- All right. Thank you very much. It's my great pleasure now to introduce a moderator for the next next discussion. Professor Mary DeRosa, who's both a friend and a colleague. She is a professor from practice here at Georgetown Law. We were incredibly lucky when she came to the law center from the Obama Administration, where she served as deputy council to the President for National Security Affairs in the Obama administration. And then she was also a legal advisor in the Clinton administration. She's a graduate of University of Virginia, where she received her BA with honors. She went on to GW Law School where she graduated Order of the Coif. Or coif I guess you could say, as we say here, she also is in charge of our Global Law Scholars program here at Georgetown Law. She teaches on cybersecurity and of course, rights in all matters, national security. So it's my great pleasure to welcome to Mary as moderator for the next session.

- Thank you. And I'm delighted to be here with April Goz. April is the general counsel of NSA, as you know, she is one of the, our really foremost experts on surveillance law, intelligence laws. She had a long career at NSA in a first a- senior policy council and operational manager, and then in the general counsel's office. Is this on? Okay, good. Senior board of council, then at the general counsel's office as associate general counsel for intelligence law. Then she left, she did a number of things, private practice. She was on the hill for a while. And then most importantly, she came to Georgetown Law and ran our tech policy and law policy program. And until she abandoned us last May to go back to NSA, We remain bitter about that but we have decided to overcome- to get over it, and our loss is absolutely NSA's gain. So we decided to do this as a fireside chat. And so I wanna start April, by asking sort of the fundamental question is kind of starting where maybe we left off in the last one in the panel of from your turn, you know, so you're speaking for the NSA, the IC, the 702, you know, nothing happens, goes away December 31st of this year. What do we lose if it goes away? And another way of asking that is, what is the value of this program? Just start there.

- Thank you for that question, Mary, thank you for the privilege of being here. It is such a- this has been such a pleasure. Wasn't the first panel fabulous? So Laura and Mary and Mary and Todd, what an incredible job pulling together all these diverse and important perspectives on a really important set of issues, and difficult issues, really important policy trade offs. And this has been a wonderful conversation so far. And thank you for allowing me to have this conversation with you. When I talked with Mary and Laura ahead of time and they gave you the privilege of doing the keynote, they asked me if I wanted to provide prepared remarks. And I think we were all in agreement that this is a much better format. Because this is the conversation that needs to be had about these issues that are so vital, both to national security, and to privacy and civil liberties. It's of heightened interest in the US, around the world. As we saw in the discussion about the executive order on protecting the privacy of non-US persons. This is a critical conversation. So again, Mary and Mary and Laura and Todd, thank you for putting this together. So what would be lost? A lot, A lot. Let me start with one headline number for you. In the President's daily brief, 59% of the articles in the President's daily brief include sourcing from FAA 702. Folks that is nearly two thirds of the intelligence information that crosses the president's desk every single day is sourced to this program. That is huge. So what gets lost if this goes away? Two-thirds of those articles, right? Don't misunderstand me. I'm not saying that 59% are sole sourced, but 59% of those articles include information from FAA 702. That means nearly two-thirds of the information in the

President's daily brief would be detrimented or in some cases perhaps unavailable entirely. So below that number, what does that mean? It means some, many of the things that you all have heard in other contexts, it means that FAA 702 was responsible for key government insights on some of the foreign- some of the strategic power and foreign adversary and other strategic plan and intentions kinds of information that is of the greatest interest to the United States government. So this is insights on Russia, China, North Korea, Iran. This is insights about foreign merchant cyber activity that is directed against parties in the US. This is certainly, absolutely, still about terrorism. Remember that this law was passed in the wake of the 9/11 attacks and absolutely it's still vitally important on counterterrorism. So as we look at as an intelligence community at what can be declassified, we look at exactly the things that Chris talked about earlier on the panel. And by the way, I should say where I am providing facts, I hope they are illuminating to the extent I accidentally step into the realm of opinion. Please know, the opinions are mine alone and not necessarily those the of the NSA or the administration or anything else, but I'm hopeful that I can provide just information to help inform this congregation. So as Chris talked about, it's really difficult when the government has to look at what to declassify and how to go about that. And the reason it's difficult is because we know that our foreign adversaries pay really close attention and parse every word of whatever is put out there publicly, whatever is publicly acknowledged. And we know that foreign targets, critical national security threats absolutely do change their behavior based on information that they obtain about how the government goes about obtaining intelligence. So we're always trying to find that balance. And that's why you find government statements about value be so carefully worded and thoughtfully approached. And now I will say that although on the value side we always have to be mindful about potential compromises, sourcing method, that potential change in adversary behavior and so forth. When it comes to the framework and structure of this program, we have a record of transparency that exceeds that of any nation in the world. There's no country in the world that is as forward leaning and as transparent as the US government has been about the conduct of this program. And so if you go to the IC on the record website, you will find literally thousands of pages of information. Some of it in the context of things like the annual statistical transparency report that are produced specifically for the purpose of reporting transparency. Other things like the redacted versions of declassified opinions of the FISC, every significant opinion of the FISC has now been released on the record. And yes, there are some redactions, but what you will find are thousands of pages of information describing what the government is doing, how it's being done, how it's being overseen, how mistakes are getting corrected as they arise. And so that record of transparency I think is just extraordinary. There's no other nation in the world that has that level of transparency.

- So I know that, as you said, know how difficult it is, but I'm going to push you a little bit and see if you can anymore detail anymore, for instance, on what this program gives you that you can't get from somewhere else. And in, you know, particular areas, particularly if you have any kind of declassified, unclassified vignettes that you can share. As I think, you know, as you know, It's important and as Chris was saying, and you have said, this is something that you gotta explain to the American public. So anything else I think looks like you have something.

- Well, to my earlier comment, this is where I'm gonna refer my notes because I wanna make sure I'm capturing everything accurately and precisely I should say. Alright, so as I mentioned 702 has helped the

government understand the strategic intentions of the foreign governments that we're most interested in. So that is absolutely the People's Republic of China, Russia, North Korea, and Iran. Key strategic insights. 702 acquired information has been used to identify multiple foreign ransomware attacks on US critical infrastructure. The intelligence derived from 702 positioned the government to respond to and mitigate these events, and in some instances to prevent significant attacks on US networks. So the IC has also used information from 702 to discover the foreign adversary had used a cyber attack to acquire sensitive information related to the US military. Hey, cause I forgot to say this when I highlight the 59%, let me just add to that, this program has saved lives. It has absolutely saved lives. So remember, 59% of what goes to the president is tied in some way 702. And it has absolutely saved lives. So foreign adversary- Where was I? Oh, foreign adversary hinges a cyber attack to acquire sensitive information related to the military. 702 information revealed a cyber attack against critical US government systems. Enabled the IC's development of mitigations to protect critical US government systems that were compromised by a cyber attack. You're hearing a theme here, right? So people often think of this- of the CT roots of this program and again, as I mentioned, it's still vitally important to counterterrorism, it is of enormous importance of cyber as well. So 702 has identified key economic security risks, including strategic mine investment by foreign actors in certain US companies. 702 acquired information related to sanctioned foreign adversaries. Was used in US government efforts without components for weapons of mass destruction from written foreign actors. 702 acquired information helped the IC discover and interrupt a foreign adversary's plan to obtain sensitive technological information that could be used to undermine US national security and of course again back to the CT roots. You know, in 2009, it protected the nation from an Al-Qaeda attack by Najibullah Zazi. In 2014, 702 prevented attacks by assisting the removal of ISIS leader, Harjit Maan. And just last year in 2022, 702 contributed to, the operation against Ayman al-Zawahri, who was one of the last remaining 9/11 architects. And all of those examples that I just read are available on IC on the record. Again, as I described, when we talk about those valued examples, it's important to be really precise in how we talk about them. But when we talk in broad strokes about the power of this program, it underpin all of the key insights passed on the president's desk and it saved American lives, it is just unparalleled. So what would be lost? We would lose all of that.

- Okay. Just a follow up on that. When it initially, and the last panel discussed, and in subsequent reauthorization, most of what we've heard about justify, or you know, of the value was about terrorism, counterterrorism. And you've talked about a lot of things other than counterterrorism. Is counterterrorism still the primary, you know, or is there a way that you can kind of, you know, say which is where you see the most value? Or is-

- It's a hard question to answer because the nature and scope of the threats to the nation's security are wide ranging and multifaceted. So to put a little bit of framing around that, remember that everything the intelligence community does is applied to a set of specifically authorizing them as designated intelligence priorities. So there is a national intelligence priorities framework, which is set by the president and is updated regularly as needed to identify what are the key national security interests and concerns. What are the linchpins of what the nation needs to know in order for policymaker to be able to make the right choices around how to defend and secure the nation. So we started at national

intelligence priorities framework. And then as the previous panel described in the way that the 702 statutory framework exists from- There are some certifications that are approved by the Attorney General, approved by the Director of National Intelligence submitted to the FISC. Anything that the intelligence community does under FAA 702, both is tied to those national intelligence priorities and specifically to certifications that have been approved by the AG, the DNI, and the FISC. So we can always tie anything that we do under 702, to a specific foreign intelligence need. A specific foreign intelligence basis. And this has become probably the most agile, flexible and important tool that we have across a wide range of threats. So does it matter for strategic power competition for cyber, for counterterrorism? Yes. Matters to us all.

- Alright, so I wanted- Again, as we heard in the last panel, reauthorization is not a given, and there are a number of, particular concerns that arise to the top. One, perhaps the most important, or at least the one that you hear about the most, is the US person queries. The criticism, a criticism of 702 and how it's used is that it is sort of calm of that or way to do domestic intelligence. And the- You're not permitted, 702 does not permit targeting of US person, but certainly in collection there is a good deal of collection of US person information. So the criticisms, there have been criticisms about that. Primarily, and we heard about the FBI in the last panel. That's mostly what you've heard about. But there have also been concerns expressed about NSA's use of of US person queries. And so I'd like you to- The volume of those are significantly less than- I'd like you to talk about, why do you do US person queries? How would you do that? Well, let's sort of start there.

- Sure. It's a great question, and I have to start two steps back from that. Here's where I have to start. Every single member of the intelligence community, every person who works at NSA who deals with this authority is a US person first. We're US citizens. All of us have sworn an oath to uphold and defend the constitution. That's what we bring in the door with us. First and foremost, not one is uphold and defend the constitution. And we do that through two missions. We do it through our foreign intelligence mission and our cybersecurity mission, but we also do it through everything else we do. We do it through how we approach privacy and civil liberties. We do it through how we construct our oversight and compliance programs internal to the agency. We do it in how we conduct all of our work. So that's thing one. Is we start as Americans first. We've taken an oath to uphold and defend the constitution. And then, from an NSA perspective, what we do is we stand at the shore of the nation and look out. Remember we're a foreign intelligence agency. We stand at the shore of the nation. We look out and we're looking for those foreign threats. So when we go about looking for US person information in 702, we do it in really narrow limited circumstances in a really precise kind of reasons. I have to say, I don't think the term backdoor is a useful term. And the reason I don't think that is because not term that is grounded in law anywhere, right? There is no language in the Fourth Amendment about back doors. There's no language in the statute about back doors. It's, it's a little bit of a pejorative term, it's a bit of a shorthand and I don't think it's a useful term. I think that that particular phraseology probably sheds more heat than light. Setting that aside, and again, I told you my goal is to offer information where I perhaps stray into opinion. Please know those are my opinions alone. So in this context, why would the National Security Agency conduct US person queries? Couple of other framing things. Remember that when we're talking about queries of already collected 702 information, we're not talking about changing

anything having to do with the front end targeting. The front end targeting remains exactly as specified in the statute. Front end targeting is of non-US persons outside the US reasonably believed to possess, communicate, or receive foreign intelligence that is aligned with the certifications that have been approved by the Attorney General. The BNI, and the FISC. That's the collection. Why might we want a query for US persons in that collection? A couple of reasons. And it has to do with the same kinds of victim scenarios that Mike talked about on the previous panel, but certainly for different purposes. Again, they have no law enforcement mission, we don't carry out that kind of work. But what we do is, for example, we look to assist when a US person has been taken hostage overseas by international organizations that we might have foreign intelligence collection on. If we had a situation where there has been a US person who's been proven hostage and we have collection on the group that we believe to have them hostage, we wanna move really quickly to be able to identify any communications that might help us identify where that person in the world is so that the appropriate government actives can take steps to try rescue that person from peril and harm. Similarly, when we have indications, there's a malicious foreign cyber actor who is directing threats against the US and we have information indicating that there is a US victim, there are times when we are gonna wanna query that, that 702 collection, the collection that targeted the foreign actors to identify any information we can so that the appropriate US government entities can take steps to warn that victim or to save off that attack or to counter that attack. Those are the kinds of reasons that we do it. And I'm gonna put it up plug again for the ICM directory website, which is code by DNI. You can find a number of unclassified information pieces on that website. They give you these kinds of examples that hopefully help explain some of that. So that's the why. And you also-

- To pause on that. So it's- Everything you've said is, nothing- none of it involves US persons where you're trying to find out if they're a threat, or- Is that?

- That's absolutely right. Because we do not do reverse targeting. There's no protectional targeting and we don't do queries for purposes of trying to get at US- If there were something that we saw in intelligence collection that suggested that there might be a reason for finding a US person to be of intelligence interest, what we do then, is we follow whatever the appropriate set of procedures to seek an order from FISC under a determination that that person is acting as an agent of a foreign power, for example. So there is no way in which the queries that we do are intended to shape a targeting or to single out US persons, except in the context of again, either trying to understand things like victim notification and warning or other purposes where again, our focus is the foreign intelligence.

- Okay, now go to the house.

- Sure. Okay. So those of you in the audience here who are FISO nerds, and I'm gonna guess there's more than a handful, because otherwise why would you be here all afternoon? Know that pursuant to the statutory framework, there are a robust set of procedures that govern how the government uses this authority. So there are targeting procedures, there are minimum procedures and there are querying

procedures. So whenever NSA is going to run a US person query, and again, in this already collected universe of communications, what we do is we have to identify what is the purpose for that? What is the valid foreign intelligence purpose for that targeting? And we have to- and in fact NSA in particular, all of this preexposure goes to my office for review to provide an additional piece of overlay around the legal justification for that query of the US person. Every single query of the US person that is run by NSA is scrutinized by the Department of Justice, which have access to all of our records around those queries. And all of those query records are made available to the Office of the Director of National Intelligence for their review as well. I should say also that before anybody even gets to that point, anybody who touches 702 to information at NSA, is required to go through annual training that includes competency based testing to demonstrate that they understand the scope of the authority, the limits on the authority and how to functionally use it. So we have this training up front. We have somebody who proposes a selector for targeting or proposes a query to be run. We have the review of the query, including by my office. We have the post query review by DOJ and OD-9. And then of course we have robust and extensive compliance reporting to the FISC and to the PFOG and others.

- So, and part of what you just talked about is compliance training programs- There have been, criticisms, there have been times in the past where you've gone to court or the AIG have raised concerns about NSA's processes, protections, and compliance reviews. What can you say that, you know, that is there- What can you say to give people comfort that is, you know, isn't, I'm not to, I'm gonna quote quote, but isn't a compliance Wack-A-Mole. That was mentioned in the last panel.

- It's a really important question. We devote an enormous amount of energy and resource to oversight and compliance internally within the agency. And we do that in a lot of different ways and we've been prompted by a lot of different factors. So in the previous panel there was some discussion about court opinions from 2009, 2011, past compliance problems as a discussion for the panel. You know, one of the things that's challenging about a program like this is the complexity. You're dealing with a lot of data. You're dealing with complicated technical systems and you're dealing with people interacting with those fat data and those systems and absolutely mistakes happen. And in some cases those have been systemic mistakes. And so what happened in the wake of those was that NSA doubled down, invested heavily in building out and expanding our internal oversight and compliance structure. We have literally hundreds of personnel whose full-time job is to manage oversight and compliance around the NSA enterprise. We also have of course that full-time set of roles complimented by the training that's required by any analyst who touches information by the roles that analysts and supervisors and others take on doing things like doing audits of queries, doing audits of- Doing the multiple layers of checks before a selector was put on cover for targeting. There are checks and checks and checks and checks and checks internal within NSA. And of course anything that we find we promptly self-report to the Department of Justice to OD-9. So I think what I'm trying to say here is that- Two things, one, any errors are errors we don't want to have. We work really, really hard to drive those errors as close to the Bureau as we can. And if you look at things like the semiannual compliance report, I was pulling up one of these just before this because I wanted to remind myself of some of the numbers. Now remember there's the annual statistical transparency report and then there's also separately the semi-annual compliance report. One of those recent reports that I was looking at right before coming down here today, pointed

out that the rate of trusting errors by NSA under this program is almost zero. And the rate of detesting errors by NSA under this program is almost zero. So we try really hard to get those compliance rate error rates down as low as we can and we know it takes a significant investment of resource and effort to do that. And whenever we have identified those kinds of problems that were referred to on the earlier panel, those were systemic issues, we have taken significant action to try to correct and redress those and prevent them from happening again.

- Another issue that comes up with respect to 702 collections, is the- is the volume of incident collection of US person information. And that has been, as I understand it, the calculating that, quantifying that has been a challenge. But there has, well there this, this recent report by some Princeton researchers that suggests a way that I will not try to pretend that I understand to do that kind of calculation, to calculate the volume of incidental data. I guess my two questions are, do you agree that it is important to be able to calculate the volume and be able to be transparent about that and is NSA looking at this Princeton, or you know, or is there some other way, are you moving towards being able to do that? Is that something, you know, for the last time say we heard on the last panel because that's basically everything. But- But anyway, we did hear, you know, it is something NSA has been tasked to do on a number of occasions and hasn't happened, so maybe you can talk about that.

- Yeah, it's such a challenging problem and here's what's challenging about it. The challenge is how to calculate or assess the proportional volume of incidental US person communications that are collected in a privacy protective way. That's the challenge. Cause remember, what do we do? We stand at the shores of the nation and we look out and what we're looking for is foreign intelligence information that is specifically aligned with the foreign intelligence needs that are identified in those certifications and flow down from the NIPF. So that's what we're looking for. What NSA doesn't do, what you probably wouldn't want NSA to do, is to maintain some kind of comprehensive list of US person identifiers. That's not our role. So, and when we are, when we're looking at collective communications for foreign intelligence purposes and we encounter something that is unknown, we don't necessarily know if it's a US person or not. If we have no reason to look at a communication at all, it's not responsive to any foreign intelligence query. And the only reason we're looking for it is to try to find out if there's a US person who made a communication that's not of foreign intelligence interest and raises really important privacy concerns. That's what we've been grappling with. Now, having talked about all that in terms of the complexity and challenge, we absolutely recognize how much input there is in this and how much input there's been in this question for a number of years now. So when the Princeton paper came out, we did look at it and there's a few issues with that particular proposal that have to do with both the math and the authority. So in terms of the math, it essentially, for those who aren't familiar with it, it involves combining data sets acquired from electronic communication service providers with data collected by the intelligence community and encrypting it all and sort of mashing it together. So the approach that the researchers have proposed is to protect that with a particular level of encryption. From an NSA perspective. You know, one of the things, one of the things we do, right, we have two missions. One of them is cybersecurity and information assurance. And we've got a lot of guidance around encryption standards. We believe it's really, really important if somebody's gonna pursue that kind of comprehensive use of information of US persons that it be done in a way that applies quantum

resistant encryption. So this particular proposal didn't apply that level of encryption. So that's a math difference of view, right? But it brings us to the second point, which is if you try to apply the same methodology using quantum resistant encryption, it's not clear that it's computational feasible because then you start to require a level of compute processing that may just not be possible. Again, that's a bit of a math debate to have, but it brings us to the third issue, which is, as the researchers themselves pointed out in the paper, because of the way they've proposed combining the information, it might very well require some kind of congressional authorization or approval to make that a lawful thing to do. So all of that said, that's not in any way to reject out of hand the ideas in the paper. And we really welcome this debate. I mean, we have tried, we have invested a lot of time and effort in trying to come up with solutions and we are happy to keep having that conversation and anything that helps advance it, again, we understand the level of interest. We just wanna be sure that there's an approach that is privacy protective.

- Okay, well I'm getting hands waved at me over there because we're past time. Do we have time for audience question?

- [Host] One question.

- One question. Yeah. I had other questions for you, but I think it's more important to get one from the audience

- Right there.

- Okay. Yes.

- [Audience Member] Professor DeRosa, So quick question, I was wondering if you had any reaction to the EDP European Data Protection Bureau board?

- Can you speak up just a little?

- [Audience Member] Yeah. If you had any reaction to the European Data Protection Board's opinion on the Biden data privacy?

- So the EO 14086, the executive order that was signed out in the fall regarding the application of privacy protections to persons around the world is something that, you know, sorry, Mary, I'm gonna say this as mentioned by people on the previous panel, really it is extraordinary for leaning. I mean, I do believe this is an- a proactive extension of formalized privacy protections, to non-citizens of the country that goes beyond anything that we've seen from any other nation in the world. And so the conversations that have been happening between the administration and European Commission on that have been robust. They have led to the framework that's shared in the EO and, you know, as one of the panelists mentioned earlier, we will have to see, you know, whether or not that gets a challenge in the CJEU. We're certainly looking forward to seeing that final determination from the European Commission on the adequacy. But I think that- I think that leads the world in terms of the level of transparency and the extension of protections to non-citizens of a nation. It's just an extraordinary framework when taken in the context of national security activities around the globe.

- Okay, well,