place, but I think doctrinally we just don't know.

MS. WALD: One follow-up on that and then I'd like to hear the other panelists. And that is that if you looked at some of the current guidelines of E.O. 12333, one of them says that -- one of the published guidelines says that if a warrant would be required under

U.S. law for a certain kind of operation, then the Attorney General should personally give his okay to it. My question, I guess, would be following up on yours, suppose it isn't strictly a warrant case, but it is a case where under U.S. law you have to have a reasonableness inquiry, the kind you just talked about -- maybe not a warrant, but mere reasonableness. I guess does it make much -- is the dichotomy really that definite -- you know, if it's a warrant here, we get the Attorney General's advice, but if it's a situation where the second part of the Fourth Amendment, the reasonableness inquiry applies, what should you do in that circumstance? Is there protection in the hierarchy inside the E.O. guideline for the two parts of the Fourth Amendment or is it okay to just have one get the highest level of supervision?

MR. KERR: I would guess that as a practical matter, oftentimes having the Attorney General approve a search based on a probable cause standard is equivalent to or maybe even higher than having a Federal judge

review the warrant application, given the realities that some judges are going to carefully scrutinize warrant applications, some less so. So, probably the Attorney General's going to take it seriously -- you never know obviously, but that's at least likely in a number of cases. So, it may not make that much of a difference in terms of the actual amount of privacy protection in terms of who does that check.

And this is, I think, a broader question in Fourth Amendment law -- you know, how often do you need a warrant versus a showing that is later proved in court? One thing that makes it difficult in the national security context is you usually don't end up in court. So, some sort of paper -- some sort of ex-ante judicial review or review by someone plays the role that otherwise is much more difficult to have without that.

MS. WALD: Thank you. Ms. Strandburg, you gave us a pretty good account of one of the questions I was going to ask you, which was how you would propose to bring the

free speech rights of the subjects of E.O. 12333 abroad into this particular kind of regime and you mentioned several of them -- specificity and several others. But I wondered, some of the guidelines, at least the ones we have access to as published guidelines, do have minimization requirements. And, of course, minimization is the technique which has been accepted by the IC and by the FISA court for a lot of the incidental U.S. persons' information collected under a 702. You can have your varying views and we've had them even on this Board as to how adequate they are. But I'm wondering what your opinion is on whether it's useful to have minimization requirements and, if so, how tight should they be or what should they be?

MS. STRANDBURG: So, I do think it's useful to have minimization requirements, but I'm not sure that it's always sufficient, so I -- but, you know, this is kind of an unknown area, right, but because courts have not asked this question yet under the First Amendment context. But I don't think that --

my own view given -- and this is based mostly on the First -- the freedom of association case law, which I think comes kind of closest. I don't think that saying, well, we'll take really good care of it once we've got it is enough specificity for bulk collection, for just sort of, you know, dragnet bulk collection. I think that the requirement of tailoring to a specific purpose is greater than that. And in some ways I take some of this from -- one place that you can -- you might think about this anyway -- is that we do have the case law saying that from, say, Stanford versus Texas or Zurcher versus Stanford Daily saying that in the First Amendment context you have to keep -- you have to apply the Fourth Amendment warrant requirements with scrupulous exactitude. And what that means in the actual context of those cases is particularity. You have a higher --

MS. WALD: I've got to cut you off in order to have one quick question for Mr. Vladeck before my time is up. And this pertains to the Second Circuit case last week,

with which I'm sure everybody's familiar. The published DOD regulations use the standard, I see, definition of collection as beginning only when, quote, it has been received in an intelligible form for use by an employee in the course of his official duties, unquote. The recent Second Circuit opinion, as I read it, seemed to lay down a contrary standard that collection begins when the information is, quote, seized by the government from its source and it's searched, quote, when its computer is scanned. I wonder if you just have some quick comments on that particular --

MR. VLADECK: I think that's a fair reading of the Second Circuit's opinion and I also think it was, at least in some ways, necessary for its analysis of why the plaintiffs in that case had standing. Because they could prove, based on the government's representations, that their information had been collected. They could not necessarily prove what had happened subsequent to the initial point of collection. And that's also consistent with what Judge Leon at least

concluded in the District Court decision in the Klayman case.

MS. WALD: Yes. But do you think that's legalized --

MR. MEDINE: I'm sorry. The time has expired. Mr. Dempsey?

MR. DEMPSEY: I guess one question I would have is to ask Professor Vladeck and Professor Kerr to comment on sort of the relationship between the First Amendment and the Fourth Amendment. So many cases, it seems to me, take one branch or the other. Most of the data privacy cases, of the past 30 years maybe, since the NAACP cases have gone on the Fourth Amendment prong -- not the First Amendment prong. But thoughts, Professor Vladeck and Professor Kerr, on the relationship between the First Amendment and the Fourth Amendment, particularly when we're talking about collection overseas but affecting U.S. persons.

MR. VLADECK: Well, I mean, I think there's obviously a relationship. I know Professor Kerr's colleague, Daniel Solove, has

written a lot about the First Amendment as a -- basically as a rule of criminal procedure. I guess my reaction is just sort of situated in the doctrines that we're living with, which is to say, that under current doctrine, I think there's much more reason to be concerned about the First Amendment implications of surveillance activities overseas as opposed to the Fourth because the Supreme Court has not been nearly as categorical in its rejection of First Amendment rights for non U.S. persons. And I think a good example of this isn't a Supreme Court case -- it's a Ninth Circuit case from a couple years ago called Ibrahim versus Homeland Security, where the Ninth Circuit held that a Malaysian graduate student who was not an LPR nevertheless had First Amendment protection sufficient to challenge her inclusion on the No-Fly List, even when she wasn't in the country. You know, which is not quite as far as, say, a non U.S. citizen with no connection to the U.S. whatsoever, but it strikes me as a much more functional approach to this question than is usually seen under

Verdugo.

So, I think there is a relationship. I think there's a natural gravitation toward the First Amendment because of the doctrinal complexities that Orin referred to.

MR. KERR: I think based on current law, the role of the First Amendment is actually much more modest than maybe has been suggested. And it's true that there are a lot of court decisions where the judges say and justices say First Amendment concerns are implicated here, we need to be especially sensitive to those concerns. But when the rubber hits the road my sense is that the same Fourth Amendment rules apply -- maybe with a teeny tweak, but not with a substantial shift. And maybe the best example of this is the Zurcher versus Stanford Daily case, which strikes me as being really at the heart of the First Amendment. It was a search of a newspaper for evidence of a crime that the newspaper happened to have because the reporter had taken photographs of a news event. And the

police wanted information about the crime, so they break into the newspaper and find what they're looking for. And the Supreme Court says that's fine under the Fourth Amendment. And if there's any case where you'd say as soon as you have First Amendment concerns, the First Amendment should have some different rule. I would think Zurcher would really be the poster child for that.

But you don't really see much of that. As you suggested, the courts usually just draw a distinction between the two. And the way I think of it is once you're dealing with kind of a good faith government investigation, usually the First Amendment concerns kind of go away in the case law. There's some -- oh.

MR. DEMPSEY: Just one quick -- Professor Strandburg, if the government agencies in those NAACP membership list cases -- if they had thought there was a crime and they had gotten a search warrant, could they have gone in and seized, right? They could have gone in and seized the list?

MS. STRANDBURG: Right. So, actually, that's pretty close to exactly how I was going to respond to what Orin just said, which is that I think that there is a substantial amount of overlap between the Fourth Amendment and the First Amendment. And generally in cases where a warrant is involved, the courts have tended to find that the Fourth Amendment requirement of the particularity requirements of the warrant are sufficient to meet the First Amendment requirement.

MR. DEMPSEY: They are sufficient?

MS. STRANDBURG: Are sufficient as long as they are -- as long as scrupulous exactitude is used. But I think that when you -- I mean, there's not a lot of case law on this, but when you get outside of the warrant context -- so, for example, in the context of subpoenas, there are a number of cases involving subpoenas for associational information in which there's really basically the court -- no one's saying that there's a Fourth Amendment right there. And in fact, the

courts have held that the third party doctrine doesn't apply and that there is a heightened scrutiny required according to the First Amendment. And courts have in those kinds of cases -- and there are quite a few courts that have done this -- have, you know, narrowed the subpoena, required greater specificity. So, I think that's the sort of best set of those cases, but there are also a few other ones. So, for example, there's disagreement among courts about the question of whether or not if you have a enough for a warrantless arrest and it's pretextual or based on First Amendment -- based on speech, whether you have to have a higher requirement than probable cause, for example.

I also think that some of the cases that the courts are really struggling with right now under the Fourth Amendment -- the reason -- this is just my opinion that one of the reasons they're struggling with them is because there really are First Amendment implications that they're not addressing directly. So, I think Jones is a good example

of that. The smart phone case, Riley, is another example of that. They're talking a lot about these really First Amendment concerns in saying that there's a Fourth Amendment interest there.

MR. DEMPSEY: Professor Kerr, I sort of cut you off there. I just wanted to pursue this one point, but you were -- do you want to finish the thought that you were pursuing or had you?

MR. KERR: Sure. And maybe this is a way of reconciling Professor Strandburg's views and my own of where the cases are now. My sort of overall summary, when I think of how the First Amendment cases play out is that there's sort of a good faith test. It's like okay, investigators, were you really trying to enforce the law or were you solely trying to harass someone? And if you were really just trying to harass a group engaged in speech, then that raises First Amendment issues. But as long as there's some sense of no, this was actually some sort of law enforcement investigation or legitimate investigation, then

the First Amendment concerns become more of this kind of like okay, well, be careful if there are First Amendment issues, but probably no major doctrinal change.

And so, there's some role of the First Amendment but it strikes me as this relatively low threshold of almost a good faith kind of inquiry. That's my best --

MR. VLADECK: But even that is more than, under Verdugo, a non U.S. person would have under the Fourth Amendment in the context in which the First Amendment might apply with any more breadth.

MR. KERR: Yeah. Assuming the person has First Amendment rights but no Fourth Amendment rights.

MR. VLADECK: Right. At all.

MR. KERR: Right.

MS. STRANDBURG: And I would also say that this good faith investigation rule has generally not been the rule that courts have used in these association membership subpoena kind of cases. It's for undercover investigations mostly with a DC Circuit

exception.

MR. DEMPSEY: Hopefully a quick question for Professor Kerr -- on your equilibrium adjustment -- is that the right phrase?

MR. KERR: Yes.

MR. DEMPSEY: Yeah, okay. So, under the equilibrium adjustment theory, you sort of look at, to some extent, the pre technological analogue, if you can find one, so no privacy right in the addressing information on an envelope because it's on the outside, therefore no Fourth Amendment right in the addressing information on an internet communication, let's say. So, that sort of retains the equilibrium.

MR. KERR: Right.

MR. DEMPSEY: How does volume play into equilibrium adjustment -- that is, does an infinity of zeroes or a billion zeroes equal zero and, therefore, if there was no privacy interest in, you know, one calling pair, should there be no privacy interest in all the calling pairs for five years or -- ?

MR. KERR: I mean, I think volume can change -- it certainly creates pressures on the doctrine to come up with a different rule. And probably the best example is Riley versus California, the cell phone search case. So, amount of stuff that's going to be on a cell phone leads the court to say, wow, a cell phone search is a totally different animal than a search of a crumpled cigarette package in the 1970's and so we need a different rule for that. So, I think volume can play a role. A little bit of a different question -- if the issue is can a lot of non searches become a search at some point because then you run into line drawing problems of well, okay, what is that point and -- in Riley the court, I think, was very careful to say, you know, we're going to have a rule -- search incident to arrest is allowed for physical evidence; digital evidence, warrant requirement such as a simple -- everything or warrant requirement.

And it's a much more complicated issue when you start talking about okay, a lot of evidence collection or a lot of volume maybe

changes the rule. I think probably if the courts were to apply this approach, they -- maybe at some point they'd say the nature of this evidentiary collection is so different because of the technological era that this evidence collection is always a search rather than is never a search. Similar to something like Riley, but it's always going to depend on to what extent does the balance --

MR. DEMPSEY: Wait --

MR. VLADECK: But that's Alito's opinion in Jones; right -- that a whole bunch of -- Justice Alito's concurrent opinion in Jones is that a whole bunch of -- you know, 27 days' worth of things that by themselves wouldn't have been searches are a search.

MR. KERR: Although I take Alito's opinion in Jones to be that people don't think that their location is monitored for a long time -- at least when they're big narcotics traffickers, which, you know, it's a half page in a ten-page opinion that cites nothing. It sort of -- and I think it's sort of hard to know what Alito was thinking. And

in this context, too, Justice Alito, from his concurring opinion in the Riley case suggests that wherever there's some sort of statutory regulation or Congress has looked at this issue, he would say probably the Fourth Amendment doesn't apply at all. So that's another issue and another approach that you could take.

MR. MEDINE: Ms. Collins?

MS. COLLINS: So, Professor Strandburg, I wanted to ask you a couple of questions about where I think you've pivoted from what the case law is to what you've argued and specifically on the metadata question. And I think you said the test is, you know, if it's equivalent to a compelled disclosure and so, this would be critically implicated by bulk acquisition. So, I guess my question to you is: If you have a situation where I take the paradigmatic case to be an administrative action directed at a lawful entity for their membership lists. There's no purpose other than to obtain the membership lists of an entity engaged in lawful activity. But if you

take on the other side, a program that is directed to identifying counterterrorism groups, so this is, I would suggest, not protected activity or certainly not with the same level of activity. If you have a likelihood of collection that is 50 percent, a likelihood of eyes on it of 5 percent, a likelihood of subsequent dissemination or use of 1 percent, does that change your analysis in any way?

MS. STRANDBURG: So, I think the important point here is what is the effect on people's exercise of their First Amendment rights of whatever the government is doing here; right -- the government program here. So, I think that in a case where the government is collecting in bulk everybody's communications with no specificity, the effect is likely to be highly chilling, right, because the government has that information. And in that information is exactly the kind of information that the court in the Shelton versus Tucker case where the law that was involved said, you know, tell us all the

associations you belong to. It's essentially the equivalent of that.

MS. COLLINS: Okay. Can I -- I just want to make sure that my hypothetical is clear. So, if you have a situation, does it impact your analysis at all where we will assume even 100 percent collection of a wide range of individuals' communications or metadata -- let's stick with metadata because I think that's where you said that you're now arguing rather than describing -- but the likelihood that this information is ever accessed or reviewed or used in any way -- let's make it .0001 percent likelihood -- is it your position that that has the same or should be considered by the courts to have the same chilling effect as a request from the government for the names of individuals who belong to an association that is engaging in protected activity?

MS. STRANDBURG: No. However, I think that I'm kind of -- even though I'm a law professor, I'm going to fight the hypothetical a little bit because I think that how do we

know what the likelihood is over the long run of information being -- that is held by the government used for some purpose, you know, over a long period of time.

MS. COLLINS: So, the court should take into consideration the possibility that either the law would change or the policies would change --

MS. STRANDBURG: Or that people are -- there are bad actors. I mean, all of these things, I think, have to be taken into account. And then the second part of it, of course, is the fit between the purpose of the collection and the compelling government interest. So, if one could show that doing this was extremely effective and very necessary to do in order to address this interest, that wouldn't be the answer, but that would certainly be an important consideration in the balancing, I think, as it always is in the First Amendment context.

MS. COLLINS: So, what do you think are the most important aspects, assuming that there wouldn't be tailoring on the front

end, so a lack of specificity on the front end? Are there any circumstances -- and this follows along with what Judge Wald is saying -- that you could envision that a bulk collection program would nonetheless meet First Amendment heightened scrutiny? I think you're positing strict scrutiny or some form of heightened scrutiny.

MS. STRANDBURG: Right.

MS. COLLINS: So, is there any circumstances under which you could contemplate a program that is bulk, making it even more difficult for foreign intelligence rather than for counterterrorism purposes so you would have lawful activity and not necessarily purely unlawful activity?

MS. STRANDBURG: Realistic situation, I think probably no. And that's partly because of skepticism I have about the efficacy of what you can do with all of this data.

MS. COLLINS: Okay. So, it is -- there is no circumstance that you could envision of a bulk collection that would meet

your form of First Amendment scrutiny? There's no protections on the back end?

MS. STRANDBURG: I mean, it would depend on -- I mean, no circumstance, no realistic circumstance, I think.

MS. COLLINS: And I wanted to actually grind the other professors on this because it strikes me that there is room if we're sort of creating the law going forward for the courts to consider. Again, like a reasonableness test and to disaggregate the notion and the potential chilling effect of collection as opposed to use or dissemination or even eyes-on access because I think it's clear from publicly available materials that there is a huge gap between collection and the probability that any individual will have eyes on and just your thoughts as smart people as to whether or not the court should look as a First Amendment matter also at distinguishing between collection and subsequent potential access or use.

MR. KERR: Great. Make me go first.

MS. COLLINS: If there were another First Amendment person here, I would ask the other First Amendment person.

MR. KERR: I'm reluctant to express a view on the First Amendment as somebody who toils in the Fourth Amendment fields instead. But I think that a difficulty I have conceptually with a lot of the different chilling arguments is I think it's so hard to say what the standard is for what chills someone, especially given that most people have such a terrible misunderstanding of what the government is doing in both directions. So, it may be that people think the government is doing much, much more than they are. It may be that the people think the government is doing much, much less. And then you have, you know, what's the role of the press in reporting stories, what's the role of the government in what they disclose, what's the role of Congress? It's sort of hard, I think, to -- I personally find in thinking through how that plays out, it's tricky.

And the distinction between

collection and use disclosure, I think it may be that courts in the Fourth Amendment context start focusing more on the downstream issues. So, the current status of Fourth Amendment law, to go back to something I know something about --

MS. COLLINS: Well done.

MR. KERR: Thank you. Is to focus on the collection traditionally and it may be that that will shift over time and there will be more attention to use based on some sort of reasonableness standard. You can imagine different ways of kind of manipulating the doctrine to focus on --

MS. COLLINS: Isn't that already somewhat the doctrine, though? I mean, if you take -- or at least that's a series of arguments that's made that if you're looking at reasonableness, you do have to look actually at -- you know, in the absence of a warrant, that you do look at what are the downstream uses and what are the protections afforded to the data?

MR. KERR: It can be in some

context, although you always have to get past what is a search threshold and so that's -- you know, in a wire tapping setting, yes. In the searching a home setting, yes. But in a lot of the metadata issues that we've been talking about and they've been very much the focus in a lot of news stories, you don't get there because at least under current law it's not a search. And so, I think it may be that the courts try to come up with some way of saying there's a search if you get a combination of acquisition and use or some -- you can come up with ways that the Supreme Court might try to reconfigure this, you know, a decade, 20, 30 years from now. It's just lots of possibilities.

MR. VLADECK: Can I offer a response on the first --

MS. COLLINS: Please.

MR. VLADECK: So, I mean, first, I think there is a structural problem in First Amendment doctrine with regard to how you measure and quantify chilling. And I don't think that's in any way unique to the context

of chilling based on largely secret government programs. I think that's actually even for public programs. I think that's a doctrinal problem the courts haven't solved, but they've accommodated.

And second, building on that, I mean, I'm struck by the Second Circuit's decision in the Hedges case. This was a lawsuit brought by plaintiffs who claimed that the scope of the, what, 2012 National Defense Authorization Act was so broad in the detention authority it conferred that U.S. citizens could reasonably belive that they would be detained by the military for First Amendment protected activities. And there's a very, I think, thoughtful and, to my view, largely correct First Amendment analysis by the Second Circuit that explains at what point you cross the threshold from, you know, a reasonable reading of a largely secret government program to a reading that requires, you know, making every benefit of the doubt in favor of conspiracy theories. Right? And so, I think, you know, there is a way to actually operationalize this.

It's just, I think, based on what's public, what the public could reasonably believe based on what's public and I think that that's not inconsistent with more general principles of the First Amendment doctrine. I think that's what Hedges did.

MS. COLLINS: And back to the expert for a final word, please.

MS. STRANDBURG: Well, I was just going to say I think it also depends on what the alternatives are. So, if you have a situation where there are alternatives that, you know, maybe make it a little bit less useful, don't fix everything, but are much less intrusive, then I think that there the need for tailoring really is what controls

MS. COLLINS: Oh. So, when you said substantially less burdensome, you were dealing with the level of the intrusion or the --

MS. STRANDBURG: Yea.

MS. COLLINS: Okay. Thank you.

MR. MEDINE: Ms. Brand?

MS. BRAND: Thank you. I

actually wanted to follow-up on this. I'm glad this came up in Beth's questions because I was going to ask you about it, Professor Strandburg. A minute ago you said something about the level of chilling that made me think that what you're referring to is some kind of subjective understanding on the part of the public about what is going on. Is that what you mean? If the public feels chilled because they have some massively incorrect understanding of what's going on that it must stop? Or what? I agreed a little bit with what Orin said about the nature of misunderstanding because if you look at some of the currently discussed programs, you've got people, including politicians, out there saying things that are just flat wrong about what these programs are and what they do. So, how do we factor that into this chilling analysis?

MS. STRANDBURG: Yeah. So, I agree with Steve that this is an area that's sort of troubling for a First Amendment doctrine in general and part of the reason for that is that the standing doctrine is so tough

that you get very few cases where courts actually get to the merits to discuss the issue. But I think I would also say that it can't be that whatever crazy thing people think is what counts. So, there has to be some aspect of sort of what reasonable people would think, you know, what are sort of reasonable concerns that citizens might have. But that's just my, you know, sort of my take, I guess.

MR. VLADECK: Well, and if I may, I mean, I think the Second Circuit goes out of its way to say, you know, what is a reasonable belief based not just upon the language of the statute, but based upon public positions taken by the government; right? And so, you know, it's not actual knowledge; it's constructive knowledge, but I think that's not a foreign concept to courts in this context.

MS. BRAND: Okay. Go ahead.

MR. KERR: It strikes me that even that standard is really hard to apply, and in the Section 215 context is an interesting example. So, looking at the statute, I would have said before this known disclosures there's

no way that authorizes bulk collection. It's an obviously wrong reading of the statute and yet that is, in fact, what the government was doing. And so going --

MR. VLADECK: But you wouldn't have been chilled.

MR. KERR: Well, I mean, me personally wouldn't have been chilled or --

MR. VLADECK: If you couldn't reasonably have believed, based upon the plan under the statute that the government was collecting all the phone records, then how would you have been chilled?

MR. KERR: And so you would say Snowden is responsible for the chilling then?

MR. VLADECK: No. I would say as the Second Circuit said in Hedges --

MR. KERR: He's not a bad actor, so he personally didn't -- NSA contractor perhaps --

MS. BRAND: All right. Let's cut to the chase because I do have some other questions. Did you want to finish your --

MR. KERR: No. It's just a hard

question.

MS. STRANDBURG: Okay. Well, but I also think that chilling is maybe -- part of the problem is the term of chilling effects. I mean, chilling effects that are reasonable are sort of based on reasonable assessments of what could happen to you as a result of exercising your First Amendment rights. And that has to include things that can happen too if there are bad actors in the government as well as things that can happen to you if everybody follows the rules. So, you know, one way to look at it is that chilling effects are a way of talking about what are the things that could happen as a result of a particular program reasonably.

MS. BRAND: Okay. Orin, I want to ask you to follow-up on Pat's question. I was also intrigued by what you said about the reasonableness inquiry should be assessed at the point of collection. I was going to ask you to give me a hypothetical and then you did give one to Pat about the Belgian example. Does that hold up across the world? If we just assume arguendo that Belgian and E.U. law are

quite reasonable and protective of privacy, what about -- I don't know -- Zimbabwe or Cuba or Iran or Russia or China or any list of places where perhaps privacy and civil liberties are not so protected? Should we -- does U.S. law on reasonableness also incorporate the reasonableness of those locations?

MR. KERR: It's a great question. It's the problem with the foreign law standard, I think. It works nicely when you're dealing with a western country that has basically U.S. law and most of the western countries -- their surveillance laws and sort of search and seizure laws are actually quite similar to U.S. law. So, you know, it might be a slight difference in how a particular law is interpreted, but they're actually pretty similar. If you apply the foreign law standard, what do you do when it's surveillance of a pipe going underwater and there is no country or what do you do if it's from a satellite or what do you do if it's a war torn nation that has no government?

There's sort of two answers to that. One would be you could say, well, maybe the foreign law standard works in some kinds of contexts and doesn't -- it's just a general reasonableness approach in other kinds of contexts. That's maybe one. And arguably, that's what the Second Circuit did in its case that involved Kenya monitoring an Al-Qaeda cell, a U.S. citizen in Kenya, where they did not look to foreign law. They kind of noted that a foreign warrant was, I think, obtained, but it was just in passing. So, you're absolutely right. The foreign law standard has its own pretty substantial practice.

MS. BRAND: Then let me twist the hypothetical a little bit more and ask if that standard applies in all circumstances because 12333 is so broad, it affects so many different contexts that it's kind of hard to wrap your head around one general standard. It applies, for example, to collection of intelligence on the battlefield by a Department of Defense element. So, if you are -- if some DOD intelligence entity is collecting information,

say on the battlefield, about a U.S. citizen who has become an ISIS fighter, what then? It's a U.S. person, it's extraterritorial. What's reasonable? How do you figure that out?

MR. KERR: So, I would say first the foreign law standard would not apply for a bunch of different reasons. It's not a joint investigation, for example, and it seems that the foreign law cases have really been limited to U.S. and foreign governments working together and --

MS. BRAND: Ok, so not foreign law, then what?

MR. KERR: Not foreign law. And then you run into what is reasonableness. And so they're different answers. The courts have suggested -- the Second Circuit suggested sort of you weight the significance of terrorism in that case. In this case with the significance of the government's interest in effectively fighting a war and then you weigh that against the amount of the privacy invasion and, presumably, the war interest wins out.

So, it may be that there's no

Fourth Amendment issues at all in the battlefield context. It may be that it's general reasonableness and that's case by case. It may be that there's a reasonable suspicion charge. We just don't know what the answer is in that setting. It's not been litigated and just has not come up.

MS. BRAND: Professor Vladeck, did you have a thought on that?

MR. VLADECK: I mean, I think Orin's -- I mean, so I share Orin's view, first of all, that I think reasonableness is the touchstone there and then the question becomes what do we mean by reasonableness. I guess I'm a little nervous about a balancing test -- not in individuals cases, but in bulk cases. And so, my concern lies much less with individual U.S. persons who are subjected to individualized searches in foreign countries and more with how you apply a balancing test to mass surveillance. Because it's not clear to me how well the conventional reasonableness doctrine under the Fourth Amendment can handle what really is a very widespread, in some

cases, collection effort.

So, I'm much less worried about the individualized battlefield or non battlefield example where I think there actually is useful case law like the Second Circuit decision than with the quality of the different question of when you're not actually targeting an individual when you're doing it in bulk.

MS. BRAND: Well, speaking of bulk, I wanted to ask Professor Strandburg: You talked about data in the bulk context. You seemed like you were talking about all data being alike, and I wanted to ask you if you think in the First Amendment associational context there is a hierarchy of data like we have in the Fourth Amendment context. Because of Fourth Amendment law or, if you're outside the Fourth Amendment. By virtue of policy and statutory law, U.S. law treats more intrusive methods of collection differently, right? And you have -- the government has to meet a higher standard, it's harder to get, et cetera. Do you think the same applies in the First

Amendment context? And just to take it down to the lowest level of generality, if the government decided to collect in bulk local newspaper articles from local newspapers, which would have stuff like who went to the Lions Club meeting, so we would have associational information, but it's clearly public information, does that cause the same concerns for you as things that are considered to be more private?

MS. STRANDBURG: Yeah. So, I think it has to depend on things like whether the government is actually getting information that isn't already out there.

MS. BRAND: So, you would say public information is just outside of the concern, of your concern?

MS. STRANDBURG: Not necessarily because there is a point at which you can collect enough little pieces of public information and put them all together and get quite a different picture than anyone would have otherwise, like anyone would normally have just from looking at the public information.

MR. VLADECK: And that's -- I mean, isn't that the government's whole theory of CUI, right of Control of Unclassified Information? This is information that doesn't need to be classified on its own, but that when abrogated, can provide more of a picture than the government wants to provide?

MS. Brand: Yeah, exactly.

MS. STRANDBURG: So, and it's also what was underlying the case involving rap sheets. There was a case that said there's a privacy interest in rap sheets, even though all of the information is out there.

So, I wouldn't go that far. I wouldn't make like a categorical statement, but I think clearly it does have to matter and it has to matter whether the data implicates First Amendment concerns at all; right? The data could be something that doesn't tell you -- I'm trying to think of a good example, but -- and that actually comes back to the technology question because as technology changes, what you -- and this is one of the huge issues in the privacy field in general is that there's

been a longstanding effort to try to define what's private information. But as technology changes, the kinds of things you can infer using data mining and so on from information changes quite radically. So, information that, you know, would have been not private at all or not tell you anything about association, you know, 30 years ago might tell you a lot now.

MR. MEDINE: I want to pick up on that technology point and go back to that discussion that was going on before with Rachel and Orin about the locus of the collection. And we heard earlier about the unterritoriality of data. I understand why in some ways it's appealing to use the location of the collection as a sort of touchstone from prior jurisdictional application of law, but since this panel is about new technology in part, it seems to me if it's not antiquated that where the matter of information is collected it will be shortly. And should that really be the touchstone for how we analyze Fourth Amendment issues?

MR. KERR: Yeah. So, I think it

should be and I disagree with Professor Daskal's approach for a couple of reasons. One is that if you're going to say that reasonableness should not be connected to data, you need to come up with some answer as to what the standard is or Fourth Amendment standard; right? And so, my sense is that those who would say that territoriality should not matter would say, well, let's bring everything up to the -- no one wants to bring it down; right? No one wants to say, well, it's on the internet, it has no location, therefore the government can get it. Instead it is no, no, no, no, we want to make everything the U.S. standard and let's bring it up everywhere around the world. And then I think, well, okay, that is basically a way of just having a universal warrant standard or something like that and we should debate that on the merits, but that strikes me as the implication. You know, one rule for all of Earth is a pretty -- I think a remarkable answer. In part because of the implication -- of the concerns in the Verdugo-Urquidez opinion, which talked about

the warfare context or talked about national security, national interests, the notion that the U.S. is different, the political community is different, we're enacting rules and police investigating cases and having government interest to protect us and to investigate cases with the ultimate goal of deterring crime and deterring wrongdoing and that that just is a different issue in the domestic context and in the foreign context.

It does raise, I think, a lot of difficult conceptual issues of what the standard should be and maybe you get sort of one -- I tend to focus on the criminal context and I think you get kind of one -- you get a workable regime in the criminal context because most of its going to be done through mutual legal assistance anyway. Even if there's no Fourth Amendment issues at all, it's ultimately going to be done through these international negotiations and then you've got a very different set of implications in the national security context when maybe it's with a cooperation with a foreign government that's a

friend, maybe it's a unilateral action that just sort of plays out very differently.

But I tend to think that despite the global nature of data, those territorial concerns are still very real and still very important in that that territorial approach still should be maintained.

MR. MEDINE: Professor Vladeck, do you concur with that?

MR. VLADECK: So, to a point. I agree that territoriality is relevant to the question that you're asking. I guess I just fear for reasons that Professor Daskal raises in the article that we're putting too many eggs in the territoriality basket. And part of that has to do with volition. So, most of the Supreme Court's territoriality doctrine is premised on the notion that individuals were making voluntary choices about where to be, about where to locate things, about where to store things. And with data, that can be true, but it's often not necessarily true.

So, for example, if you're a U.S. citizen living in the U.S., residing in the

U.S. but it just so happens that all of your e-mails are stored on a server overseas and that they can only be accessed from overseas and you don't care if it's archived, you might be surprised to learn that the government doesn't need a warrant under the Second Circuit and Ninth Circuit approach because the data is overseas.

So, you know, I think that Orin is certainly right that the answer cannot be a Fourth Amendment to rule them all, but I think that there is a lot of gray area between the categorical off switch of Verdugo and the categorical on switch of, you know, any access to the U.S. anywhere gets you full Fourth Amendment protections. And I'm not sure why we should be so afraid of trusting courts as they do in every other Fourth Amendment context to strike the balance in that situation.

MR. MEDINE: Professor Strandburg, I want to push you to the limits with the First Amendment and see if you'll go there, which is there is a -- from the prior discussions suggests a lack of territoriality

to the First Amendment and maybe even some questions of whether non U.S. persons may have First Amendment rights. In the context of U.S. surveillance programs overseas of non U.S. persons, which could chill those non U.S. persons' speech association rights and then, as a result, deprive U.S. persons of the right to receive information from those, do you see a First Amendment constraint on the government's activity in that context?

MS. STRANDBURG: So, you noticed I carefully avoided that in my remarks -- partly because I think that, you know, for the most part, it's hard to make the argument that non U.S. persons have First Amendment rights, I mean, except in the kinds of situations that Steve mentioned earlier, you know. But when they're just there, they haven't come here, they have, you know, nothing to do with it, I think that would be a big stretch and I think it would also be extremely hard to implement and probably also have what I think is the undesirable effect of ending up with watering down the First Amendment rights of U.S.

persons.

MR. MEDINE: Although again, is it affecting U.S. persons' rights to receive information if you're chilling the speakers' ability to speak?

MS. STRANDBURG: Right, right. So, you know, I think that seems kind of farfetched to me -- your particular hypothetical -- so I would say, no, probably not. I don't know if one could come up with a hypothetical where the reasonable chilling effect on U.S. speakers would be significant enough that it would really be the rights of the U.S. persons that you would be concerned about. But again there, I think it would be the focus would be on the rights of the U.S. persons. And off the top of my head, I don't have such a hypothetical, but there could be one.

MR. MEDINE: Professor Vladeck, getting back to the Fourth Amendment, if the United States is conducting surveillance overseas, and again, we talked about this earlier, where there's maybe incidental

collection of U.S. persons, what are the Fourth Amendment constraints on that -- on the collection activity or are the constraints more related to use, dissemination, retention? And, again, sort of maybe pushing things to the limits, if U.S. wants to engage in collection activity overseas without a foreign intelligence reason of non U.S. persons, just bulk collection to see what's going on without any suspicion or targeting, but knowing that that will inevitably collect U.S. person information, are there constraints on the U.S. government's surveillance activities under the Fourth Amendment?

MR. VLADECK: Sure. So, I think the part of what Judge Sand was struggling with in the Bin Laden case was in a true internal collection case, in theory the collector doesn't know that they've accidentally collected something until they've collected it. And so, there is no way meaningfully to anticipate the incidentalness of the collection. And in that context, of course were there to be any Fourth Amendment

implications, it would have to be on use and dissemination -- not on collection because the collection's already occurred.

What Judge Sand was worried about -- I think rightly so -- was in the context in which you know that you are going to incidentally collect. Shouldn't there be some constraints on the front end? The problem is I'm -- perhaps Orin is familiar -- I am unfamiliar with any cases since Bin Laden where that's expressly come up. And so, I don't know that there's case law on the subject. I have to say my own sort of view is that that distinction is one that makes sense to me analytically -- that if the government is truly stumbling upon information versus just not targeting but knows that they're going to collect anyway, that that maybe ought to have Fourth Amendment consequences.

And so, with regard to your second question about collection overseas, I mean, I do think there are Fourth Amendment consequences. Because of the Second and Ninth Circuit decisions, perhaps there's no warrant

requirement if you are known to collect on U.S. persons overseas, but maybe then the question is is incidental collection reasonable? And that answer might depend on technology. Is it impossible to collect what you are clearly legally entitled to collect without some incidental collection? And if the answer is yes, then perhaps maybe that's reasonable. So, that's how I would cash that out without knowing sort of the details of what exactly the capabilities are.

MR. MEDINE: All right. And Professor Kerr, one final question: Is there a foreign intelligence exception to the Fourth Amendment?

MR. KERR: Foreign intelligence exception to the Fourth Amendment.

MR. MEDINE: Exception to the warrant requirement.

MR. KERR: I mean, I would think so. I think that's probably the most consistent reading of the cases -- that the warrant requirement would not apply in the foreign intelligence context. You're talking

domestically that's what most Circuits have held and that's certainly a plausible answer. But doctrinally, we just have those Circuit Court opinions from the '70s and that's all we have at this point.

MR. VLADECK: Which all require a primary purpose.

MS. WALD: We have been told that we have a waiver from whoever the highest authority is in this operation because we've come in 15 -- well, 10 minutes ahead of our schedule. As a result, each panel member gets two minutes to have a discourse.

I have one question for Professor Kerr: Having read your equilibrium adjustment article and hoping I understood it, I thought you said at one point that when technology changes and new programs that weren't contemplated by Congress, when it's a statute that's involved, are not a good fit for the statute that's relied upon to authorize them the intelligence community should go back to Congress and seek approval for the new program. That seems to -- if that's the right

interpretation of your argument, it seems to be in accord with Judge Lynch's opinion in the Second Circuit case, but how would we apply that concept, if I've got it right, to E.O. 12333 where there's no underlying statute? Does it suggest a strong need for the regulations to be periodically reviewed and updated with perhaps more consistency than we have had to date?

MR. KERR: Yes. So, this gets to the question of really how the Foreign Intelligence Surveillance Court should have construed Section 215 and I think it's appropriate for the Foreign Intelligence Surveillance Court to apply what I call the Rule of Lenity basically saying if the -- basically, some clarity is needed before a court should interpret a law as authorizing this broad collection program. And so, that is consistent with Judge Lynch's opinion for the Second Circuit. I certainly agree with the underlying merit interpretation.

In a context where Congress has decided not to regulate, as you indicate,

there's no statute to interpret for which there should be a rule, you know, for which lenity could apply. The easy answer to is that you should have an Act of Congress -- that is theoretically possible

MS. WALD: Well, how about the regulations? We do have a whole bunch of AG regulations on E.O. 12333 supplemented by every departmental who's involved regulations. Is there any sort of internal requirement that, you know, they want to do a new technology program, it doesn't exactly sort of fit what they've been doing. Do they have any responsibility to put that sort of out in the -- not identify the program, but get approval for the program?

MR. KERR: I don't know about approval. It's not enough of a context that I'm personally familiar with enough. But certainly given that technology is constantly changing and the implications of preexisting rules and programs are changing, you'd want to have continual oversight to see, you know, this is how the program worked five years ago, let's

see how it works today because the answer could be really different.

MR. MEDINE: Mr. Dempsey?

MR. DEMPSEY: So, a question for Professor Kerr, which is: I think you've written about -- I'm putting my own gloss on it -- that in the computer search area or possibly in the technological data search area, the warrant alone is not enough for at least -- even with a warrant you get so much information that a search still might not be reasonable if the government collects more than would be reasonable. Any indication that the courts are moving in the direction of looking at that? I remember there was this case involving what I refer to as the other CDT, which was the drug testing, the Barry Bonds steroid thing, and then there was that Ninth Circuit opinion and then it was withdrawn and it was replaced by something much more general. But in the past two or three years have the courts begun to look at the downstream use of data and any indication that merely having a warrant, which would say give us everything and everything

might be far, far, far more than ever before, including lots of things that are incidental, any progress on that, any signs of where the courts might be going?

MR. KERR: There have been a few developments. First, two courts have suggested that perhaps there should be a cutting back on the plain view exception for digital evidence without directly answering that. And that was what I had written about in a 2005 article. The Second Circuit and the Massachusetts Supreme Judicial Court both said maybe we need to rethink this and then remanded the case back to the trial court, so we don't have answers yet.

And then also, more recently, I guess last year, the Second Circuit decided a case called United States versus Ganias involving the government had over-seized evidence in a computer search, held onto that evidence, a person's evidence that was stored on a government storage device. Years later the government had probable cause to search that held file again and the Second Circuit

said you can't go back and search that, even with new probable cause, effectively creating a use restriction, which is that whenever the government is collecting, over-collecting because the nature of computer searches is that they're so broad. That's sort of hermetically sealed off, even from a subsequent search based on probable cause. So, that is, I think, the most remarkable development along these lines. It's, again, this thinking of, you know, yes, the government can get a search warrant, but just having the search warrant doesn't mean that they can do anything they want. There are actually restrictions on when they can go back or maybe plain view with the latter. We're not sure of that yet.

MR. MEDINE: Ms. Collins?

MS. COLLINS: I wanted to go back actually to something you all were exploring when Rachel cut you off, unfortunately, which is what is rule of misinformation in addressing the chilling effect and how should courts and -- Professor Strandburg, I would love your thoughts on, you know, what should a court do

if there is a general belief in what the government is doing and there is an impact on the plaintiff's conduct but they're absolutely wrong about what the government is doing? So, they have been chilled?

MS. STRANDBURG: Yeah. I mean, that's just a very tough one and I don't know that I have -- I mean, especially if it's something where a large number of people -- I mean, if it's a few crazy people on the edges, that's one thing; right? But if it's where a large number of people -- I mean, the easy answer is well, the government should tell you things, tell you the information that you need to know so that you know that this is not what they're doing. I would think that in many circumstances, that's probably possible, and that would certainly be my first choice way to address that problem.

MR. VLADECK: And that's exactly what happened in Hedges. I mean, so in Hedges, the District Judge issued a nationwide injunction based upon the plaintiff's, in my view, rather speculative assessment of the

government's intention authority. And the Second Circuit basically, you know, made it worth the government's while to clarify its position in its briefing and then relied heavily upon the government's position in its briefing and the government's disclaimers of some of the specific findings the District Judge had made about the scope of the authority in explaining why there was no real chilling effect. So, I think it's not only possible; I think we've seen it in a national security case.

MS. COLLINS: And what is the role of the potential government bad actor because I actually sort of saw expressions going different ways to the notion that a court should consider or should assume that there may be bad actors within the government who will misuse information once the government has the information? So, is it your position that the court should presume that there will be bad actors?

MS. STRANDBURG: I think the court should take into account the possibility

that there may be bad actors -- not presume that there will be, but take into account the possibility that there may be. I think that that has to be the right answer given everything we know from history -- both our history and the history of other countries with respect to surveillance. So, yes, I think that one has to assume that and I think that not in this context, but in the context of the perhaps it exists or perhaps it doesn't due process right to information privacy, courts have taken into account what are the things that the government has done to make sure that there won't be bad actors that are able to make use data.

MR. VLADECK: I mean, I think the question is just is it reasonable to believe that, you know -- is it reasonable given the program to believe that government officers will overstep? And, you know, we actually have legal doctrines that are based on the assumption that at least in some circumstances government officers will cross the line. You know, qualified immunity wouldn't be that

exciting without that assumption.

So, I think the question is simply: Is the belief reasonable on the part of the listener that misconduct might occur?

MR. MEDINE: Ms. Brand?

MS. BRAND: I will retroactively give Beth one minute of my time, and I will try to take just one minute since you guys went over on that one. Just going back, though, to the question that Beth asked, it can't be, can it, that chilling and the First Amendment implications of a government action depend on subjective public intent? I just don't see how that can be. And it's interesting -- this Hedges case -- you know, the government making a factual statement in a judicial filing in court -- that may educate the plaintiff in that case. It probably doesn't educate the public, depending on how much press it gets or whatever, but then that becomes a very subjective analysis right.

MR. VLADECK: It's worth reminding ourselves that the Obama administration's definition of who could be

detained under the AUMF was promulgated in a brief filed in the DC District Court. So, I think I would certainly agree with you in the general typical case that court filings do not make public statements. I think in this sphere, though, they have.

MS. BRAND: Well, I think you're conflating an issue about whether policy should be made in a brief or whether a factual statement in a filing in a court has some effect on the public's subjective understanding of what the government is doing, and therefore whether the public is chilled. So, it has to be either, I think, limited to the objective understanding or at least the information made objectively available to the individual plaintiff, or it has to be some kind of objective standard, which is, of course, what we have in the Fourth Amendment context.

MR. VLADECK: I was never trying to suggest they should be subjective.

MS. BRAND: No. I wasn't -- I was directing that more to Professor Strandburg. But what is your --

MS. STRANDBURG: Yeah. I'm not suggesting subjective, either, but I am suggesting what a reasonable member of the public would think, which might not be identical to what's actually going on. So, I think that there is a potential difference there.

MS. BRAND: How does a court decide what a reasonable member of the public thinks?

MS. STRANDBURG: How does the court decide what a reasonable person does in anywhere. I mean, this is -- you know, this is something we do all the -- that courts do all the time. Arguments on both sides evidence and --

MS. BRAND: All right. My time is up.

MR. MEDINE: Professor Strandburg, it doesn't seem as though the First Amendment has really imposed a significant constraint on government surveillance activities, say, in contrast to the Fourth Amendment. Do you see that developing because

on the balance national security ends up carrying a lot of weight, even under a strict scrutiny standard? Do you see that changing at all or are there arguments to be made to give the First Amendment more of an impact in regulation in this area?

MS. STRANDBURG: Well, I think it is changing. Now, whether to the extent that First Amendment considerations are beginning to inform what courts are doing under the Fourth Amendment more. Whether that is the way it will go or whether courts instead will recognize more specifically as, you know, they have in certain areas like these subpoenas and so on, that there is a more direct effect of the First Amendment. You know, I don't know. My personal view is that it would be better if courts did that because it would bring up the issues that courts are really worrying about in some of these cases and allow them to be dealt with directly.

MR. MEDINE: Thank you. Any other comments? Okay. Thank you very much to the panelists. We appreciate your thoughtful

responses. We're going to take a 15-minute break and start sharply at 3:00 since lots of people in the room and on the stage have travel arrangements, so we're going to start promptly at 3:00. Thank you very much.

- - -

(Whereupon, a short recess was held at this time.)

- - -

MR. MEDINE: Attention. Hello. The Chair is speaking. I need a gavel obviously. We're going to begin the third and final session of today's meeting on Executive Order 12333 In Practice.

MS. BRAND: Thank you. I'm Rachel Brand and I'm going to be moderating the third and final panel of the day, which we've entitled Executive Order 12333 In Practice, which will examine how the Executive Order, other law and policy, governs how the intelligence community collects, retains and disseminates information about U.S. persons. It will also examine the mechanisms that the Executive Branch and Congress have put in place

to oversee activities conducted pursuant to the Executive Order.

So, just to -- mainly for the benefit of the panelists, to tell you how this is going to go logistically in case you didn't see the previous panels, each of you will have up to seven minutes to give your opening remarks. There is a yellow card in the front row. Rebecca has it at the moment. So, when two minutes are remaining in your time, the yellow card will go up. When the red card goes up, your time is up. And then, so what I'm going to do is I'm going to first introduce Michael Allen, and after you're done speaking I will introduce the next panelist, and so on. I intend to be brutal on the timekeeping because a number of us have to catch planes. So, if I cut you off in mid sentence, no offense. It's just a matter of timing.

So, our first speaker today is Michael Allen. He is the managing director of Beacon Global Strategies, L.L.C. From 2011 to 2013, Mr. Allen served as Majority Staff Director of the House Permanent Select

Committee on Intelligence or HPSCI. Prior to joining the HPSCI, he was Director of the National Security Preparedness Group, which was the Bipartisan Policy Center's successor to the 9/11 Commission. Mr. Allen additionally served in a variety of roles in the White House, including a variety of roles in the National Security Council. Thank you for being here.

MR. ALLEN: Thank you so much for the introduction, Rachel. Mr. Chairman, thank you and the PCLOB for having me here today. I'd like to focus my remarks on the state of Congressional oversight of the intelligence community. The activities of the IC are absolutely critical to our national security. Intelligence is the lifeblood of our decision making process. It's very important, of course, for our soldiers to be able to see over the next fox hole. It's critical for presidents to receive national intelligence on everything from ISIS to the Iran nuclear program. And, of course, its core most important function is indication and warning. And so, I applaud you all for taking on these

topics in the seriousness with which you treat it.

While intelligence is critical to national security, oversight of the IC is among the most important functions in our democracy. The President is asking the men and women of the IC to put their lives on the line and do very dangerous things for their country. But to be able to perform these tasks, the IC needs the support of the American people, whose interests are represented by the members of Congress, serving on the House and Senate Select Committees on Intelligence. Because some of the IC's activities are controversial, the oversight committees are obligated to scrutinize the activities of the IC to ensure they're consistent with our values. This is among the highest duties that the Congress has in overseeing the Executive Branch.

There are many misconceptions about Congressional oversight of intelligence. Many of the academic papers and books, I think, miss the boat altogether. This is in part, naturally, of course, because the Intelligence

Committees necessarily operate in secret, as the Constitution actually contemplated, but my experience working with and for the Intelligence Committees over the last decade has convinced me that members of Congress largely take their oversight responsibilities very seriously.

I'd like to review what, in my humble opinion, are several hallmarks of effective Congressional oversight. The first is the annual authorization bill. So much of the academic literature out there does not appreciate what exactly the Intelligence Committees do. They perhaps look on Thomas and find a very short unclassified intelligence bill and say to themselves, well, there's nothing here. In reality, the Intelligence Committees draft a classified annex that travels with and is attached to the actual annual authorization bill. This is the engine of Congressional oversight. It directs -- it gives direction on specific programs, it fences dollars until certain conditions are met, it sets personnel level and it actually sets

ceiling on -- dollar ceilings on certain programs and, of course, for certain agencies. Congress for a time -- from 2004 to 2011 -- did not or was not able to enact an annual intelligence authorization bill and I think Congressional oversight suffered as a result. Luckily, we were able to restore that practice in recent years and I think that is all for the good.

The reason is, of course, is that while it's very important what members of Congress say -- and I do believe the Executive Branch responds to members of Congress -- Congress needs to be able to give force so that it can pass legislation to back up what they say in law. I think the intelligence community notices when they go up to the Hill, if the committees are not getting along or can't do their job or are dysfunctional and don't pass an authorization bill every year, I think they smell weakness and I think they might be able to think, well, I have to endure a beating up here in a hearing. But at the end of the day, I know they can't do anything about it.

The second, I think, crucial hallmark of what the Intelligence Committees do for oversight, which, again, I think is under-appreciated are the hearings that the committees do. We're used to this as Washington people. We see so many committees every day, so many committees doing a variety of different hearings every day. Secretary Rumsfeld actually visited the HPSCI a few years ago and he was, of course, occasionally famously in an oppositional role to Congress, but he reminded us on the HPSCI, or at least the membership, the power that they have to have a hearing, it sets an agenda for the Executive Branch. In many cases it causes most of the members, at least in the particular subject matter area, to drop what they're doing and to get ready for a hearing. It forces bureaucratic stases to be addressed and very often policies to advance.

So, in the House Intelligence Committee we had at least two hearings a week and many other one-off briefings and other hearings, as the case may be, and I think that

benefitted enormously and I think oversight benefitted enormously from that.

Another key aspect is leadership and membership of the committee. Key to effective oversight is, of course, bipartisanship. Congress speaks louder when they speak together. And again, of course, if they're sending conflicting messages to the intelligence community, I think oversight by and large would be harmed.

Also, an active membership is absolutely key to Congressional oversight. Members have to invest the time and they have to invest a lot of, frankly, time when they're not in front of the camera or doing things with their constituents to be able to come down to a skiff and learn about the complex 17 agencies of the intelligence community. But that's not to say our oversight structure is perfect. Well, I should say as an aside, it is the envy of the world. Annually the equivalent -- the British equivalent of the Intelligence Committee comes and visits us and they marvel at what the House and Senate Intelligence

Committees have in terms of access to information sources and methods. And an Australian trip revealed much of the same thing, so I think we're the envy of the world. Congressional -- the oversight, of course, is vast. I think we could probably work in many ways to make sure that we had more staff with professional and technical backgrounds to be able to tackle this stuff. I'm happy in the Q&A to go over how we staffed each aspect of 12333 and the collection programs.

But finally, I think the last thing I'll mention is that another way to strengthen Congressional oversight is for the National Security Council to resist the impulse to limit who gets briefed in on what program. For example, often the gang of eight is invoked too frequently and I think we should do less of that so more members feel empowered and have access to information. I'll stop right there.

MS. BRAND: Thank you very much. Our next speaker is Timothy Edgar. He is a visiting fellow in International Studies at Brown University's Watson Institute for

International Studies and has also taught at Georgetown University Law Center. Mr. Edgar served under President Obama as the first director of Privacy and Civil Liberties for the White House National Security Staff. From 2006 to 2009, he was the first Deputy for Civil Liberties for the Director of National Intelligence. Thank you for being here.

MR. EDGAR: Thank you very much, Ms. Brand and Chairman Medine. I'm pleased that you're examining this issue, Executive Order 12333, particularly because of the importance of the activities that are conducted under this order. My perspective on these activities has been shaped by my experience inside and outside of government in ensuring that national security activities are constrained by privacy and civil liberties safeguards. So, in addition to my government experience, I was also an attorney at the American Civil Liberties Union. So, I understand the perspective of the outside advocates as well. And I would say that the job of lawyers and privacy officials inside the

intelligence community is really mostly to administer the two basic systems of oversight that were first established by the Church Committee Reforms of the 1970's -- the Foreign Intelligence Surveillance Act and E.O. 12333. And of these two, in my experience, E.O. 12333 is by far the more important of the two, even though it receives less attention. And that's because FISA has a definition of electronic surveillance that is very specific as to where and how information is collected. It requires court orders, it involves considerable effort by government attorneys and involves all three branches of government in oversight. So, there's a lot of oversight involved when you get the FISA court involved.

On the other hand, E.O. 12333 governs everything else. Those that are not regulated by statute do not require a court order and as a result, as a practical matter, these activities are less transparent, even when you look at the standards of classified programs. And that's because they're less well documented and they involve less people really.

Realistically, they usually involve just the Executive Branch, although Congress often does get involved in oversight of the activities. There's just so many of them and across such a wide array of programs that it's difficult for Congress to oversee them without the kind of prompt that FISA provides.

Since the Snowden revelations began in 2013 there's been a lot of debate here as well as abroad about surveillance reform. While much of the debate in this country has focused on bulk collection of telephone records and other FISA activities like prism, in the rest of the world the attention has really been on the continuing revelations of a variety of NSA activities that are conducted overseas under E.O. 12333. These include reports of very intrusive activities like collection of massive quantities of communications -- the practice the government calls bulk collection and that critics call mass surveillance -- as well as alleged activities that undermine encryption or securitive communication systems. These are all areas I think that you should be

considering looking at.

President Obama has actually addressed many of the concerns or some of the concerns about privacy and civil liberties in intelligence collection and signals intelligence collection under Executive Order 12333 in Presidential Policy Directive 28, PPD 28, which we haven't talked about much this morning. Hugely important as a matter of policy and as a matter of law, it limits bulk collection under any authority for signals intelligence to six specified national security threats. Those are counterintelligence, terrorism, WMD, cyber security, threats to military forces and transnational crime. Those are all very important topics, but that's a relatively narrow slice of the total topics that are usually covered in foreign intelligence collection. And it also does things like saying that the government needs to consider the privacy and civil liberties of everyone around the world -- that is, foreign citizens -- in deciding whether to go forward with signals intelligence. That's a pretty

soft requirement. You just have to consider and weigh these. But that's still pretty important. That's really quite significant because when I was in government, both at the White House level and at the ODNI, this simply wasn't a consideration. There was no Presidential Directive or policy that said, hey, this activity may be producing some intelligence, but when you compare it to the huge impact on the privacy of a very large number of people overseas, it's not worth it. That just didn't compute. Privacy of people overseas didn't count. It wasn't covered by Executive Order 12333. It wasn't covered by FISA. It wasn't covered by other statutes. Now it does under PPD 28.

It also includes this language, which came to mind when we had the discussion of the First Amendment in the last panel. The assumption in that panel was really when we're talking about the First Amendment, it's really we're talking about U.S. persons. Yes, certainly, but under PPD 28 there's at least a nod to the interests of foreigners when it

comes to First Amendment type rights as well as other things. PPD 28 contains this language: The United States shall not collect signals intelligence for the purpose of suppressing or burdening criticism or dissent or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation or religion. This is a sentence which applies to everyone around the world -- not just to American citizens. I discuss some of this in an article which I have also left out on the table following the advice of Professor Slick.

So, the question really I think you need to look at is very welcome and very timely. I have asked -- in my written statement I have suggested there are several examples of factual issues that you could be helpful in. One is how effective have programs under E.O. 12333 been in preventing terrorism? I think this is going to be a relatively easy case for the government to make, but I still think it's worth it for you to make them make that case. We'll learn a lot about the importance of those activities as well as any

pitfalls.

The other is what percentage or proportion of the government's efforts under E.O. 12333 have been directed at preventing terrorism versus other national security priorities or other foreign policy priorities? This limitation of bulk collection I talked to you about -- that was six threats. So, I think that's useful. It would be helpful to the public to understand is this 50 percent of what the intelligence community does? Is this 80 percent? Is it 10 percent? This can be helpful to understanding the impact on privacy.

And then are there limits beyond what's in PPD 28 that should be put on particularly intrusive activities such as bulk collection and what about this undermining encryption and security? That's a subject which PPD 28 doesn't cover, but which recommendations by the President's Review Group were made and I think that's an important issue.

And then really how has PPD 28 actually affected intelligence activities under

E.O. 12333? Its early days, PPD 28 was only signed last year. It was implemented earlier this year. But I think it's worth taking an early check-in to see has this changed practice, has it helped just codify what the government was already doing. That may impact what we think the government was doing.

MS. BRAND: Thank you.

MR. EDGAR: I see I'm out of time.

MS. BRAND: You're out of time. Thank you for observing the clock. Our next speaker is Mieke Eoyang. She is the National Security Director at the Third Way. Prior to joining the Third Way, Mieke had a long career on Capitol Hill, most recently serving as Chief of Staff to Representative Anna Eshoo. From 2007 to 2010, Ms. Eoyang served as a professional staff member on the House Permanent Select Committee on Intelligence. From 2002 to 2007, Ms. Eoyang was the Defense Policy Adviser to Senator Kennedy and before that was a professional staff member on the House Armed Services Committee. Thank you for

being here.

MS. EOYANG: Thank you, Commissioner Brand, Chairman Medine, Commissioners Collins, Dempsey and Wald. Thank you for inviting me. First I'd like to say I agree with everything that Michael Allen said and I cannot emphasize that enough in terms of the seriousness and the importance of Congressional oversight and the seriousness with which members approach their task. In the interest of not repeating that, I am going to focus my remarks on the limits of Congressional oversight -- in particular, as members of Congress understand the limits of intelligence oversight in comparison to their oversight tools that are available to them on other national security committees, having served on both Intelligence and Armed Services.

There are some differences between the tools that the committee staff and the members have available to them when they conduct oversight over the intelligence programs. First, we often hear that from members of the intelligence agencies that

Congress has access to everything -- or Congress sees everything. And I want to just first draw a distinction between having access and the ability to see everything and actually being able to see everything. The assumption that Congress has seen everything that the intelligence committee does and therefore has approved of it is both logistically impossible and I think factually incorrect and an unfair assumption about Congressional oversight. A $70 billion enterprise, as discussed in the last budget submission, it's just too large an enterprise for the staffs of the two committees to get their hands around completely.

The other thing is that Congressional review is not a guarantee of either civil liberties protections or Constitutional sufficiency. And for good reason, members of Congress, when they're approaching these programs, are often thinking first of their effectiveness at protecting the country and, second, of the budgetary effectiveness and good stewardship of taxpayer dollars. Civil liberties concerns and privacy

concerns are a question for them, but they may not be the primary or secondary concerns. It may be tertiary or even lower than that, depending on what interests are at stake.

Then in thinking about those issues, Congress doesn't always get to review the legal basis for programs. There's an assumption -- there's often assumption that programs that come under 12333 that it's such a well established Executive Order that you may not go back and review the legal basis on which those programs lay. We have seen and there have been public reports of times in which members of Congress were not given the legal opinions that would underlie some intelligence programs. My understanding is recently that's changed, thought I would say that being on the Intelligence Committee's a little bit like being in the movie Memento -- you only know the time period in which you're there. Michael Allen and I did not serve at the same time, so we may have different -- slightly different perspectives on the ways in which the relationship worked.

But most importantly, the Congressional Intelligence Committees do not have full access to the range of oversight tools that are available to other national security committees -- sometimes for good reasons. Because of the sensitivity of the programs involved, Congressional tools like the Congressional Budget Office or the Congressional Research Service or the American Law Division of the Congressional Research Service are not available to them for their expert analysis on those programs. Reading in that many people would be problematic and a risk to security. However, the committee had made an attempt while I was there and I know it has worked with intelligence agencies to try and get the General Accountability Office in to be able to conduct the kinds of financial audits and systemic audits of functions of the intelligence community that the committee staff themselves are not properly resource to be able to do. For a long time the intelligence agencies were resisting that kind of oversight and I'm not sure whether or not the committee

has ever successfully gotten GAO to come in and do an audit of a program. However, if you look in the most recent National Defense Authorization Act, the Armed Services Committees regularly use the GAO to review highly classified intelligence programs and the results of those audits may remain secret and classified, so only available to appropriately cleared audiences.

The other challenge -- one of the other challenges that the Congressional intelligence committees have is their access to whistle blowers. There has been a fair amount of Congressional debate about the intelligence community Whistle Blower Protection Act and whether or not that actually encourages or stifles Congressional whistle -- or whistle blowers from coming in to Congress. There have been public reports of whistle blowers who have said that their treatment and the difficulties they've had coming to Congress inside the classified spaces have led them to go to the press, which in many cases can be very harmful to national security. If Congress had a

clearer path to whistle blowers, it is possible that people would not bring those to the press. But part of the challenge of having an effective whistle blower regime in the classified environment is that it is difficult to communicate back to the community of people who might be able to uncover waste, fraud and abuse that their concerns will get adequately addressed when they are addressed in secret and behind closed doors. However, the perceptions of some whistle blowers based on the treatment of others that were public has certainly suggested that there is a chilling effect of whistle blowers not coming to the community.

And then the other thing is that the members of the two intelligence committees are not equally situation when it comes to intelligence oversight. The House intelligence committees are staffed by a core staff which is controlled by the chairman and ranking member. On the Senate side, individual senators will have their own designee who is cleared in addition to the core staff. That means when members of the Senate disagree with the

position of their chair or ranking member, they can have the assistance of a staffer to help them wade through the legal or technical issues to help them given all the other demands on their time. The House has chosen under House rules not to have that system to provide a cleared staffer to the members of the House Intelligence Committee, providing those resources costs would increase the legislative branch appropriation, so that's a larger decision. But they are not equally situated that way.

The Senate also has a technical support working group. And during my time there, the House did not have access to a group of cleared independent intelligence experts who they could turn to for advice on the technical nature of programs. You have to remember, these members are not automatically familiar with intelligence programs, the business of national security or experts in the law, so they need some additional expertise to help them.

And then the House and the Senate

are differently situated when it comes to access of the entire body to seek classified information. House rules set up a very rigorous process for members not on the committee to seek classified information that's in the control of the Intelligence Committees. The Senate has as a practice allowed all Senators to see that. So, thank you.

MS. BRAND: Thank you very much. Our last speaker of the day is Matt Olsen. He's a lecturer at Harvard Law School, an ABC News contributor, and cofounder of a cyber security technology firm. From 2011 to 2014, Mr. Olsen served as Director of the National Counterterrorism Center or NCTC. Prior to joining the National Counterterrorism Center, Mr. Olsen was the General Counsel of the National Security Agency. Mr. Olsen also served as the Deputy Assistant Attorney General for the Justice Department's National Security Division. That was from 2006 to 2009 -- sorry. And he also served as a federal prosecutor for over a decade. So, thank you for being here.

MR. OLSEN: Thank you very much

and thank you to the Board for inviting me and for your focus on Executive Order 12333. In my last position as the Director of National Counterterrorism Center, I had the opportunity to work on many occasions with the Board and with your staff and we always benefitted from your direction and guidance and advice. So, again, I appreciate the opportunity to be here.

So, I'll focus my remarks on the operational aspect of Executive Order 12333, how it works in practice. Obviously, my views are shaped by my experience both at NSA and NCTC and the Department of Justice. I'll begin just with a few comments about how I see the executive order, how it's important in practice and then I'll talk a little bit about the limitations or restrictions that the order imposes on the activities of the intelligence community, particularly with respect to NSA, since that's what I know best.

The first point I'll make and I know the Board knows this, but I think it bears repeating -- Executive Order 12333 is not itself the source of any authority. It is the

foundational Executive Branch document for the organization of the intelligence community and the conduct of its activities. It imposes structure in the intelligence community, it provides direction to intelligence agencies to make sure that their activities support policy makers who are responsible for national security, but it doesn't itself provide the authority for any particular program or any particular collection. It instead operates against the backdrop of authority that is provided to the President and to the intelligence community under the Constitution and under Federal law.

Okay. From an operational perspective, intelligence agencies like NSA, again, which I know best, rely on Executive Order 12333 really every day to delineate their role and their responsibility. In addition to describing the general responsibilities of the community, the order essentially lays out the specific role of each department and agency. For example, Section 1.7(c) says that NSA shall collect, process, analyze, produce and

disseminate signals intelligence. And it also says that no other agency has that same responsibility. I know that NSA personnel are keenly aware of the specific provisions of the order and the duties that it expressly provides to NSA as well as those that it reserves to other elements of the community. So, in my experience the Executive Order really stands out among any other Executive Order as far as I'm aware in that it is a handy on-the-desk reference guide to just about every employee at NSA for what they're supposed to do every day. I'm not aware of any other Presidential order or directive that plays such a central role in the day-to-day role and duties of people up and down the chain.

So, beyond just assigning responsibility to intelligence agencies, the order imposes significant restrictions on their activities. And I think this is probably the most important function of the executive order. Many of these restrictions aren't necessarily mandated by law, but they do give force to the language in the first section of the order,

which says that the U.S. government has a, quote, solemn obligation to protect freedom, civil liberties and privacy rights of U.S. persons. So, for a couple examples -- intelligence agencies must use the least intrusive collection techniques feasible within the United States or against U.S. persons overseas. The FBI is generally the only intelligence element authorized to conduct physical searches inside the United States and the borders of where the other ways in which the order restricts the activities of the intelligence community.

From the perspective of protecting civil liberties, the most critical provision, from my perspective, in the executive order is the one that mandates that intelligence agencies may only collect, retain and disseminate information concerning U.S. persons in accordance with procedures approved by the Attorney General. This provision is the one that gives rise into all of the Attorney General guidelines that every element of the intelligence community is obligated to have and

that must control its activities -- often referred to as AG Guidelines or Minimization Procedures.

NSA, for example, operates in accordance with Attorney General approved procedures that are set forth in U.S. Signals Intelligence Directive 18, sort of an obscure term to everybody except for everybody at NSA, who has to touch U.S. person information who knows USSID 18 or back and forward. They are trained on it before they can touch signal data. They have to prove every year that they know it well. The way in which it operates is on a daily basis for those who are involved in the SIGINT collection or handling of SIGINT information that may touch on U.S. person information.

It, itself -- those rules, those AG rules have a number of rules and limitations that apply to protect U.S. persons' privacy and civil liberties. Importantly, NSA may not use a U.S. person as a selection term -- name, telephone number, e-mail address -- to search databases containing information collected

under 12333. There's an exception to this prohibition in that NSA may conduct such searches if the Attorney General finds probable cause to believe that that U.S. person is him or herself an agent of a foreign power. NSA generally may not identify a U.S. person in a disseminated intelligence report unless the identify of that person is necessary to understand the foreign intelligence of the report or to assess its importance.

So, NSA's compliance with these rules is subject to extensive oversight within the Executive Branch. My former office, the General Counsel's office, the Office of Compliance and the Civil Liberties and Privacy Office at NSA all have a role there. I think we've talked about Congress' role in overseeing these activities. And then beyond the letter of the executive order and these rules that implement its mandates, in my experience the spirit of protecting the rights of Americans is deeply imbedded in the culture of NSA's workforce. My experience is that they take these rules seriously and they strive to follow

them. There's a recognition that a heightened standard applies to information about Americans. And that really NSA's authority to conduct its mission depends on its ability to comply with these standards. And it would be my expectation that the Board in its prior reviews has made similar observations about the NSA workforce.

So, again, I appreciate the Board's focus on the order. I do think that many of the discreet counterterrorism activities carried out under the order are classified, but the general information about the order and how it serves in directing and constraining these activities can and should be discussed publicly as you're doing so here today. And the Board can continue to provide valuable advice and guidance to the intelligence community on the specific activities relating to the executive order and counterterrorism activities in a classified setting, if that's necessary. So, thanks again. I look forward to your questions.

MS. BRAND: Thank you. The Board

members will also be subject to the yellow and red card system, just so you know. And I'll start with my questions. Michael, I wanted to ask you -- we may have, because of the time, cut you off when you were talking about your suggestions for improvement of Congressional oversight. Was there anything that you didn't get to that you'd like to say now?

MR. ALLEN: There definitely was. I mean, one is that I think that the members of Congress and the intelligence committees need to strive honestly for more transparency. In this day and age I think we have to try and get the support of the American people. I think, as President Obama said frankly in his speech last January, so much of the media about the Snowden revelations is sensationalist. I think we're now in a different mindset. The previous mindset was let's never talk to the press, let's -- you know, many in the intelligence community ironically didn't like the one annual unclassified hearing we held each year, the Worldwide Threats Hearing. But I think we're in a different place now where we need to

strive for transparency -- not only because I think the American people deserve to know more, consistent with sources and methods, but also I think it will support the critical intelligence gathering mission of the country.

MS. BRAND: I want to ask you and Ms. Eoyang both, based on your experience on HPSCI, about the extent to which the budget is an effective oversight tool. You mentioned it. I've heard a little about it. I frankly don't personally understand how the HPSCI and the Appropriations Committee would intersect on budget issues and whether -- you referred to fencing off funds. Is that used as a club? How does it facilitate oversight? If you could just explain how that works.

MR. ALLEN: Yeah, sure. The authorizing and the Appropriations Committees sometimes get along very well; sometimes they don't. I guess the best way to look at it is that we're supplying the authority to do certain activities. The National Security Act requires that each intelligence activity be specifically authorized, which is the reason

why the intelligence committees have got a seat at the table, frankly. And the appropriators are literally the check writers. We work together in many cases to set funding levels together and personnel levels together. It's a different set of eyes that approach the same problem, but primarily from a budgetary, hard core numbers perspective.

Your second question --

MS. BRAND: And how does the fencing off work?

MR. ALLEN: The fencing works this way: For example, if the Congress has issues with a particular program or, as was mentioned earlier, issues that the community is not focusing on a particular issue or has a problem with an NSA collection program, we would, the staff under the members' guidance, write in particular conditions that must be met before the CIA or the NSA or whoever the case may be is able to access the funds. So, we would often fence $80 million until such time that the committees have been reassured of A, B and C. And so, this is a strong means by which

we exercise Congressional oversight.

The other way is frankly reprogramming requests. I didn't have time to talk about that, but you all know the problems with the federal budget process. We have to go annually -- so many things change. By the time you ask for things, by the time the money's appropriated, each committee is bombarded with reprogramming requests, and the practice is that the intelligence committees have to sign off on reprogramming requests, which is essentially where we, the CIA or the NSA, are redirecting money from this purpose to another purpose. We have to sign off on those, and that is another leverage point for the Congress, which frankly uses it for not just changes to what's before them, but often about particular programmatic, some would say sort of intel policy issues that are related. So, Congress, I think, has a lot of tools at its disposal, if it operates fair and bipartisanly and does its job.

MS. BRAND: I'd like to give Ms. Eoyang a chance, too.

MS. EOYANG: To Michael's point about the importance of the Intelligence Authorization Bill, I was on the committee in the years when we didn't have them, and the challenge is that the fences only work if the bill is enacted. And so, if there's no bill enacted, then it really reduces the leverage of the committees and their ability to make policy that way. The Appropriations Committees got into the habit in that time of putting in language that said that any program that was appropriated was also authorized, making them king of the hill in terms of all policy decisions. When the two committees don't play well, the authorizers lose tremendous power to the appropriators because if the appropriators can carry that provision, notwithstanding an Intelligence Authorization Bill, but all the fences that the intelligence committees have are moot.

And this is particularly important given the staff sizes between the two committees. The Appropriations Committees have smaller numbers of people looking at the same

programs than the Authorization Committees do.

MS. BRAND: Okay. Thank you. Matt, I wanted to ask you: In practice, you talked about how employees of the NSA and other agencies -- they know USSID 18, they know 12333, they take this stuff very seriously. How is it exactly that they feel the consequences if they don't? How does the rubber hit the road there?

MR. OLSEN: You know, in the most extreme example, there's disciplinary action for those who, you know, purposely violate those rules. And there have been a handful of those instances. The -- you know, in those instances where mistakes, people make mistakes, you know, in good faith, you know, I'm trying to think if I can think of a specific example to be really concrete, but I can't think of one off the top of my head. But what my sense is is that people are taken off the access to the SIGINT information, so they're removed until they have additional training and then can pass the test. I mean, they literally have to pass the test before they can touch the data. So,

that's I think it happens. I mean, that's when the rubber hits the road.

MS. BRAND: Okay. Go ahead.

MR. EDGAR: Yeah. I was just going to say that one of the requirements is that these violations be reported to the Intelligence Oversight Board on a quarterly basis. That creates an entire compliance culture, compliance system in which violations are collected. And some of the Snowden leaks have actually been the result of exactly those processes. In other words, the reason we know that these violations happened is because NSA and other agencies were collecting them and monitoring them in order to prevent them from happening as much in the future.

And my view is that your compliance system is only working if you do see violations. If you see a bunch of reports that say zero, zero, zero with, you know, hundreds of thousand of people working in a huge program, that means your compliance isn't being measured correctly.

MS. BRAND: Okay. I have another

question for you: You said that we should look into how much 12333 activity is counterterrorism-related versus other foreign intelligence purposes. And that question is important to us because it goes with our statutory mandate, which is limited to counterterrorism. But I don't think that's what you were talking about. Can you elaborate on why you think that's important for the public to know?

MR. EDGAR: Well, I mean, it's important for you for that purpose clearly, but it's also important, I think, because you have this mismatch between the government officials often saying, look, we need these important surveillance programs to keep us safe, and that often gets translated into this is about terrorists. And there's a significant portion of NSA and other agencies which are directed towards that goal. There's also these broader issues. And then sometimes you get critics and civil libertarians saying, ah ha, this really isn't about terrorism, this is about something else and somehow that's nefarious.

I just think that having more transparency about, you know, not getting into sources and methods, but just saying, you know, this is roughly speaking how much of our efforts are devoted to these things is extremely helpful. And your reports earlier on some of the FISA activities were helpful just in getting out a public record that allowed that debate that we've been having to be more informed. And this is a place where you might be able to show some of that, you know, if it's 50 percent, if it's 20 percent, if it's 80 percent. If you're talking about something very intrusive like a very large amount of collection of signals or other types of things that are controversial, it's going to matter to the public whether this is mostly about terrorism or this is mostly about something else.

MS. BRAND: Okay. Unless anyone else had anything on that, I'll give up the remainder of my time. Do you want to go next, David? Beth? Okay.

MS. COLLINS: So, I'll have a

comment and then a question. I will say all I could think, Matt, when you talked about the AG guidelines and how much we should look at those and the effectiveness of those and the implementing policies, we're, I think, unanimously concerned about the age of many of those guidelines, the lack of updates even in a changing technological world and then perhaps the development of a separate process under PPD 28, which may not always fit completely well with the 12333 guidelines. So, that's more my comment.

But my question -- and I want to take the view of the experts here to -- shamelessly here to try and do my job better. How do you know the questions to ask to figure out what the IC is doing? How do you avoid the if you can guess what we're doing I'll tell you about it phenomenon?

MR. ALLEN: Well, at different -- I think at different times in the committee's history there have been different views on this. When the committee is in a hyper partisan mode, I definitely think that the IC

begins to get in a more defensive posture when they come up to the Congress. I think when the Intelligence Committees --

MS. COLLINS: Sorry -- by hyper partisan, is that because they feel like no matter what they answer they're going to be -- they're going to catch hell for it or do you find that it goes with party?

MR. ALLEN: They are being berated for particular programs or the way particular analytical judgments have come out and they're being very clearly used by, in some cases, both parties for a political purpose.

MS. COLLINS: So politicized maybe rather than partisan atmosphere; is that fair?

MR. ALLEN: Well, I use partisan because I think, of course, politics is endemic to Congress. It's a political body. I think, but I guess I understand it could be used in the sense of the word, too, but I think we're talking about the same thing more or less.

But I think when the committees are at their best, they're working together and

they're strict but fair and I think if they are that way and the committees know that they can share more information, they do. By the way, most committees are -- this is going to be a real surprise to people -- are very -- I'm sorry -- most of the agencies are very interested in coming up to talk to the committees I think because they want to know that the people's representatives have their backs. People like to say, oh, well, the only power Congress has is power of the person. That's not going to be applicable until the end of the year when you pass the bills. That's not always the case, I'm sure. And I know of examples, especially a report that was done when Mieke was on the committee, of examples where they believed that there were instances where the CIA didn't keep the committee fully and currently informed.

But in some of the most controversial programs, generally it's been my experience that people want to come up to the House and Senate Intelligence Committee and say, hey, guys, here's what I'm doing, please,

you know, I want to hear about it. And I know of covert action programs and other programs that have received a negative reception from the Congress right there at the table and the CIA and others have gone back to the National Security Council and said, you know what, the Congress is not with us on this, and that matters to them. So, I think that, you know, that helps induce more information out of the agencies

MS. COLLINS: Let's actually turn to a time where if there was a perception that the community was not being as forthcoming as they could or should have been.

MS. EOYANG: So, I would actually like to disagree with that characterization that Mike makes about it being partisan. I think it has more to do with the Executive Branch's mindset about sharing. My experience is that when the Executive Branch has a very strong view of, say, a unitary executive and they are not interested in sharing, it doesn't matter which party controls the chair in Congress for them to withhold information.

Likewise, it does not matter if the President and the Chair are of the same party and the Chair takes a very aggressive role towards a particular intelligence program for the community to get in a, as Mike says, a defensive crouch. It's more about the relationship between the heads of the agencies, the White House and the Chair themselves and the ways in which they get along and the ways in which they feel like they can trust each other to share information. They may be of the same party and they may be of different parties. That just varies and I think that varies from time to time.

It is very difficult, I think, for the committee to -- when the relationship changes to feel like they have the sense of trust in the information. So, a hangover from a previous time when the committee discovered there were things to which they were not briefed may result in them being more aggressive and questioning more doggedly against an administration that is willing to share. And so, I think that is part of the

challenge. The tone of the questioning really affects the quality of the relationship.

But to your question about how you ask -- how do you know what you don't know -- part of it is in the access to documents. And as committee staff and the members of the committee, we are reliant upon the representations made by the Executive Branch officials to the best of their ability to make them. So, if they make them in error or they make them with an intent to limit the information, it is really difficult.

One of the things we have done and you see Congress doing is asking for the supporting documentation on that so that you get a better sense of not just the representation made in the briefing, but how is the program described, what are their internal documents to characterize it for themselves. That sometimes helps. Summaries made by the Executive Branch to characterize a particular program may not capture the fullness of it or may not capture the complexity of questions that a particular oversight actor may have in

mind.

MR. OLSEN: May I make a very quick comment, which is to say that it would be, I think, a misimpression to leave here that, in my experience at least, the intelligence committees have so much more information and there's such a degree of cooperation with the Executive Branch against a back drop of a system of separation of powers as compared to my experience at justice and the judiciary committees -- just night and day. Much less flow of information to the judiciary committees, much less interaction. The intelligence committees and the intelligence community have a synergistic relationship that I've never seen anywhere else across Congress with respect to -- and the Executive Branch. So, I think that's an important point.

MR. ALLEN: I would just say quickly -- I know you want to get to another question -- the CN's, as we call them -- Congressional notification processes -- I mean, they pretty much paper you with every success story and every program that goes off the

rails. And so, I think they're very interested in building a paper trail. And also, frankly, travel. People like to lampoon members of Congress for exotic trips. You learn a lot when you go out in the field and see the station chief and talk to the individuals who are doing the jobs in the field. And we often learn more out there than we do back in Washington and we can follow back up on these particular issues.

MS. COLLINS: Tim, did you want to weigh in on this? I know you've been in various roles.

MR. EDGAR: This is a huge issue. It's an issue even within the Executive Branch and I think having these formal processes, CN's or programatic reviews, are absolutely vital. You know, in 702 you've got a whole system for the FISA court to weigh in on what is essentially programatic reviews of surveillance programs. I think that we should explore every way to make it more programatic so that you don't have to be guessing the question of what should I ask you because I do think that's a

problem, even with the best intentions and with the best relationship.

MS. COLLINS: I doubt I have enough time for another question, so I'll pass along -- how are we doing this?

MR. MEDINE: Thank you to the witnesses for sharing your perspectives with us today -- very helpful. Matt Olsen referred to the relationship between the agencies and the intelligence committees and you used the word synergistic. At a certain point, you could get over into too close of a relationship. So, a question for Michael and Mieke: What do you think was most effective in preventing, for lack of a better word, capture or too much of a closeness between the oversight committees and the agencies?

MR. ALLEN: Yeah. I mean, I think there's an urban myth out there that I've heard repeated to me hundreds of times that, oh, well, the CIA recruits people for a living and they're going to recruit the members of Congress. I really don't -- I really don't subscribe generally to that theory. I think at

some point there is -- there's definitely occasionally a wow factor at some of the things that are happening in a respect that follows for their particular mission. But I don't think that any of the members of Congress just become captured by what they hear from the CIA. I like to say when witnesses would come to me and say how should I approach this particular hearing, I would often say, listen, members of Congress, for all their faults, understand spin. They recognize spin immediately because that's part of what American politics is all about. And so, you should be as forthright as you can because if you're not, a member of Congress is going to smell it and you're going to be in trouble.

MS. EOYANG: I would say that's right that the oversight that occurs behind closed doors is quite robust and I think a lot of people assume that because they can't see it to being robust, therefore it's not, and I don't think that's true. We have had experiences where the senior defensive -- or senior intelligence officials were expecting

the members of the committee to go out and defend and validate the community's activities. And on a bipartisan basis, they rejected that characterization of their role. I think that it is not -- that they may have certain programs that are their favorites for various reasons -- personal, constituents, interests, what have you. But that's different than overall capture.

And the thing that I think prevents the members from being captured is the reminder that at some point some day things may become public, either through mandatory declassification or, as we've seen over and over again, through leaks. And what they have said on the record, though classified, may define them.

MR. DEMPSEY: Another question for Michael and Mieke, again along the lines of that question about how do you do this well: Do the committees adopt an oversight agenda? Do you tell the agencies this is where we're going for the next year or this is what we're looking at?

MR. ALLEN: Most definitely. I mean, what Chairman Rogers did was reinstitute a regular oversight schedule over covert action programs, for example. So, we had a quarterly covert action review where the staff would work to prepare for that quarterly hearing and do a deep dive on the particular program, brief the members, so that on the Thursday that these CIA officers or whoever came before us, that we were in a position to go deep, so to speak.

The chairman also reinstituted, for example, the quarterly CI and CT briefings from the FBI. I think that we have a long history, in part because of abuses in our history of the Congress asserting its oversight over the Central Intelligence Agency, and I think we have less of that in the FBI context. I think they paper the committees less. I think that generally it's harder for them to talk about open law enforcement investigations, and that makes them uncomfortable and that's understandable. But I think that we tried to reinstitute the process where we would quarterly do these basic staple reviews. And

in addition, the chairman would announce, here are the three things I'm going to focus on this year. Often they were a covert action program and the like. And the staff director made sure, consistent with the chairman and the ranking members' priorities, that each of the budget examiners for each of the 17 intelligence agencies had an agenda of the two or three things that they were going to look at.

And for your purposes, I think it's important to remember also, we've got a suite of lawyers as well. So, we have budgetary people looking at the NSA from a personnel and programatic approach and we have lawyers looking at it from a legal and I guess privacy and civil liberties approach.

MS. EOYANG: On that though, Mike, you said the word reinstated raises something really important, which is that the regularity of the agenda and the processes that are set are determines by the Chair themselves. On HPSCI, at least on the Democratic side, there are term limits so that they have regular

turnover of the head of the committees, so the processes may change from time to time. I am not sure what the current processes were, but obviously they were not the same under Chairman Rogers as they had been under previous chairmen.

MR. DEMPSEY: Tim, hang on just one second. I want to ask Matthew this specific point: You were on the receiving end of the oversight process both at the NSA and at the NCTC. From your perspective and really looking at it as objectively as you can because maybe you thought that it was a bit of a pain, but leaving that aside, what was the most effective oversight or methodology of oversight that you experienced? Or what were the elements of an effective --

MR. OLSEN: One thing that comes immediately to mind is that what I did on a regular basis, which was to have a round table format discussion with the members -- not a hearing format, but just sitting around the table, literally a round table, and have a discussion about the top terrorism threats that

we were tracking. And we did that, you know, on a, I would say, three or four times a year, obviously classified. That broke down the sort of five-minute rule. You know, it broke down many of the things that I think sort of impede the free flow of information or make it a little bit harder to formality and, I found, a great way to impart information to the members. So, that was one -- you know, lots of interaction with the staff, having the members come out to the agency, also, you know, again, the lack of formality there.

But to your original overarching point, Jim, on the receiving end of this, I found the interaction, you know, synergistic might be an overly strong word. I don't disagree with the concern on one end that it could be too close. But the -- I felt that it was important and useful for me to talk about these issues, to get the advice -- you know, literally, truly to get the advice of the members who have real thoughtful reactions to what we were doing and where we were going.

MR. MEDINE: Tim, you wanted to

offer something?

MR. EDGAR: Yeah. Just I think that the capture issue is a real one and it's also a very serious public perception problem that reminds me of the FISA court capture concerns. The same exact set of concerns, same exact attempt to push back by many of the judges for many years, even decades, saying, no, we're not a rubber stamp, that's just not the way things really work, if you could only see what we do. And I think that by declassifying many of the FISA court opinions there has been a benefit to sort of prove that that is clearly the case. And I guess, you know, the old adage is that Congress is always calling for reform and never reforms itself. This may be an example where some additional transparency in exactly what we're talking about in letting in more transparency into these Congressional reviews. I mean, every Congressional hearing is noted as, you know, closed hearing on intelligence matters. You know, could we do a little better than that? Here's the general topic of the hearing, here's

some unclassified comments about the hearing, here are some examples where Congress is pushing back, here's some declassified reviews that were conducted. That would go a great deal towards, you know, kind of showing the public that these reviews were quite substantive and useful.

MR. ALLEN: So, that's happened. I mean, the Abdulmutallab underwear bomber -- the Senate Intelligence Committee put out a report that, I think, helped the NCTC along the way of creating pursuit teams. The joint inquiry after 9/11 was a voluminous multi month process and, of course, also -- well, many other public reports that we've put out.

MR. OLSEN: The HPSCI report on Benghazi was also in -- largely public and very useful.

MR. DEMPSEY: Let's hold it there. Thank you very much. I really appreciate it. Thank you.

MS. WALD: Okay. I've been listening carefully and I'm getting two viewpoints and it may be that they come

together. But I think some of you are telling us that overall, if you look at it, the intelligence committees are doing a pretty good job of oversight. But we're also hearing some of the specific questions about -- I think, Mike Allen, you raised the question about, for instance, the NSC having the -- currently the authority to decide who gets briefed on what and perhaps there could be more push back on that or however that's dealt with. And, Ms. Eoyang, you raised the question about inaccessibility to the GAO, to the CBO office, to -- somebody raised a question about not having -- oh, you did, too -- about not having -- being able to review the legal -- I assume you mean OLC type opinions on that.

And there are various other things which raise questions to me about it which are before the intelligence communities -- or I agree with everybody else -- an essential party of the apparatus of the whole intelligence community. Is it just that Congress is a political body and the intelligence committees don't have the -- don't

always have the push, the whatever it is it would take to get those kinds of resources that they think they need? Or, as we all know, sometimes the political -- current example, I don't even need to specify -- you know, it becomes clear that they're really divided in substance wise, but since they are so essential, I keep wondering why there isn't more sort of push back to say, look, we need this to perform our Article One function of oversight and so, why should the NSC say to us, we're going to decide who -- you know, you, et cetera -- I don't mean to overemphasize that example, but just I keep thinking is this at all, to put it bluntly, a conundrum of their lawmaking in the sense that they don't fight hard enough or is it they simply don't have -- you know, the access to whistle blowers, they just don't have the clout with the political leadership of Congress to get what they think they would like to have for their --

MR. ALLEN: I can address these, I think, quickly and then I'm sure Mieke would like to get in here, too.

MS. WALD: Oh, I'd like everybody who wants to. That's my only question, so...

MR. ALLEN: No problem. Look, this may surprise you coming from the Bush White House -- I think we over used the Gang of Eight model. I think it was born from a fear post 9/11 that we needed to keep things as quiet as possible. I think by the end of the Bush second term, we had largely abandoned the Gang of Eight process and President Obama has -- well, not abandoned the process, but used it in much fewer cases. And I think President Obama has also not used it very frequently. He used it for the Osama Bin Laden raid, which has now been declassified, of course, and another instance that I can think of. And that is because Congress has pushed back. Members of the Gang of Eight have said to the NSC and to the CIA, I hate it when you tell me things that I can't tell my membership. And so, I think there has been a push back over the last ten years so that -- and I think Congress has succeeded.

On the GAO, there's just -- there

are differences, there are ideological differences about this. We have let them in the door on certain programs, but it's -- let's just say that it's not all Executive Branch people are people favorable to the view of the Executive Branch are excited about the GAO getting into some of these areas. Congess is united on OLC opinions. They think it's ridiculous that these are held back and they frequently make such a big stink about it that they win at the end of the day. I can think of three or four examples.

And on whistle blower, it might surprise you that the Republican majority unified with our Democratic minority supports changes, at least under Chairman Rogers, to the whistle blower statute so that whistle blowers wouldn't have to check in with someone in their building before they were able to come to Congress because we found that to be inhibiting. It's not been enacted yet.

MS. WALD: Do you think that's a trend that because of the heightened public attention that's been given in recent times to

the whole intelligence and intelligence surveillance and oversight that that's a trend that after all of those -- I can remember the 9/11 Commission itself, the WMD Commission, almost every commission always came up with saying Congress needs to give more vigorous oversight to the intelligence community and here's a long list of things we think you ought to do, most of which have not been accepted. Maybe they're not all good to be accepted. I don't suggest that, but it seems as though nothing sort of happened, but do you think that's a trend they're going in the right direction towards more vigorous oversight, more wanting to know more information about on which they can operate --

MR. ALLEN: There's certainly a trend that the committees want more information and I think they demanded and they largely get it. But the effectiveness of the oversight function I think does wax and wane, depending on, again, who the chairman and ranking are, who the members are, the spirit with which they attack the oversight mission and the rest. But

what I was trying to do with my remarks today was sort of advance the state of the debate about Congressional oversight.

MS. WALD: Yeah, sure.

MR. ALLEN: I'm not saying it's perfect. I can give you another ten ways to improve it, but --

MS. WALD: You can do that by writing us a letter --

MR. ALLEN: I'll write you a letter. I'm not going to do it now, but everyone is stuck on the same 9/11 Commission talking points, which is Congressional oversight is dysfunctional and there's been 15 years since that and I think we need to -- we need to update with conventional wisdom.

MS. EOYANG: I would say just in response to one of the 9/11 Commission recommendations, though -- sorry -- this is not on. In response to one of the 9/11 Commission recommendations that they consolidate committee oversight on that, I actually think that consolidating committee oversight runs a greater risk of committee capture than by

having the different committees approaching Appropriations, House, Senate, different aspects of it under other committees, Armed Services, because then you are not so dependent on the one Chair or ranking members' attitude towards the community, but you have a bunch of different philosophies about it and so you get different results and different levels of oversight in that.

MS. WALD: What about -- just the last sub question on that -- we hear in many quarters that a great deal of difficulty lies in the fact that the staff members, even some of the leading staff members, don't and can't seem to get -- I don't know why -- security clearances so that they, too, can participate in looking at the classified material and talk with their members about that, which seems, considering all the people in the contractors and subcontractors in the country that have security clearances, why that seems like it's simple enough.

MS. EOYANG: That's been actually a matter of great frustration for the members

when they are told we can tell the members something, but then they cannot tell the staff -- they cannot consult and get the benefit of their staff. There have been at least one publicly reported example of this where it was a dispute between the members and the previous administration. There is, I think, a Constitutional question that underlies that --

MS. WALD: What is that?

MS. EOYANG: -- about whether or not the Executive Branch, once they've given the information to Congress, that they can control the flow of that information. There are House rules and Senate rules that control the flow of the information inside the branches. But I don't think it a settled question that the Executive Branch -- on a classification system that is based on Executive Order and executive regulation can bind a separate but equal branch of Congress if the chairman of the committee says I have heard this thing and I want to consult my lawyer who is appropriately cleared to other programs

inside classified spaces. If the members can have that conversation under the Speech and Debate Clause on the floor of the chamber and are able to do that constitutionally, I'm not sure what the application is for the Executive Branch to say to Congress you can't choose who inside your branch you can consult with, assuming that appropriate security measures are taken.

MS. WALD: It does sound like a kind of question, though, that if you really do want to have it, the Intelligence Committee wants to have effective oversight that it would be at least a plausible subject for negotiation or --

MR ALLEN: I really think this has gone away.

MS. WALD: Really? It's still talked about a lot.

MR. ALLEN: It is. I'm sorry -- I see the red light. But I think honestly that a lot of this happened in the Bush years when we restricted billets on programs that have since been declassified. I didn't have that

experience in the HPSCI. I think the SSCI has it a little bit more because they have more people. But by and large, we did not get a lot of resistance on the number of staff read into programs.

MR. MEDINE: To continue that line because we've heard from staff members who were not on HPSCI and SSCI.

MR. ALLEN: To repeat, we've heard concerns raised about staff of non HPSCI and non SSCI Senators and Congressmen and Congressmen just don't have the time to go and read classified documents and they typically rely on staff, as they do across the board, so it puts them at a real disadvantage to committee members who have staff -- but have clearances and the staff to analyze. So, thoughts about -- and therefore, it makes it harder for the members not on the committees to vote intelligently on surveillance legislation when they haven't really been fully briefed. I think that's sort of in some ways the point that was raised earlier about expanding the number of members of Hill staff who have

clearances and also if the Hill staff, Hill members feel that way, why don't they pass a law mandating it?

MS. EOYANG: I think, to Michael's point, we have seen a more openness from the administration to talking about this. But in terms of the administration's ability to lean forward and be more transparent, when there are legal rationales or legislation pending before the Congress, I think it's incumbent on the Executive Branch to try and declassify as much of the public policy debate as they can to give those members who do not have cleared staff access to what's necessary to decide good public policy on behalf of the American people. I think we have a slow thawing of a very intense secrecy regime. I'm not sure what happens in a future administration on that. But I think because of the sensitivity of some of the programs involved, it would be difficult to give all 435 members of the House a staffer who has access to some of these programs. I think that that's a bridge too far. But -- and I know that the

committees have tried to -- at least we certainly did -- tried to make available the committee staff to members who wanted to come read the documents, but that does not necessarily obviate the schedule pressures on a member.

MR. MEDINE: I'd like -- given I have limited time, I want to move on to a different question and I'd appreciate each of your answers to it, which is the following: In the course of our 702 study, we looked at the oversight of that program and we saw a judicial oversight in the FISA Court approved 702 request to companies. We saw intra-agency review, supervisors reviewing what analysts were targeting and how they're using the information. We saw very rigorous inter-agency review of Justice Department and review by the Director of National Intelligence as well as Congressional review. And I was very impressed with the scope and the depth of that oversight process. In 12333 we don't have judicial review and we don't -- and I guess we really want to look into whether there is

inter-agency -- I don't know if you want to address that or not -- or are we just limited to intra-agency review? So, I'd appreciate each of your thoughts as to whether there is sufficient rigor in the 12333 oversight and, if so, where does that come from?

MR. ALLEN: Well, as I said in my testimony or at least I tried to get to this point, I mean, it's obviously a vast amount when you're talking about $70 billion over 100,000 employees and 17 agencies, so every Congressional committee has to pick and choose what it focuses on. But 12333 is just sort of shorthand for everything else. It's often shorthand for the foreign intelligence collection programs overseas and I'd -- you know, there's not to say we couldn't do more work on it, but we do. We have the covert action reviews, we have the counterintelligence and the counterterrorism reviews, we do a host of other programatic reviews throughout the year. So, it's true it isn't bound up nicely and says 12333 review, et cetera, et cetera. That's because generally we sort of think of

that as everything that's foreign intelligence collection and that's sort of like what we do everyday down at the committee in addition to FISA and some of the domestic intelligence authorities. But that's really the vast majority of, I think, what we thought we were doing and what our job was and so, I would submit to you that we do have -- we do have oversight over 12333.

MR. EDGAR: So, I think Mike and Mieke made fantastic points about the rigorousness of Congressional oversight, but I do think that the lack of any judicial or quasi-judicial oversight is really quite glaring in some E.O. 12333 activities that raise some of the same privacy and civil liberties issues as FISA activities. I think there's a whole range of reasons. You've talked about members who don't have cleared staff, you've talked about, you know, the very wide range of questions that members of Congress are asking precisely because they are asking all the policy questions that you don't get in a more legal focused review. So, I

guess I would say that it's important but it's not a substitute for other kinds of review and there may be activities that require either judicial or some kind of quasi-judicial type of review.

That said, I also think that it is absolutely the case that the United States leads the world in terms of the quality of our intelligence oversight -- judicial, Congressional, internal Executive Branch oversight. And one of the recommendations that I make is that we should not be shy about that in a way that I think we have been. I think we've been in a defensive crouch frankly since the Snowden revelations started and I think we should be out there saying, hey, where are your, you know, cleared staff for your intelligence committees, which, you know, some of our closest allies don't have. Where are your reviews? Where's your FISA court? You don't have any of this and you're coming and complaining to us about, you know, allegedly runaway surveillance programs. So I think there's a way for us to both improve and reform

our surveillance programs and maybe even add more oversight and review where it's necessary where the issues are there and at the same time not be defensive about it but say we think this is a great system and we want to make this system even better and this is what we're doing about it and what are you doing about it.

MS. EOYANG: I'll let Michael's comments stand --

MR. MEDINE: Okay. Mr. Olsen.

MR. OLSEN: It's very hard really to answer that question, I think, because of the breadth of activities that take place under 12333, as the Board is aware, as you're aware. You know, so, I mean, to Tim's point on the judicial review for covert action that's done under 12333, but it doesn't seem likely -- you know, so I mean to recruit a source that's done under 12333, no. Certain surveillance activities that don't involve any U.S. persons, you know, specifically tapping a phone, you know, or -- so, it's hard to answer that question, I think, meaningfully, to be honest with you.

MS. EOYANG: Actually, I do have one thing to say about it

MR. MEDINE: Okay. Very quick, yes.

MS. EOYANG: Which is that Mike's point about it being foreign means that unlike some of the surveillance programs where we're talking about not knowing incidental -- knowing that you're going to incidentally sweep up some communications of Americans, on 12333 we're mostly focused on non U.S. persons outside the United States. So, the questions about judicial oversight and Constitutional review, it's -- the laws and the legal framework there is very different, so we are talking about the President in his Article Two authorities and the limits of extraterritorial application of the Constitution for those kinds of reviews it's not clear that they apply the same way

MR. MEDINE: Thank you very much for the panel. We really appreciate your thoughtful responses and extremely helpful to us as we approach 12333, as with all the other panelists today as well. This concludes

today's public meeting. It's 4:17 p.m. A transcript of the meeting will be posted on the Board's website, pclob.gov. Members of the public are also welcome to submit comments on today's meeting and 12333 generally by visiting regulations.gov. Comments there are being accepted until June 16th.

And now, all in favor of ending today's meeting, please say aye.

VOICES: Aye.

MR. MEDINE: That was a vigorous aye. The meeting is concluded. Thank you.

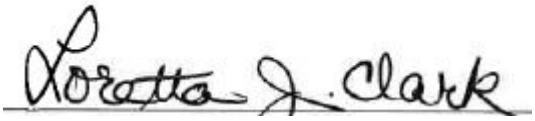
- - -

(Whereupon, the meeting was concluded at 4:45 p.m.)

- - -

C E R T I F I C A T I O N

I, Loretta J. Clark, a Court Reporter and Commissioner of Deeds, do hereby certify the foregoing to be a true and accurate transcript of my original stenographic notes taken at the time and place hereinbefore set forth.



LORETTA J. CLARK
Court Reporter
Commissioner of Deeds

DATED:5/26/15

(The foregoing certification of this transcript does not apply to any reproduction of the same by any means, unless under the direct control and/or supervision of the certifying shorthand reporter.)

I

J

