- Hey, why don't we go ahead and get started. It is my great pleasure to welcome everybody here today. I'm Laura Donohue. I'm a professor here at Georgetown and Director of the Center on National Security. And I'd like to thank the American Bar Association. I saw Holly was here earlier, I saw Holly, the great Holly, and the Standing Committee on National Security and Law School for co-sponsoring this discussion with us. As everybody here, like we know Section 702 is heating up, it is coming up for renewal in December of this year. There are many, many issues to discuss and it was seen by all of us here at Georgetown that this would be a proficuous time to step up and really engage in the conversation in a really meaningful way to try to move the ball forward. So I am thrilled by today's speakers. If I could put together a dream lineup, this is it, for actually discussing FISA and Section 702 and all of the issues that we see. So the program for today is we're gonna start out with a panel. Following this, we will have a keynote address by April Doss, who's the General Counsel of the National Security Agency. She and Professor Mary DeRosa will be a lot of the issues that are really at the forefront of this discussion. And following that we'll have a second panel, which my friend and colleague, Mary McCord, Professor Mary McCord here at Georgetown will be moderating. I'd like to start out by introducing our panels on the first panel. Our emphasis here is going to be on the issues right now surrounding Section 702, how it works and what the questions are with which we're represented going into the renewal debates. First I'd like to introduce Wyndee Parker, who's the National Security Advisor for the Office of Democratic Leader, that's New York Congressman, Hakeem Jeffries, in the US House of Representatives, sitting to my left. From 2009 to 2023, Ms. Parker served as the former speaker of the House, Nancy Pelosi's, National Security Advisor. Prior to that, she served as the Deputy Staff Director and General Counsel of the House Permanent Select Committee on Intelligence. Ms. Parker also has served on the American Bar Association Standing Committee on Law and National Security. And she holds her bachelor's from Duke and a JD from Ohio State University College of Law. Wyndee, welcome. In August of 2022, Mike Herrington, who's sitting to the far left, he joined the office of the FBI as Senior Operations Advisor for FISA Section 702 reauthorization. So he, like Wyndee, is right in the middle of all of these debates. He has investigated computer intrusion matters in the FBI for over 15 years, and he recently served as a Section Chief at the FBI's Cyber Division. Prior to that, Mr. Herrington served as an assistant special agent in charge of the FBI's Los Angeles field office and in Richmond, Virginia as well, and prior to that, in San Francisco, my own hometown. He holds a BS in electrical engineering from the United States Military Academy at West Point and an MS in Information Technology Management from Carnegie Mellon. Welcome, Mike. Sharon Bradford Franklin. Sitting in between Wyndee and Mike is the Chair of the Privacy and Civil Liberties Oversight Board. Prior to her appointment, Ms. Franklin served as co-director of the security and surveillance project at the Center for Democracy and Technology, as well as Policy Director for New America's Open Technology Institute. From 2013 to 2017 Mrs. Franklin served as Executive Director of PCLOB. She began her legal career as a judicial clerk to Honorable Jane Roth, and she graduated from Harvard College and Yale Law School. Welcome. Brad Wiegmann, sitting to the far right, my far right, has served as Deputy Assistant Attorney General for National Security since March of 2009 at the United States Department of Justice National Security Division. He has been a career government attorney for 27 years, having previously served at the Departments of Defense and State and at the National Security Council. Most of his career has been focused on national security and international law, including counter-terrorism, counterintelligence, counterproliferation, cyber policy, economic sanctions, the law of armed conflict and related litigation and policy matters. He is a summa cum laude graduate of Duke University and magna cum laude graduate of Harvard Law. Welcome, Brad. Next to Brad is Liza Goitein. She is a Senior

Director of Brennan Center for Justices Liberty and National Security Program. Liza is a, sorry, Ms. Goitein, I should say, is an internationally recognized expert on presidential emergency powers, government surveillance and government secrecy. She's testified numerous times before the Senate and House Judiciary Committees. And she previously served as counsel to Senator Feingold, Chair of the Constitution subcommittee of the Senate Judiciary Committee. As well as she was also a trial attorney in the federal program's branch for the Civil Division at DOJ. She graduated from Yale Law School and clerked for the Honorable Michael Daley Hawkins on US Court of Appeals for the Ninth Circuit. Welcome, Goitein. Finally, to my right is Chris Fonzone, who was sworn in as ODNI, I'm sorry, State Office of the Director of National Intelligence General Counsel on June 24th of 2021. During the Obama Administration, he served as Deputy Assistant and Deputy Counsel to the president and legal advisor of the NSC. Before his tenure at the White House, Mr. Fonzone served as special counsel to the general counsel at the Department of Defense. He also worked at the Department of Justice at OLC, the Office of Legal Counsel and on the Civil Division Appellate Staff. He clerked for Stephen Breyer, the Supreme Court, and Judge Harvey Wilkinson, Court of Appeals for the fourth Circuit. He attended Cornell University and Harvard Law. Welcome, Chris. All right, so let's jump into it and get to it. I'd like to start out just to create a kind of a common understanding of where we are. What are the origins of Section 702 that's now up for renewal? And how has this evolved really since its enactment in 2008 and then 2012, 2017 that brought us at this point in time? And I'm gonna turn to Wyndee as we saw she was in the middle of these debates throughout that time and really well placed to help us understand congressional understanding and kind of the crafting of Section 702. Wyndee.

- Thank you. Okay, great. I think a lot of us were shocked and stunned when heard in December of 2005 through "The New York Times," that there was warrantless surveillance going on inside of, well, by our government outside of FISA. Those who otherwise had dealt with FISA for many years had thought that that was like a holy grail and very sacred. And we also reminded that following 9/11 we asked what changes is, if any, are necessary to FISA to deal with the threat that we faced following September 11th. Following that, we engaged in the following years in detailed and lengthy discussions for the executive branch who insisted that they needed authorities to surveil people or one ended communications that were outside of the United States, non-US persons who were reasoned of being located out of the site of the United States. In 2007, the democratically controlled House did pass the Restore Act. It was designed to provide the authorities of the executive branch that it needed, but also had a lot of civil liberties and privacy protections woven in. The Bush Administration rejected those efforts and said that that bill was not sufficient. And what followed was in 2007 we passed the bill that, the Protect America Act. And one of the key things of the Protect America Act, it was, we called it the Umbrella Surveillance Program that did allow collection to go forward without FISA court approval. It did so by removing from the definition of optional surveillance, the surveillance of people reasonably assumed to be located out the side of the United States. Importantly, and this is critical for many people, including Democrats who voted for that bill, the Protect America Act, it contained a six-month that forced the Congress and the executive branch to work very closely together to figure out kind of a long term solution. That long term solution was found in the FISA Amendments Act of 2008. And that bill and that piece that that statute contains, 702, which is what we're here to discuss today. The debate that went back and forth was very intense in the lead up to the 2008 bill. There were key discussions about the authorities and whether or not they would be, you know, sufficient to ensure privacy and liberties protections and also give the

executive branch the flexibility to engage the type of surveillance that it needed. Also, in liability, immunity liability for the telecommunications providers was also a key point of debate. In the House we had members who insisted that liability protection should not be given unless and until the administration fully complied with congressional requests to turn over requested information related to the previous programs that were conducted following 9/11. So here we are today and we are on our, you know, we've renewed Section 702 as well as various other aspects of the FISA Amendments Act multiple times and we're postured to do it again.

- Okay, thank you. So we have traditional FISA, we're the church committee, right? And Rockefeller and Pike Commission that come together and find all of these abusives. And we have a 1978, the Foreign Intelligence Surveillance Act introduced. And it sounds like congressional understanding was that all foreign intelligence would be conducted through FISA. There was also a statement in FISA this would be the sole means for the collection. But then was stellar win, post 9/11, we have this program operating entirely outside of FISA and efforts subsequently by Jack Goldsmith and others at OLC to try to fit that into the FISA framework. So when Congress found out they were surprised, right? That all of this was going on. And so then we have the 2008 FAA, the FISA Amendments Act. And that's where we get Title VII of FISA which actually introduces three provisions. So we have Section 702, which is for non-US persons reasonably believed to be overseas where we intercept in the United States as . Then we have 703, which I'd like to hear a little bit more from 703 and 704 because this is the first time we saw protections for US persons with anything approximating a warrant procedure outside the United States because after , of course and Chief Justice Rehnquist, we don't have a warrant requirement to US persons overseas. We just have the reasonable requirement under the force. So can you talk about 703 and 704 as well?

- Yeah, so we did have like Attorney General protections, or excuse me, we did have a requirement that the Attorney General had to approve that collection of US persons oversees and it was embodied in an executive order. And so we decided that that should be folded in statute, 703.

- So you codified the executive, well, the guidelines under section 12 until 3 to bring 703 and 704, fair. Okay, great. So under 702 we have five requirements, right? You cannot target a person in the United States. You can't engage in reverse targeting. That's, you know, if you know that, you know, I talk to my grandma all the time and she lives in Paris, stationed as non-US person in Paris, you can't target grandma trying to get at the person in the United States. So no reverse targeting under the statute. You can't target US persons under the statute. You can't intercept wholly domestic conversations. And it has to be consistent of the court, right? Those are the requirements for Section 702. And all three of these provisions, 702, 703, and 704 are absolute renewal. So Chris, I'm gonna turn to you. How does it actually work in practice? What are the logistics of 702, 703?

- Sure, one point just add on the prior discussion, I think that you made the point that Congress thought all Foreign Intelligence , and I think that's not true of Foreign Intelligence instructed outside the United

States can ties this person which has always been done in the present constitutional authority, and I think 702 way to find a compromise between that type of intelligence collection and the intelligence collection was being done under what's traditionally called Title I or traditional FISA. So basically what what FISA is today, and I think this is, it's been amended but basically the law of passed in 2008, there's a law that allows an IC to target non-US persons look at outside the United States for possess or expect to communicate foreign intelligence with the system of US electronics communication service providers and requires the IC to do incentive, follow certain privacy protections. And then it creates a framework that's overseen by all three branches of government. And the way that this works in practice is as follows, it's sort of a process that happens every year. So every year on an annual basis, my boss, DNI, CAG, staff to submit to the Foreign Intelligence Surveillance Court things that are called certifications scribe categories of foreign intelligence that the intelligence can use to authorize to obtain under Section 702. Alongside those certifications, the AG and DNI also submit a set of rules that will follow in using Section 702. Specifically, those rules are rules designed to ensure that 702 is used only to target non-US persons who locate outside the United States, rules of safeguard any US person information of the ICF teams by targeting US persons. So for example, if a non-US person target is in communication with US person or mention the US person in communication, yes, he must follow certain rules to safeguard that information. Rules of state when and how the information may be theory between foreign intelligence and rules for how the information may be shared and how long they be retained. So every year the sent this package with these certifications and these rules they will follow in collecting intelligence over the certifications. And the states have to review them to make sure they comply with FISA, and as Laura said, the fourth amendment. And then if they feel like they meet those standards, the FISA will write a written opinion that will provide the executive branch saying that we approved the use of 702 this year. Once the executive branch gets that opinion, the AG and DNI can then write written directives that compel US communication service providers to assist with 702 collection. So that's the sort of first phase of the process. The second phase is after providing those directives, the government can submit specific foreign intelligence targets to the companies without having to go back to the court in each instance. So as when Wyndee said earlier, this is a umbrella authority, it basically doesn't require the approval of each individual target approves a program and the executive branch will give the targets to the companies after the program's approved. To submit a specific target, however, it's not like the executive branch can excuse anyone they want. They have to make report a specific basis, a basis or targeting a specific selector like a phone number, her email address, assessing that the target recognized that selector is anonymous person located outside the United States and that that person will communicate, possess or receive foreign intelligence information. So the executive may just make the written determination to find and again pass along to people who received the directives who assist on selecting intelligence. After that's done, DOJ reviews those targets targeting determinations to make sure they comply the law. My office at the DNI and also our privacy's office and DOJ engage in more systematic oversight of the program. And then there reporting requirements to both the American public and congressional judiciary committees instances non compliance have reported back to FISA. So it's programmed in all three branches of government have a role in overseeing.

- Okay, and we started with 89,000 targets in 2017. That's the first numbers that we have. We're now up to about 232,000 targets that are determined by the AG and DNI that nobody actually sees the targets. They just sign off on a certification of targeting procedures. So FBI, you know, actually that's right, this

will sound very familiar to you that this is incredibly effective, this program, and it's very, very useful. Can you talk a little bit about how it's used in terms of it's effective?

- Right, absolutely. So I think to really understand the value that the DNI gets outta this to understand our unique role in the intelligence community, which we are responsible in a way that no other ICA agency is for addressing threats to United States homeland and civil Americans. And so our use of the 703 bargain is very tightly tailored to that. And in fact we will only receive collection under Section 702 if it is relevant to one of our pending open national security investigations. So we're not going receive collection otherwise as that's works out to you at the beginning of this year, about 3.2% of the total collection in the IC not under 702. So that's a quantitative difference, but qualitative difference is just as important, which is if we are receiving information under 702, it's based on a non-US person located overseas who has some sort of connection to one of the national security threats that the FBI specifically investigates. So counterterrorism and counterintelligence, proliferation of weapons and mass disruption, foreign cyber activity. So our collection is tightly tailored around our use in that. And one thing that we've found in addressing all of those threats is that in today's environment, the primary threats, national security threats to the United States are located overseas. So it's really crucial for us to have this ability in these non-US persons located overseas so we can see outwards so we're able to protect ourselves inwards. And 702 is really those agile and deficient tool that we have to do that. And that agility is particularly important 'cause in our today's technology environments, one thing that we've seen is that these foreign adversaries are able to move very quickly, even within hours or sometimes minutes, they're able to move on the new accounts. And it's very difficult for us to move with the speed where we can actually keep up with them and maintain visibility without the agility that the 702 affords us. So how does that look in practice? I mean, we really use this across all of our national security authorities and it's crucially important in doing so. And counterterrorism, which was, you know, earlier on, our largest use of this, which has actually been reduced over the past years, gone more towards our counterintelligence cyber emissions. But it still remains a crucial portion of our counterterrorism mission. And it has even saved lives. This is our way of being able to keep paths on foreign terrorist organizations to see who they're attempting to recruit or get into the homeland who attempt to do us harm for our foreign intelligence and counterintelligence permissions who allows us to keep tabs on those foreign intelligence officers located overseas. We're seeking to recruit US persons to collect information or engage in other claim best sign intelligence information within the United States, steal our technologies, our sensitive intelligence. And, you know, probably our largest use right now is in our cyber realm where we see, again, highly sophisticated and aggressive cyber adversaries, many of which work for and exist overseas and work for foreign intelligence services move around quickly, as I said, because of the technology environment, but also this is just crucial for us to see what they're doing. And we've used this, for example, to see critical infrastructure and being able to disrupt those before they can do damage or cut off damage before further damage can be done. Subsection two is incredibly important in finding some of the details that we need to go out and conduct an effective victim notification with, for example, cyber victims. So we can actually provide them actionable intelligence to allow them to find an intrusion on their network and then we can work with them to get that out as opposed to just telling them you've been hacked, good luck with that.

- So if that really relies on this, and I think it's worth noting that all the other agencies combined, right? If you look at, you know, NST, or if you look at CIA and National Counterterrorism Center and the NSA, together, they query this data approximately 7,400 times a year. But the FBI, when the numbers finally came out, it kind of surprised everybody last spring. It's almost 3.4 million times a year. So you're kind of a heavy user of this raw data that's coming up. Do you wanna comment? Are all 3.4 million to counterterrorism and so on, or is there kind of more going on there within the CIA?

- Yeah, no, that's a great question. So there's a lot going on there. And I would say that the 3.4 million applies to calendar year 2021. I'm not getting out ahead of the by Friday by saying that we had, because director has already said this, we had a approximately 94% drop in that number of those queries into 2022 in the wake of a series of major reforms that we did in 2021 and 2023, which we're getting into later. I don't wanna get get too much into that now, but regardless you have 200,000, which is the 2022 number, about 200,000 is still far more than our other counterpart agencies do. And that is because of our focus on protecting the homeland and protecting Americans. So we are very much interested in this foreign outward looking collection, identifying that information that is relevant to protecting that inward looking victims and threats against the United States. So while our collection is like the other intelligence agencies focused outward on those non-US persons located overseas, what we are looking for that has specifically is how they are looking to target Americans, American companies, American institutions and homeland itself. So that is one of the factors for why we're querying this so much more with US person related terms. A couple of other factors that play into there. One is our batch querying where if we do a large batch query, we are going to count all of those terms as a US person term if even one of them is. So we are applying that extra protection is afforded US persons to every single term in a badge where we can't necessarily separate out which ones are us persons, which ones we're treating as US persons under the presumptions in our policies and which ones are non-US persons. So that's gonna increase our number. Also, what is going to increase our number is what I alluded to which is presumptions. In many cases these query terms are, we don't necessarily know exactly who they pertain to when they come into our possession with TIM or some sort of other intelligence collection. So if we don't know this specific person or the US person's status of the specific person that indicator explained it to, we will apply the presumptions which are defined in our policies and we'll say that we're treating this person as US person and providing that additional protection. And those are counted among our numbers as well.

- Okay, Liza, you've written a lot about this and just security. We have two parts, right, that you've done part one and part two on 702. All 3.4 million, are they compliant with the statutory provisions? Are these sufficient explanations? Your thoughts?

- Is this on? Okay. Sure, thank you, Laura. So we did hear about some of the ways in which Section 702 have been used in order to collect intelligence about foreigners abroad who pose threats to the United States because they're engaged in cyber attacks or terrorism or deliberation of weapons of mass destruction. If that were all the Section 702 were used for, we wouldn't be here today. The reason why Section 702 is so controversial and the reason why its reauthorization is in doubt is because it has become a rich source of wordless access to America's communications. Now, how did this happen?

Section 702 surveillance invariably pulls in large volumes of Americans communications because Americans communicate with foreigners. This is generally referred to as incidental collection because the targets are supposed to be the foreigners, not the Americans. If the government's intent were to actually spy on those Americans, it would have to get either a warrant in a criminal investigation or a FISA Title I order in a foreign intelligence investigation. That's another type of individualized probable cause order. So what Congress did in Section 702 to try to keep the government from using it as an end run around these requirements was two things. First, it required the government to minimize the sharing, retention and use of this incidentally collected information. And second, it required the government to certify on an annual basis, so it was not engaged in reverse targeting, meaning it's not using Section 702 to spy on Americans. What's become abundantly clear over the last 15 years is that these protections have failed. Rather than actually minimize this sharing and retention of America's communications, the NSA routinely shares raw Section 702 data, including Americans communications with the FBI, the CIA and the NCTC, National Counterterrorism Center. And all of these agencies retain the data for a functional minimum of five years with several exceptions that allow retention for much longer periods. In addition, all of the agencies have procedures which the FISA court has approved that allow them to search through the Section 702 data for Americans phone calls, text messages and emails. So having obtained the data without a warrant based on a certification that they were not seeking to access the communications of particular known Americans once the information is in their hands, all the agencies served with looking for the communications on particular known Americans, that is a bait and switch that undermines the spirit, if not the letter of the prohibition on reverse targeting and increases an enormous hole in the Fourth Amendment. The FBI reportedly conducted 200,000 of these backdoor searches in 2022, that's less than 3.4 million, but it's still more than 500 warrantless searches for Americans communications each day. And they were not all for the purposes of trying to identify victims. And hopefully I'll just talk more about that later. Congress and the FISA Court have attempted to reign in these back circuits at least a little bit by imposing some limitation on them. But-

- Sorry, can I just interrupt you? Can you give some examples of the ones that don't count in your view that actually have been discussed in the press and certainly in the biannual -

- Yeah, I promise I'm getting to that. Yeah, so I will give you those examples but I wanna talk first about Congress's requirement that it impose in 2018 that the FBI obtained a warrant before accessing Americans communications in a very, very small subset of US personal queries. I think we'll be talking more about that later as well. According to the ODNI Statistical Annual Report, this requirement has been triggered about a hundred times, actually, probably likely more than a hundred times. According to that same report, the FBI has never once complied with it. That's a 0% compliance rate for the statutory warrant . Outside of his narrow category, the FISA Court has approved a rule that allows the FBI to conduct US person queries if the query is reasonably likely to return foreign intelligence or evidence of the crime, that's a pretty low bar. Nonetheless, the FISA Court has found on multiple occasions over the last few years that the FBI has engaged in, quote, "widespread violations of this minimal rule." And to give you some examples, the FBI has run queries for a US congressman; a local political party; multiple US government officials, journalists and political commentators; two Muslim American men who stole a fence that a witness saw them loading boxes into a vehicle; people who applied to participate in an FBI

citizens academy, religious community and business leaders who are applied to do that; repairmen, who came to the FBI to fix things. There is a long list of some pretty disturbing violations of fifth of this minimal internal standard. Now, I know we're going to be hearing about some of the changes that the department has made, some new internal guidance and procedures and training and all of that. And again, I hope that later I'll have a chance to explain, I'm a little bit skeptical of those improvements, but just more importantly, even if the FBI could ensure a hundred percent compliance with its internal rules, an internal determination that a search is reasonably likely to return evidence of a crime or intelligence is not a warrant, it is not a probable cause showing to a court. And that is what the Fourth Amendment demands when the government wants to access Americans emails and text messages and phone calls. As just as Chief Justice Don Roberts said in 2014 in a Fourth Amendment case that's actually strikingly analogous in Section 702, that founders did not fight a revolution to gain access to government agency protocols. So I'll leave it there for now.

- Okay, sure.

- Thank you. So I just wanted to start out thank you by noting that I am here in my individual official capacity. The Privacy and Civil Liberties Oversight Board, we are five member bipartisan board, and I'm speaking for myself and not necessarily any of my fellow board members. I also just wanna note by way background, back in 2014, the Privacy and Civil Liberties Oversight Board published a fairly comprehensive review of Section 702. We are now engaged in updating that and deepen the leads and working through toward our new report. So by the way background, I'm here. So I wanna speak to two aspects of what's been on the table just now. First, is with regard to incidental collection as has been described, that's, you know, when an American is on the other end of a communication with a non-US person target outside the United States. And as Mike described, we want to know, right? So the validity to reverse targeting is prohibited, can be contextual, but we actually want to know who the valid targets are talking to inside the United States, if they're boding with . It's very center. So incidental collection is a feature and not a bug of 702. It's deliberate, it's intentional and I would say, it's something that can help protect us. However, Americans, they can't be targeted, but their communications are entitled for amendment protection, as Liza was just describing. So the scope of that incident role collection matters. And one issue that is hopefully in play now again as 702 comes up for reauthorization is trying to get a sense of what is that scope of collection. When the issued its report in 2014, one of the recommendations was that the IC developed a number of metrics to help give insight into the scope of that collection. And at the time, as I said, well, some of these, not all these will work with you, but ultimately the IC announced actually we, it is infeasible for us to develop a meaningful estimate of the scope against incidental collection of information. Now, I'll mention there have been since that time some professor at the Princeton, who have put out a paper that seems like worth exploring. I am not a sophisticated techie to be at the weeds and understanding exactly proposal, but as I said, worth exploring. But bottom line is, in my view, the difference here is over what is meaningful to policymakers. And when the alternative is having no estimate. An estimate that has some more error can still be, in my view, meaningful to Congress. And so I hope that that is an area to assess. The other piece I just wanna speak to quickly is on this issue of what the government calls and queries, what privacy advocates refer to as backdoor searches. And as Liza with outlining, we do have the Fourth Amendment issues here

where Americans communications should be protected by Fourth Amendment. and when there's no judicial review at the front end, understandably, legitimately because those target are not people with recognized Fourth Amendment rights, when it comes time of the government to go searching through those collective communications, seeking the information of a specific American, specific person who has recognized Fourth Amendment rights, in my view, that should require independent judicial review. And so this is a place where I will be urging Congress to incorporate a requirement for by support review of those US person theory terms. Hey, fortunately we have lots of lawyers in the room, but one in particular from DOJ. So Fourth Amendment search?

- See if I can figure out, okay, so it works. Okay, so we heard a lot about the Fourth Amendment. Let's talk about what the courts have held in this area. So the FISA Court has approved, as Chris mentioned, this program every year since 2008, it was adopted. Knowing the US persons credits have have existed and have approved program has consistent with the Forth Amendment every time. So there are some of that in this report. Remember these are district board judges from all over the country, regular district board judges. eight of them, eight different ones over that time period have approved this found consistent with the Fourth Amendment. This program has also been come up in criminal cases. Relatively rare, but sometimes we use vice information in the criminal context and this issue has come up. Every district board that has considered the issue of US person first has also found it consisted with the Fourth Amendment. Again, what their conclusion is this the data that the government has already lawfully collected. It is not a Fourth Amendment search to go through information that is already lawfully in your custody in this context. That's what the courts have included. There have been three courts of appeal as well that have considered the constitutionality of Section 702. They didn't actually get into the issue of the queries for the most part, but all of them above the constitutionality of Section 702. There's one case in the Second Circuit is the only case in which they consider whether a query is an event. They consider that it might be a Fourth Amendment event, but even that court did not impose a warrant requirement. So there's no court has ever found that there's a warrant requirement for US person queries. This is also important to understand consistent with Congress's understanding, we've currently characterize the backdoor searches, but Congress is well aware that the government will be searching for US person information in this data when it was passed. You look at the report that authorized this, they said that they said exactly what Ron State telling me today that queries of this information for Fourth Amendment, I mean for US person information are not Fourth Amendment searches. That was Congress's understanding at the time when this program was adopted. So this is also consistent with case law in other areas, but there's a Supreme Court case involving searching DNA databases where they said that searching through DNA that the government has lawfully collected to find bad guys and matches is consistent with the Fourth Amendment. So, that's the first thing just on the law. The second point I'd like to make is about practice most practical, in light of what Mike said about the number of queries, 200,000 in FBI or even if you excluded those and cut that number in half or considered only the ones that that NSA and the other agencies do, which is less than 10,000. There's no practical way that we can do that volume queries and apply for probable cause of warrants in the FISA Court. The highest number of FISAs that we've ever had in the FISA Court is about 2000 or so queries. So multiplying that by tens of thousands would be impossible for this court and for the large department to do. So, while it sounds like a good proposal, there's there's no way that we could do that. There's no way. Also, a lot of people, the whole purpose of 702 is not to have a probable cause standard for this.

And so this would really take us backwards from the whole purpose of having 702. We just don't have the resources and it's not practical to adopt this conclusion. Third thing I would say is, is not like as if we don't have rules. We do have every single, as Chris mentioned, every single targeting decision is written down by the targeting agency by MSA and reviewed by attorneys at the Justice Department who have to conclude whether the standard is met and report it in confined errors to the defense. So we have an alternative mechanism that we think is more efficient. We do report those compliance errors, and they do come up, and they're reported to the Fisk and can take legal action and so forth has as it sees fit. So it's not that there's been an area where there is no oversight. We do have rigorous oversight. It's just done through a different mechanism that's more efficient. The one thing I guess maybe the last thing I would say is, look, we operate in a competitive intelligence environment, obviously we're a country that respects the rule of law and cares deeply about similarities. Any compliance problems are a problem for us. And we'll talk about the reasons why we have some of those and what we can talk about the steps that we're taking, and Liza's right, we have had some problems in making sure that we follow the rules that we set for ourselves, and we make no excuses for those and we need to do better on those. But we have, I've been spending a lot of time evaluating what some of our other countries do in this area. Obviously countries that don't respect the rule of law like Russia and China have none of these constraints and we're in a competitive environment with them and work Korea and so forth. But we also look for our allies, other countries that share our values in France, Germany, UK and so forth. And while they also have rigorous privacy protections, I don't think we'll find any system in the world that has the type level of rigor, what we're talking about here in terms of oversight of this type of collection, which all these other countries also do, including what rules on how big queries were data they've already collected. So I think it's important to keep this in context. And how close with that.

- Thank you very much. So quick clarification, and then Wyndee and then Liza. On the Fisk 2000 limit, right under Title I, Title III, 2000 is really the most per year that we've had. Does your critique hold if magistrate judges or ordinary judges can do it enough to assist judges for a search of the database?

- Yeah, I think, I mean, I think we couldn't flood, you know, all in words if you opened it up and said we're not gonna have these things centralized in the Fisk, which the whole purpose of having a Fisk is to centralized in place that can handle classified information to help expertise in this area and so forth to be able to handle this in one centralized place. If you threw it out the window and said we're gonna have mastery judges all over the country do that, that would mitigate it to some extent. We create other problems doing that. I still don't think they could handle the volume that we're talking about of queries when you're talking about in a case of this, say you have 200,000 in queries, imagine what the lawyers would have to fan out all over the country on a regular basis. You have a daily drum beat of these all the time. It's just not practical.

- Great, thank you. So I hear , I think.

- Okay, so I just would note that, you know, Brad, I understand what you're saying about the court amendment, our kinda understanding of it at the time, but I also, you know, its important that, you know, like Congress and American public, they reassured that reverse targeting really wasn't occurring. I mean, that was totally key to FISA 702. That is a cornerstone of it. And so as such, when we did the reauthorization of FISA in 2018, we did in institute something that didn't go far as far as some people would've liked with respect to establishing kind of a court order requirement. But it did require a court order based on probable cause when FBI criminal investigators, non the national security side, but the criminal side wanted to review the contents of communications that were returned as a result of a US person theory. And so, you know, so it kind of reflects that Congress had this like lingering concern about, again, reverse targeting and also the collection of US person information and specifically the contents of the communications as opposed to metadata which has traditionally been seen as being, you know, kind of having less protections or deserving less protections than your actual contents of your communications. Also, with respect to the compliance issues, thank you for bringing that up too, that has really, really undermined I think efforts related to instilled confidence in the American public and in the Congress about FISA and those who are conducting operations. I'm glad that those compliance matters have been kind of discovered and uncovered and shared, but there will be more that's needed. And I think that that's also going to play into the reauthorization process this year. It's great when we have kind of the Department of Justice, the FBI taking steps to address these in-house, the IG also, the Attorney General, excuse me, the DOJ and AG taking critical steps too to, you know, do these reviews and compliance reviews. But we still need to ensure statutorily to that there are additional limits and I think that will be debated as we move forward perspective.

- So on the F2 orders, there's never been an order applied for, even though more than a hundred times the FBI has been clearing it as exactly what contracts anticipated. Can you comment a little bit on that?

- No, to say it's extremely affirming.

- That they're not following the statutory procedures?

- Yes, actually.

- Okay, Liza.

- Here.

- Thanks. And just a couple of quick points, mostly in response to Brad. First of all, in terms of the constitutionality, this is an issue that is very, very far settled. The FISA Court has approved the

constitutionality of Section 702 surveillance consistently. Among the handful of federal courts that have had a chance to review this, there's actually a divide among the judges. It's true that the district courts that have looked at backdoor searches, again, not very many of them have upheld them as constitutional. They have relied very heavily on a misrepresentation that the Department of Justice made in litigation. And as a former Department of Justice employee, I did not say that like that, but I went back and read the brief and I also read how the decisions referred to brief. The department told the courts that in the course that minimization requires the government to review Americans communications in any event. And what the courts found was that the intrusion occasion by US person queries was less than the intrusion that's required in general by minimization. That is not an accurate characterization of minimization. So I think you have to take these district court decisions with a heavy grain of salt. Among the court of appeals to them basically said it's not an issue here. In the 10th Circuit, the two of the judges said it's not an issue. The third judge says, I think it's an issue. I think there probably was a background search here, even though the other two judges weren't short whether there was a backwards search, and I think that would be unconstitutional without a warrant. And then in the Second Circuit case, the courts account there were serious constitutional concerns with warrantless factor of searches and they remanded to the district court the reason they didn't require a warrant was because they needed more fact finding from the district court because there are certain searches that would be exempted from the warrant requirement 'cause of certain exceptions of emergency and such. So that is a more complete picture of where the courts have held. This is still very much unsettled case law, and it's unsettled in context outside 702 as well. What kinds of limits apply when data is collected. And then one very quick thing, the fact that, there's a case, I think it's a Supreme Court case, might be part of appeals and I'll try to find it, but where the court held or stated the fact that the government would be required to obtain a large amount of warrants is not an argument against a warrant, right? Presumably there wouldn't be 200,000 warrant applications because presumably the government doesn't have probable cause in a lot of these cases 'cause it's not required to. So it's going to apply in fewer cases, it's going to conduct your searches of America's communications. That is a feature of the Fourth Amendment, and not a bug.

- Let me push back just a little bit on that. So you are right in terms of the geographic course, which were the Fisk, when they were collecting abouts communications upstream, that's when the Fisk said there is a Fourth Amendment problem here. But as soon as they got rid of abouts collection, then the court said, okay, no longer Fourth Amendment problem. What's your response to that?

- Yeah. No, I'm not denying that's the Fisk had held that backdoor searches are not a separate Fourth Amendment event and they don't have to be defeated as a separate Fourth Amendment event. Other judges have held differently. Constitutional scholars have written about this. , a very prominent Fourth Amendment scholar said, you know, I think that this is wrong. I think a backdoor searches of a separate Fourth Amendment event, this is all evolving, the fifth operating in an echo chamber and we tend to see, I don't think they're a rubber stamped by any means, but I think it's very plain reading their opinions that they see their job as getting to us. And so I think as we see more and more of these cases going through the regular courts, we're gonna start seeing some decisions going their way.

- Okay, Brad, on the Fourth Amendment?

- Yeah, so without debating Liza's read on some of the cases, I just respectfully disagree that there's never been a case where anyone has applied a warrant requirement. So the fact remains, no one has ever held the warrant requirements applicable. And I think we have to remember, put this in context for talking about incidental collection. You have a regular Title III wire tab. Chris and I are talking, I'm sure. Chris get caught up in it 'cause he's calling me on the phone. There's no warrant with respect to Chris, but we can pull through that information, we can use it against Chris and I can look at other wire tap information, see if I can find that information on Chris. Or let's say Sharon gives me, you know, is a walk-in and gives me a laptop full of information on it, could have lots of useful information on it. We can search through that data. We don't have to go get a warrant when she's provided that to the government, or it's a consent. So Mike gave me consent to search his house and I get tons of information on other people that live in Mike's house 'cause he's given me consent. There's no warrant to them, but we can search through that information and get all the time. This is what the government does every day with all manner of information that they have about US persons. To conclude otherwise we have a going to court all the time with in all manner of other consents just to try to get that access today that's already in our possession. And to adopt this rule that we have to go back to court all the time is just simply impactful.

- Sure. So I'll just say a couple of things there. First of all with the Title III wire tap example, of course there is an individualized judicial review at the front end. So that provides some level of protection for your communications being collected. I know, and then you gave consent as an example, which, so another recognized exception, both court amendment.

- That's non-US person status outside the US, the other one.

- The other things, two things. One, we can look at this even if it isn't constitutionally required as a serious privacy intrusion that requires protection. So as a privacy policy matter, we may want to think about these are intrusions on Americans' privacy that should be protected. And even if you don't call it a constitutional requirement, it is something that can require protection as a policy matter. One other thing I do wanna say is I do think, just stepping back to the conversation by reverse targeting, et cetera. I don't mean to suggest in any way that there are violations of reverse targeting. I am not aware of that. This is a totally different situation that we're talking about. We're not talking about inappropriate targeting here or even necessarily inappropriate or even inappropriate collection. This is what can the government do with the communications once it has acquired them. And so I wanted distinguish with the collection stage from the querying stage. I think the vast majority of what we're talking about here pertains to the querying stage where we are talking about the particular rights of the people. is something that I didn't intend to.

- No, no, no, it it's unlike all the other examples that Brad gave. Those situations where someone brings you something, you gotten that Title III order. Section 702 is a situation where the only way the government can get this lawfully in the first instance is by certifying that they're targeting only foreigners overseas. Now, I understand that the word target as a technical legal matter doesn't apply to a US person query. I think if you're a United States person and the government has a criminal piece against you, has searched Section 702 data for your communications, balance your communications and use them against you in court, you would probably be pretty baffled to learn that you are the target, right? So that term has some technical legal significance. In terms of the impact on America's privacy, not so much. And also again, as I was saying earlier, there are plenty of constitutional scholars who are saying that a US person query is a separate Fourth Amendment event. You have a seizure at the front end and then you have a search. It's different from .

- Chris.

- I just make some big three quick points, which throw off some of the prior comments. I think, one, it bothers me a little bit as sort of lawyer in the intelligence community when this is framed as the government's doing something wrong or engaging more on the surveillance, you're doing backwards searches. As Brad pointed out, this is a program that a federal court has approved every year since it was authorized, that congress has reauthorized three times. I mean, I think that reasonable people can disagree about whether or not you can be allowed as the US person for in certain circumstances. But, you know, the intelligence community tries to obey the law as best we can. And I think that in this case, the courts in Congress have decided this is a program that we can use. Doesn't mean should always use the both senator legal authorities, but this is program that has repeatedly been reviewed by the courts and our elected representatives. And it feels like framing this as the intelligence community misbehaving is something that is not appropriate. Now, compliance issues and , I'm sure Mike will talk about the steps the FBI has taken to address what you've mentioned earlier on the compliance side. But actually engaging in this program framing as the intelligence community and something wrong feels inappropriate to me. Which leads to the second point. Second point is that reasonable people can't disagree about this is I think that it's clear on the stage that there's reasonable people on the stage that disagree about this. And as Sharon said, just because something isn't debated legally doesn't mean we can have a debate about what the policy consequences are of doing something. And there are obviously legitimate privacy and civilities considerations when we engage in US persons search and queries. At the same time, you know, there's a number of blue-ribbon commissions, the 9/11 Commission and other commissions after it that have complete continually emphasized the intelligence community US government that you have to connect the dots. You shouldn't silo law enforcement and intelligence activities and you have to be able to connect between the two. And by requiring a warrant requirement, by putting this a warrant requirement, as Brad said, you'll effectively be doing that in this context. So I think that that doesn't mean that that's necessarily the right answer doesn't necessarily mean, it just mean this is a policy choice, it's a difficult one. Which leads to the third point. Not all US person queries are the same. I think the Congress recognized that when they said they put in place certain requirements for, you know, US person queries that have a criminal element to them, you know, queries that would be looking for evidence of just a ordinary crime are very different than queries that are

undertaken to prevent serious national security threat that's impending the FBI's information may be happening. There're different than queries that the FBI does to identify victims of national security threats and try to help them out. So I think that if we move beyond a legalistic discussion of whether the Fourth Amendment allows us or the Fourth Amendment doesn't and get down to what are the policy costs and benefits, the different types of queries, that might be a much more productive conversation to have, because we think that there are obviously privacy consideration be relevant, but there are also very serious of why we wanna do these as the government being bold outside entities.

- So I'd like to push back on that just a little bit, it's not as though 702 has always operated well, right? So in 2011, Judge Bates issued an opinion where he found that the government actually started collecting under the FAA under 702 before the court had actually approved and before any of the certifications had gone into place. He also discovered that they were collecting all abouts limitation or all abouts communications, not just the ones the court said they could. And in addition, they were collecting multi communication transactions, which included domestic conversations, including entirely domestic conversations. In fact, so much so that the government admitted that they knew they were knowingly collecting tens of thousands of domestic communications. and it didn't stop there, right? So in October of 2011, Bates put into place certain procedures and the court then found out in 2016 that there was a lack of candor and in fact they were violating the prohibitions or about collection that the court had placed. They noted it was a very serious Fourth Amendment issue and together with noncompliance. For seven years, 702 collection had been violating Americans' Fourth Amendment rights, right? So this isn't entirely accurate that this program is operating completely appropriately. When we look at the Fisk opinion from 2018, 2019 and 2020, you see all the non-compliance issues, which Liza mentioned earlier of how do you come to the conclusion that this is all being done appropriately?

- I don't think that was an entirely fair characterization of what I said. I think what I said is that courts in Congress have determined this program is consistent with the Fourth Amendment. It doesn't mean that the intelligence community, the government doesn't make mistakes in executing the program. You've recounted a number of mistakes in the past. I think that's, in some ways, I'm not gonna say that mistakes are a sign of a healthy program, but I think the fact that the government is willing to acknowledge the mistakes it makes, or to identify the mistakes it makes. I mean, if a compliance program doesn't identify mistakes, it's not much of a compliance program. The compliance program, the whole point point of it is to identify when you do things wrong, so you can correct it. I think the thing the, you know, all the issues you've identified, we wish they couldn't have happened, they shouldn't have happened. We don't want 'em to happen. But the fact that they did happen, they were identified by either the government or the FISA Court and then we then subsequently correct them, I think is very important. I mean, I think that Liza talked a lot about some recent FBI compliance problems. I think Mike can give you chapter in verse, and this is probably the most recent and the most important, the current debate, how we've addressed the most recent compliance problems. I think they provide a pretty good example of compliance problems that we wish wouldn't have happened, they shouldn't happen. They did happen. And we learned from them and put in place additional protocols to try to address those problems. I mean, I can't say that we're happy those problems happen, but I think I can say that this is a

sign of us being willing to learn from our mistakes and try to make the program best it can be. A program that overall in Congress that continuance said is a lawful one.

- Great, before I go to Mike, I saw Brad grab the mic.

- Yeah, yeah. Just the few points on the , from the Justice Department perspective, not acceptable, you know, no excuses for the problem and it has been, FISA have had compliance problems over the years. But I think it's also important. Second point is, you know, as Fred said, you know, DOJ and IVs and others are responsible for identifying these compliance problems. So I agree with Chris that it's designed that the system's working, that we're examining this and overseeing it, identifying these problems, reporting them to the court and then fixing them. And anytime we have a large technical system that has a large volume operation, in my experience and all of you have experience with computers, you're going to have these types of issues when you talk about computerized information. I'll give you just one example and I'll turn to Mike to talk about some of the . But, so one of the reasons FBI recently failed to comply with some of the query standards is because the searches are federated. What I mean by federated, if a bunch of different, is my layman's understanding, correct me if I'm wrong. You're searching through a bunch of different databases. An FBI agent is going in and saying, I need to find out about something going on in my district that I think is a threat or whatever, and I can work it out with you with any standard, maybe with no standard. And I put in a search term to search for that. They may have been, and the evidence shows in many cases, they were unaware that search was gonna include a database that included vital information, 702 information. So there's talking a bunch of things and they didn't even know at the time that it was gonna be 702 that they had to meet the reasonably likely to obtain foreign intelligence information. They should have known that but it's not an FBI agent going outside to Americans. It's having a computer system that is not well designed. So what we've done, and Mike can talk about this greater instance, is make it so it's automatic so that in the computer system, automatically before you touch that 702 data, something's gonna pop up on the screen that says 702. Do you have a justification here? And what is it? And right, you know, put that in or whatever. And maybe it's so automatic. We have these same problems. By the way, for those of you who are national security meetings in the audience with national security lenders years ago. It was a huge issue. It was an FBI investigation with national security lenders. They were different steps authorize national security letters. Sometimes agents were using the wrong statute or the wrong authority or the wrong standard. And it was a big compliance problem at a time. So we developed something called the NSL subsystem, technically, which makes it, it is kind of , right? So it's automatic. You have to identify the right statute. Does it fit under this type of investigation? It kind of boxes to check that has largely eliminate a lot of those compliance problems with the NSLs. And so look, we ask a lot of our FBI agents, and look, I don't wanna make any excuses for the errors, but they're doing their best to try to protect people and we're trying to put things in place to correct these errors when they come up. And I'll turn that to Chris to talk about the things that we are doing to address recent concerns.

- Okay, great. Thank you, Brad. So yeah, I just wanna, you know, reiterate that, you know, we agree that the compliance incidents, and probably said this, you know, that were identified in this series of

compliance reports were unacceptable. And we're a scale's not unacceptable to Chris's point. Like any compliance regime is going to surface some non-compliance. But the amounts on the scale that we were seeing was unacceptable. And that's led us to take action for sure, but also led our external oversight just looking at this to identify, to surface these and to provide that for us to act as well. So one thing that you, you know, that people should keep in mind is that all of these reports have been made public to date predate the reforms I'm about to talk about that we implemented in 2022. So we do have some indications about our compliance post those reforms, but that has not been released in a redacted publicly release form to this date. So we do you ask that when we're discussing reforms that are necessary as part of reauthorization, we've taken into account the current state of the compliance or and not the past state, which is, you know, and most of what we've seen so far. We look forward to hopefully soon sharing some of the results of the compliance improvements that we're seeing. So, well, before that, I do wanna know that once we identified this as a problem, we identified the best way to go about addressing it is to look at exactly what the problems you're seeing and identify the root causes behind this. So we identified kind of four major areas that were causing the majority of these problems. And that's where we took action. So one of those changes is the one Brad handled which is we changed our better aid systems where you now have to actively opt in to query against FISA data, if you have access to that data. Not all of our employees do. You have to actually have a mission need, request it from your supervisor, have it documented, complete a series of mandatory trainings, and now as part of one the other reforms, on an annual basis, complete additional mandatory training to regain access, otherwise you'll be removed from access.

- Just on that point, just to be clear. So for 13 years, from 2008 until 2021, it was automatically returned, and so queries were automatically run against 702?

- I wouldn't say automatically run. So it was automatically selected in our valere system. So when you're going into the system, its are just a variety of different databases, which again was part of the recommendations from some of the commissions that looked into like 9/11 before Hill Commission where we weren't searching all the databases that we needed to surface information to appropriately address threats. So we engineered a database that allow us to search across multiple databases at the same time to mitigate the operational risk with not searching raw FISA when we needed to we were opted in, you know, so when you go in there, it checks all the boxes including the raw FISA. So we changed that in 2021 so that the boxes contain raw FISA if you have access to them in the first place, are unchecked. So that if you are just running a regular check, it's like, hey, here's a contractor coming in to do work in our field office. We wanna make sure that he doesn't have a criminal record or connections to the national security threat before we let him into our office to install your hardware. Then that's not going to run as raw FISA unless you specifically choose the against raw FISA and say yes, I meet this FISA query standard to run against FISA. One of the things that's mitigating the operational risk, which we're still very cognizant of cause of our responsibility to use this data that we have to best protect United States, is if you have access to raw FISA and you didn't check that, it's actually gonna remind you and say, are you sure you don't wanna include raw FISA? But then you move on from there if you're done. But it let you to back out and, you know, proactively check that. If you say that, yes, I do wanna raw FISA. It won't let you proceed from that point. I'm getting . But, so this is one of the big contributors to

this problem and our query numbers, which, you know, I wanna emphasize this was not the point of our reform, not . It was lower. It was to make sure we are querying compliantly. But a lot, well, I would say the suite of performance that we implemented had a substantial change in our practice around querying. So that's what we're seeing in this problem. We're we're seeing that doing it differently and that's one of the things that's contributed to the large problem.

- Yeah, great, and you also mentioned the training, right? So initially they had to be trained by January of '22 and now it's annually the FBI is requiring training in your documents. Can you comment, one of the things that really interested me, so two days ago, right, the FBI opened up all these documents, they're now online, you can find them, and they will be in the Foreign Intelligence database as well after May. One of the really interesting points was now you have to consult an attorney. So it seems like there's a growing industry for our students to actually... Talk a little bit about this, you know, the babysitter requirement, right? Like, now before anybody does this, they have to consult an attorney. And if it's a sensitive political circumstance, one can think presidential elections, maybe. It has to go to the deputy director. Can you talk a little bit about that?

- Right. Absolutely. So those actually hit on two of those four root causes that I haven't discussed yet. The first one is that additional training and clarification. So what we released on Monday was the query guidance that we worked with DOJ to clarify some misunderstandings in terms of what the actual standard was on the part of a lot of our employees. So this was the defendant of guidance that we should in November of '21 be clarified. Especially one of the big points there is the justification problem. During inquiry, there are three parts of the greater standard. One, if you have to have an authorize purpose to return foreign intelligence information or crime, which the FBI is the only agency that has that evidence of crime purpose, which I can talk about all day because that's important. The second one has to be reasonably designed to not return more information than you need to answer the investigative or analytic question that you are opposing per this database. And then the third one is the justification where you must say a specific factual basis. You actually have to have facts that you can articulate that your query is reasonably likely to return foreign intelligence information or evidence of a crime from raw FISA data specifically. So, so this is one of the things that really limits our use for evidence requirement of a crime only purposes, any criminal cases that are unrelated to national security. 'Cause this database is collected non-US persons overseas related to foreign intelligence, it's very difficult in a purely criminal case that has no connection to a violation of national security that you have a specific factual basis information in this database that's a foreign intelligence database. So if you look at last year's report, I believe the evidence of crime numbers that we reported were, I think it was 12 compared to 3.4 million US person queries. So it's actually a relatively small use case for the FBI, there. I do wanna kinda jump over to the-

- Sorry, before you do that, because those 12 cases which required you to get an order from a court, but there were zero orders sought from the court, can you address what's changed that the FBI is gonna follow the law, follow the statutory provisions?

- Right. Yes, absolutely. So I do wanna clarify there that those 12 did not all implicate F2. So we actually reported that, you know, in encounter one we got zero F2 warrants, which in fact we had knocked on the F2 order 'cause it's such a narrow circumstance.

- Sorry. But there are over a hundred times, right, that have qualified. So even though it's narrow over a hundred times the law requires that . So what has changed that that's gonna change ?

- Right. So in 2020, and now in 2021, that was actually four instances. So when we're talking about a hundred that reaches back a few years before one of the other reforms that we implemented, which changed our database system. So a lot of those almost a hundred violations were cases where, someone had conducted a query for evidential requirement only in our federated database would've required an F2 order to view the content, but did not actively choose to view the content. Instead they were presented a preview of that content because of the way our database system was was configured. So what we saw was that people were reviewing content without actually taking that next step to say, yes, I want to do the content and therefore I'm going to go seek an F2 order.

- This is important just to, so you do the, you do the search and then, you do the search and then this isn't all them, but at least some number of them, you put the search in, then you have to go in to actually get the data. So instead of like it gives you a, oh, here's a popup box that says here's what's gonna be in the data you get. Okay, all right, now it's too late. You've already able to tell it, you're supposed to go get a court order before you looked at it and the system was configured so that you would get this preview like a little summary or something that pops up from the data or at least a header or something like that. And so, look, it's a violation. It's not good. I mean, I don't wanna keep apologizing for these, but I think it's important for the American people to understand the causes of these. the violations are bad. It's sound bad 'cause they are bad. I don't disagree with anything Liza said. It's not a pretty record that we have here, but it is important, as Mike said, to understand the reasons for them. Sometimes it's technical, sometimes it's training. There's a variety of different factors of each of them. We at DOJ discover these, we analyze these, we work on training, we work on fixing the problems. And so just understand the reasons, I think it's important.

- Liza, do you wanna comment on this? Then we'll go back to you then.

- Yeah, on the remedial measures, I think that would be a lot more convincing if the standard in question that the returned for an intelligence or evidence of a crime was anyone. But this is the standard that's been in place in the beginning, in fact, before that because it's also part of the minimization procedures for traditional FISA. So it's been around this whole time and throughout this period the Department of Justice has come to congress for authorization and said, you don't have to worry about America's

privacy is protected because we have in placed robust training and robust internal oversight that is more than sufficient to protect America's privacy. So given that history, I think allowing would be remiss if they can take these new assurances with a somewhat of a grain of salt. I would also say that the FBIs, these violations from the last few years are the latest in a long line of FISA court opinion stating after 2009, revealing violation of the systemic violations of the rules designed to protect American's privacy. In multiple instances, the FISA court held that these violations rendered the operation of the program unconstitutional. In each case, the defending agency says, okay, we'll have your procedures, we'll have your training, et cetera, et cetera. And then the very next year there's another FISA court opinion with 40 some pages of violations, maybe new violations, maybe some of the old ones. As Julian Sanchez, who I think is gonna be in the next panel, has said the government has been engaged in a game of compliance whack-a-mole for the last 15 years. And so that context is important, but encourage people to actually go back and read some of these FISA court opinions where you see the courts sort of building frustration with this pattern. I just think that's something to keep in mind. Know, of course this isn't something about bad people are doing, it's not . But that doesn't mean it's also like, I'm okay, you're okay. These are minor policy disagreements. I think it's important, it's important to get this right. Yes, Congress has approved it in the past, but Congress has another shot this year. And sometimes these are compliance issues where the rules aren't being followed, but often the rules themselves are problematic, very problematic, I think constitutionally so, different judges are starting to disagree about that, but we need to have that conversation. I like and respect everyone on this panel. I just met Mike but he seems great.

- You seem great as well.

- This isn't personal. It's very serious. It is serious, and we have real disagreements.

- Great, thank you so much. I'd love to move on to the next talk. Do you wanna finish up on the compliance? Anything you wanna get in before we pause?

- So the last part that you alluded to, I just wanted hit real quick, which is we did identify certain areas where additional, you know, scrutiny and approval and, you know, additional lawyers in the process were warranted in two of those were when we were conducting large queries, which we defined as, you know, a batch job that results in over a hundred queries where we need to get attorney preapproval to make sure that we're meeting that standard, and an attorney has said, yes, we're meeting that standard, but of course a failure to meet the standard would affect many more, you know, people potentially than if we were querying an individual firm. And the other one is those sensitives queries where in some categories required attorney's preapproval. And yes, for domestic political officials and candidates in and higher sensitivity levels, that requires the deputy director of the FBI to sign up on those before they can be run. And you know, one deputy director of the FBI, so obviously this is a... And he's a very busy man, so this is obviously a pretty high bar for those particular circumstances. So that's the fourth of the categories that I wanted to get into. You know, one is the training, two, and one thing I would note for

that is like we're talking about those four F2 violations and you got going on. That was before that additional guidance and the updated training went into effect going on as well. So we expect that to mitigate that behavior moving forward as well. So training and guidance, the updated requirements, the re-engineering of the additional database systems and then the additional things. And moving forward we had one additional kind of reform. We office internal audit. We already got robust external oversight over us that's watching us, but we identified the need to do our own internal oversight and beef that up. So we stood up a whole new office to look at our use of national security authorities, identify internally where we need to influence more controls and get better to prevent these errors before they happen and do that on an ongoing basis instead of just relying on this one time 2021/'22 performance, so.

- Okay. Actually Sharon, I just wanna give you one last bite of the apple because all these issues to address non-comp compliance, right? So now we have an opt-in as opposed to an opt-out system. We have attorneys being part of the process, we've got this internal audit, you know, all these things. Are these sufficient too as far as you're concerned? I know they're not sufficient for Liza. Are they, yeah.

- So thank you. I wanna say that those are welcome and should be encouraged and I do think we need more. I do wanna build a little bit though on something that Liza just said, which is, and from our review, we're not seeing, you know, government agents going out there with improper purpose, you know, and willy-nilly trying to violate the law. And I don't mean to suggest by saying that I think the safeguards are insufficient, that is what's going on. I also wanna say that from my view, and I know, not speaking for the board members, but have a little bit, you know, a few things that we're already seeing, you know, this program is valuable and it has privacy risks, and Congress can and should address those privacy risks without undermining the core value of the program. So I know there are some folks out there, some in Congress who are probably calling for a full repeal, et cetera, et cetera. Sorry about notes, I'll give them a minute. That is not what I think where this debate should be happening. And the debate that we're having up here I think is much more focused on the key privacy risks that Congress can and should address. And so I do wanna make that point quickly.

- Great, thank you. So we've been able to touch on abouts collection, we've talked about incidental collection back doors, the querying, the non-compliance. There are yet more elephants in the room, another one is the witness regime and back in the last, in March 15th in fact of 2020 when the three temporary provisions expired in FISA, this is the aerobic wire tap, Section 15 of the provisions. They were largely derailed, I think, over the amici procedures that were being proposed in Lee-Leahy amendment in the Senate. So that House had passed a bill in order to continue the three expiring provisions. The Senate then did not pass a bill and the three provisions of FISA actually expired. So I'd like to turn to Wyndee to talk a little bit about the Lee-Leahy amendment and what's happening with the amicus process and kind of how to think about the amici in the context of some of these concerns because that's one of the ways in which Congress has sought to try to shore up some of the concerns that have popped up.

- Over the years the FISA Court, sorry, I'm sorry. Over the years, the FISA Court very early on, they had they, I think that they felt that their hands were a little bit tied when it came to the Leahy, so that we wanted to make clear that Leahy were encouraged. And so there were been different things done and authorizing in 2018 bill, the payment for the people who provide that sort of assistance for a novel and some significant interpretations of the law and also technical amici. So Lee-Leahy amendment with really, really focused on the amicis and they wanted to go beyond the novelist significant issues, which was the same at the time. And they went to really encourage the appointment by the FISA Court. Again given the FISA court some discretion, but really encouraging it in instances where there were significant concerns related to activities protected by the First Amendment where there was a sensitive investigative matter and that included the investigation of a domestic or American public official or political candidate, religious or political organization or the news media, also matters that involve a request for approval of program technology or use of the technology, and also the authorization of programmatic surveillance such as 702 and those issues that otherwise related to not of significant civil liberties and concerns as well. And so of course the 77 to 19 was a vote on that. So strong support in the Senate. And the Senate sent back the House bill with that amendment and the House was going to take up the FISA bill as amended, but we were stopped by then president.

- Would you like to talk about that? It's not that .

- So that we can amendment. But President Trump told the House not to pass the bill, House Republicans in particular. And so all the support that had been gunnered for the bill, and the station in 2018 was brought to a screeching halt.

- And I suspect, Brad, you might have an explanation as to why that was the case. Can you discuss your philosophical differences with the Lee-Leahy?

- I can talk about that. I'm not commenting on what the president may or may not have decided back then. It's a different thing. But in terms of the amicus provision, look, we think the existing amicus provision has worked pretty well. I mean, the Amicus is a friend of the court, so ultimately it's someone who works for the court to provide assistance that the court makes as necessary threat to make decisions. And the current amicus provision allows the court to appoint an amicus essentially whenever they want. And then if it's a novel and significant issue, there's a nudge from the Congress to say, please do it in these cases unless you really think it's inappropriate. And the big amendment someone mentioned earlier, the thing that's helped it is having a pre-cleared security clearance covered group of, I think it's five individuals with expertise in this area who have the clearances who are on call and then funding to pay for them to perform this function. And that's also good. It's been used multiple times, numerous times, including the detracted 72 applications. I think the court would say it's effective. The court by the way commented on this provision back in 2014 when it was first being considered, and said, look, we know what our business here at the court, we welcomed having an amicus provision, but the good cases in which we need the assistance of amicus are relatively smaller, is what the court said. And

why is this? Because the vast majority of FISA cases that are going into the other part of FISA so that not reauthorization, the vast number of applications are federal one, federal three applications, which are ordinary applications but probable cause standard against a set of facts. And they have legal advisors to help the court perform that function. And they're relatively straightforward. It's the same type of analysis they do with every search warrant, every Title III wiretap applications in those contexts. Those are also ex-party. There's no need for amicus. The amicus by the way, doesn't meet with the target obviously for obviously operational reasons. So they're not gonna be able to explore any additional facts or provide any additional value add. They're just gonna be making legal arguments, which the court can already do in assessing this and which they're used to doing. And so they really just not need it for the majority of cases. And so the government's concerns with the Lee-Leahy were few. One is that would that it was written in a fairly broad way because significantly span the number of cases in which the court would be required to appoint Amicus, even in cases where the court did not need any assistance. So that would really slow things down with the court and clog it up because our experience has been, while the amicus has invaluable, it doesn't slow things down significantly in cases that are operationally time sensitive. And when the ordinary period is you have seven days between the filing of the application and when the court is required to rule. And that's a quick talk and this for obvious reasons when you talking about actual security, we need to get that information right away, get up on that target and you gotta wait once a month, we see what happens with meeting have an amicus. And in our experience, you have briefing, you have been up case, have be appointed, you know, it's a back and forth and briefing schedule, and just takes labor intensive and way more time. You can do that in some cases, but not in many of them. And that's one of the things the court recognized. The other big concern with was he kind of provided a free, a provision to which they would have access automatically to any information they wanted basically in the government's files. So this is both a constitutional problem 'cause the executive controlled classified information, he controls what information can go. I don't think the AMT had any concerns about the information they have necessary. The court basically has the reins in terms of they think they need see particular information to assist the court in making arguments to the court. They can do that. But allowing the amicus to just ask for whatever to have a right to get whatever pacified information they want raises operational concerns and could prevent us in some cases, even from getting information from let's say foreign governments so I'm willing to share the information that they know that . So those are some examples of the type of concerns that we had with the bill.

- Okay, so just so we're clear actually at ethics time you mentioned Title I, Title III. So the tweet that came out had a lot to do with the role that FISA had played in the 2016 presidential election. So we had Horowitz Michael, the inspector at the DOJ came out with a study that found that for hurricane, that there had been many kind of problems for the applications of the court for the four individuals that he focused on in his first report, that there were issues of where information had been emitted from the files. In one case there was an email that had been doctored by somebody at the FBI in order to hide information from the court itself, for which was sufficiently concerned after the issued that report in December that he came out with a second report in March, which timed actually was coincidence with the consideration of the three expiring provisions. This time he pulled the applications for 29 US persons and found between five and 65 errors per application to the Foreign Intelligence Surveillance Court for Title I. In those cases, some of that information went to the probable cause determination. He was

sufficiently concerned that he then conducted a third inquiry, which reported then in August of 2020, where he found approximately 400 errors in all of those applications. So that whole debate about Title I and Title III kind of overtook the consideration of the expiring bridges much the same way right now we see a lot of concerns that still center on the 2016 presidential elections and way in which FISA was used, kind of overshadowing this debate here as well. So I'd like to turn to Liza to comment both on the Horowitz kind of line of concerns while separable from this, the way in which it's playing into 702 renewal and secondly on the amicus provisions, whether you agree with Brad that they're sufficient, whether you think Lee-Leahy was good, whether it didn't go far enough, whether the House were, where are you on the amicus?

- Okay, so on the Lee-Leahy depending on I guess what Congress you're in, you know, this is basically good government. I mean anything that passes defendant on the vote of 77 to 19, you have to work to find problems with it. So what it did essentially was it expanded the number of cases in which supposed to participate. There is no case, not a single one motion court is required where they used to have . The court can always issue a written finding that some cases we find this is not appropriate and not use media, but it expanded the categories of cases in which it's presumptively appropriate to include sensitive investigative matters were defined as cases involving religious organizations, political candidate, and political officeholders and the media and maybe one or two others. So I mean, really, you absolutely would want the court to hear from another party. I mean, if foreign governments aren't going to give us information because five additional people within the executive branch who are pretty clear that the highest level of clearance are going to see this in , that's not a problem. That's a different problem. It also, you know, allowed Lee-Leahy access not to any materials they wanted, but to all the materials that are relevant to the case that the amicus was participating in. And it allowed amici to petition the FISA court to certify its own decision for appeal because otherwise if the FISA court rules in the government's favor, there's kind of no way to get some kind of appeal to the FISA court of review. So, you know, very basic government stuff. It also included some provisions addressing the Title I FISA accuracy problems and requiring the Department of Justice to implement accuracy procedures and to disclose to amici and to the FISA court, any exculpatory admins in their possession. Again, very basic good government kind kind of things. So yeah, I think that the Lee-Leahy should passed, it would've passed as part of USA Freedom Reauthorization if it weren't for that amici. And in terms of some of the Title I issues, I think what that shows to me is that this year reauthorization is very unlikely to be limited in Section 702. It's probably going to address some of the policy with Title I of FISA, and may very well go beyond hands well because it's important to understand that Section 702 is the one part of an ecosystem of often overlapping authorities that increasingly we are seeing sort of gas and loopholes in this network of authorities that are allowing for different kinds of warrantless collection of Americans' Fourth Amendment protected information. And if you just fix one of the loopholes and one of those authorities, then the surveillance can shift to another authority that might not have a sunset in it. So I think this really is not a question about technical fixes to Section 702. I think this is a broader question that Congress needs to have a reckoning over when we think it's appropriate for the government to be collecting and having access to Americans' most sensitive information and, you know, making sure that whenever that happens, it's happening pursuant to statutory and review with appropriate safeguards and the judicial oversight.

- Title I, Title III and executive order overview.

- That's not what I thought you were looking at before. I like to talk about the FISA before amicus.

- Sorry sorry.

- Talk about really quickly about amicus. So I can't say whether we'll be addressing that in the board's upcoming report on Section 702. But I did wanna speak to this because back in 2014 in the PCOS report on the Section 215 program, it also looked at the operation of the FISA court and this predates the 2015 enactment of USA Freedom Act, which created the amicus role. And at that time, back in January, 2014, the unanimous recommendation of the privacy is then privacy in Civil Liberty's Oversight Board members was that Congress need to create what the board then called a special advocate role. And that role was very similar to what ultimately became the amicus role, but it was actually stronger in the board's recommendation than what ultimately was enacted in the law in all three of the ways that would has been talking about. It urged that the role be broader than the novel and significant legal issues or role, including things like the requirement for the annual certification, the 702. It also spoke to the access information requirement. And I think that personally is a critically important outcome of what would've been enacted to ensure that the amici can access to the full record at issue in that case to the same extent as the government attorneys do. Has there been any aspect of that information? But the panel of certified amici are people who all have court level security clearances and so to have access to the full record that's at issue in the case in which they're appointed. And then the third as I mentioned, is to enable them to be able to petition for appeal. It would have to be discretionary, as Brad noted, they are not representing a party, so it couldn't constitutionally be a mandatory appeal but to petition for a discretionary outright of appeal and all those three ways were what the board recommended. It was stronger than what ultimately was enacted amici. And I think should be that... I hope that Congress will take the opportunity of this sunset to expand and strengthen the role in those ways. Wyndee, do you wanna comment on this? You're good.

- when I said, point Liza made about whether this is mandatory. Right again, right now the court can appoint amicus whenever they want. So be clear, they can do it whenever they want. And this is all for assistance arguments in the court. So right now they have the ability to appoint amicus whenever they want. The supervision would say you must appoint an amicus unless you find it is inappropriate. So that's a standard, that's a legal standard. The court is gonna have to make a finding that it is not appropriate. And so the question is what does that mean? When is it inappropriate, right, to appoint an amicus? Maybe they would find it in a particular fat pattern, not appropriate because of the urgent speed need, but it could be difficult for courts to make those findings. And if they did in have to spend a lot of time making those and justifying those, you know, broad swath of cases. So if it's not a case, if it is not, what is the reason for it? In other words, if they have ultimate full discretion turning down, why do we need to do provisions? They can already, in any case, novel cases that Liza mentioned, if the court

feels there's anything novel or unusual or any reason they wanna appoint an amicus in any sensitive cases, they can do that today. I just wanted to be clear, they can do that today and they're doing it.

- Liza, a quick response?

- I mean, the FISA has in the past on occasion found that it's not appropriate and they said it's 'cause we don't need it in this case. So it's not that hard for them to do it. I think what it does is it creates a little nudge, a little bit of a presumption, but I think that's helpful because the FISA court might actually need some help and not know it. You don't know, you don't know, right? I mean, they don't know what the arguments are that are going to be raised. And you know, not a lot of people wanna hear that they should be getting help. That's human nature, right? So I think it's a very good thing for Congress to get just a little nudge. They can always say, no thank. Okay, we're gonna embark on our third and final general topic before opening it to questions from everybody who's gathered here. And the third kind of big trache as it were, is the international dimensions to all of this? So if we think about Max Schrems, our buddy, the law student from Austria, who has brought a series of cases against the United States because of both 702 and 12333. And I think no better person to go to with the question and the update really as well as where you think things are gonna head? Are we going into Schrems 3? Is this new board gonna be... Can you talk about the executive order? And give us a quick history, what bough us to this point.

- Sure, I'm happy to talk about this. So I think Brad mentioned the international mention debate earlier. And just before getting into trends, I think the thing that when I think about international mention this, the thing that strikes most with the fact that this panels happening at all. I mean we have the Justice Department, civil society, intelligence, community, academia or legislature and independent privacy and oversight body, all here talking in authority. I don't think this type of thing happens in most countries and I think that's really important for two very, very important reasons. The first is drawing from from Laura's question. So I think that making sure we get the rules right in this area is integral to unlocking cooperation with our partners and allies. You know, she mentioned the trans decision. Many people in the audience see Alex are probably very, very familiar with the trans decision. But basically for those who aren't, to transfer data from Europe to United States, you need a lawful basis to do so. One lawful basis is that the European Commission has deemed the country that will be received as having adequate protections under that country's laws or the data that will be transferred. In 2016, oh, I'm sorry, earlier than that, the United States negotiated agreement, all the privacy shield, which was a set of commitments we made about protections that would be in place under our laws and some executive branch commitments that Europe Commission team is being adequate and providing adequate protection. In a case called Trans-sue, Which, you're right, indicates there was a premise law , which made a similar decision about an earlier arrangement. The European Court and European Union basically said, no, the US, protection they provide for data are not adequate. They aren't essentially equivalent to what you would get under European law. We obviously disagreed with that decision, but it doesn't stop us from our state department, the commerce department, our National Security Council embarking on a negotiation with the European Union to put in place a second arrangement, which was

concluded last year called the Data Privacy Framework, and US Data Privacy Framework whereby we made a set, an advanced set on our laws to arrive at solution that both US Commission thought provided essentially public protection was provided under European law. The centerpiece of that framework is from the US side is Executive Order 1486, which basically replaced the substantial portion of PBD28 and did a number of things. I think three probably worth mentioning here. One is for the first time it laid out the set of legitimate objectives pursuant to what the United States would engage in signals and intelligence activities. Everyone in the audience and everyone in the country can go look at the reasons why we engage in signals and intelligence activities and look through and see what your government's doing in your name and about why we're conducting intelligence. The second thing is building on PBD28, we put in place set of enhanced protections for how we conduct cavil's intelligence, how we minimize information, how long we retain it, what procedures we have in place and have to abide by in doing that. And the third, we created an novel redress mechanism that allowed individuals whose data is being transferred pursuant to in this the Data Privacy Framework or the analogous framework, to come to and ask if anything inappropriate being done with my data. So I feel the European Commission felt like this was a sufficient set of commitments to testify, proceeding down the process to make another determination which will allow David to flow freely under this legal justification again. That process is ongoing, and I think that it is a commitment to it. It shows the commit the US has to engaging intelligence activities with division privacy safeguards. Which leads to, I think the second and maybe even more important reason why I think this sort of thing is so important. You know, this is something that DNI have spoken about quite a bit, is how information technologies and intelligence, they sometimes unlock used as tools of oppression by authoritarian governance. And I think that's why it's so crucial that governments like the United States and our partisan and allies who share our values in Europe, put in place procedures and protections that show that you can engage in intelligence, you can engage in a further world of intelligence, like Brad talked about earlier, in a way that still is protective of privacy and civilities. And I think that, you know, 702, you know, we've talked about, you know, maybe there's some changes that Congress will I'm sure debate for the next year on the margins, but 702 is a program as a whole is I think part of a edifice, an apparatus in the United States engages in activities that shows you can do intelligence while also furthering privacy. And I think that's a really important example for us to say in the world where a lot of countries are increasingly doing differently.

- So picking up on Liza's final comments from before, there are two interesting aspects to Shrems and the October 7th executive order that I think need to be brought to the surface, and I'd like to hear your response on them first, is we now have an Article II adjudicatory body for anybody living in one of our besties, you know, in country within we best friends, anybody who's over there including a US citizen. Like if you go to Dublin and you think that Facebook is gonna transfer your data back to the United States and because of concerns over 12333, Executive Order 12333 as well as 702, now anybody outside the United States can go to an adjudicatory board. So, you know, the first question here is what about US citizens within the United States? You know, is this a different standard than others outside the United States are getting? There is no adjudicatory board for any US person who's concerned about 702 within the United States. Second, you're seeing confluence here with 12333 and 702. So is there willingness on the part of the IC to see other provisions in 12333 like provisions now that apply equally to 702 and 12333 second collection? Are there other ways in which 12333 could be brought into the FISA framework?

- To me? To me.

- To you.

- Okay, thought that you're asking Liza. So taking the those in turn, I mean, I think the executive order was in, as you said, it is agnostic, the citizenship of the people who be benefiting from the redress mechanism with anyone data being transferred from Europe to the United States. I think that it was crafted to address a specific geopolitical issue, which was the Shrems decision and putting in place protections that would allow the European Commission to proceed toward max determination. And it's meant to address that problem. I don't think it necessarily addresses other issues. I think there are US persons for reasons that Brad I can speak to. And I think anyone receive a lot more protections than European systems do. And I think we were passing the executive orders and active redresses specific set of problems. In terms of 12333, you know, so this goes back to the very beginning of the panel we've had here today. The executive branch has always conducted intelligence outside the United States targeting non-US persons under the president's constitutional authority is an authority, you know, without sunset. So, I think, you know, it is, so I think that this is something that the executive branch is always regulated itself. There's 12333, there's 1486, there's a set of AG guidelines for how we conduct intelligence under those activities. This is not an area where there's no regulation. There's been extent that executive branch regulation, which I think would stack up against regulatory regimes of any country. I put it up against the very best versions of any peer intelligence community in the world in terms of how you regulate this type of activity taking place overseas against non-citizens. You know, it would be a a pretty enormous step to bring that sort of intelligence activity that's always been under the domain of the president within a framework that's regulated by Congress. This is an issue that's kinda always been within the president's constitutional authority. And I don't think that that's something that really, it would be just a really a very big step, and I think we're focused now on 702 and what are the issues people have with 702 and how can we address them rather than making this dramatic change in the architecture of our national security horizons regulated.

- Thanks very much. Chris and Sharon.

- Thank you. So big one thought that I threw out on our prep call, which I think why Laura is turning to me, is ways in which these may be linked, as I think Chris may be clear and Laura made clear, of course this new executive order doesn't apply to singles intelligence conducted under Section 702 and the administration of course has made their representation. We're there, right? We're good. But one thought is with an executive order, of course it's not something that we would assume the FISA court would consider itself to have authority to enforce. So there may be ways in which Congress wants to think about are there pieces of this that can and should be codified as part of this reconsideration? And just, I'm not necessarily endorsing this, but it's throwing the pearls of potential idea for consideration,

which is, you know, the 12th legitimate objectives, I think is the phrase, for which civil intelligence can be conducted. If in some future date the administration wanted to propose a purpose for Section 702 collection that was outside those 12 purposes, the FISA court might say we can't do anything about that. We can't enforce that because it is not in statute. And so that is one potential thing to think about, whether if that were codified then in the circumstance where the government worked and say we want to conduct surveillance for purpose outside that scope, then FISA court could enforce it.

- Okay, Brad, you've been deep in the Schrems. I'd like to hear from you about these 12 legitimate objectives that Sharon's mentioning. I mean, these seem to meet the proportionality requirements, if not the redressibility ones, right? Because the redressibility is what the panel is set up for. Do you think that the executive order, that there will be further litigation, that it will be sufficient for the European court, the new regime that's put in place? Where do you think there is gonna be debate and discussion if anywhere on there? And what do you think about this kind of proposal where you actually codify the same protections that were extended to European Union ?

- So I think we feel pretty good about the protections, the additional protections that we provided. The commission certainly does. And so they've issued a draft accuracy finding. We expect that will be finalized sometime later this year. But we also recognize and fully expect that it will be challenged again. And so we'll see Howard Ferris in the European court, is fine. , we done a good job. We think, as Chris said, I think the system that we have, particularly with the new protections, compares favorably to any protections in Europe or really anywhere in the world, honestly, in terms of the level of protection that we have and the level of transparency, as Chris said, that we have as compared to any country in the world that doesn't. So whether your justice will agree, I'm not sure. In terms of codifying it, it could mean one of the ways the system can work is because it was done by executive order as a constitutional matter. So I think it would raise some tricky constitutional issues. Maybe not was limited to 702 collection, something obviously Congress has regulated already and so independent of this mechanism, if they wanted to look at the executive order and impose new constraints on what the purposes are, we're honestly all within those purposes anyway. And if you look at them there, there's a number of different national security interests and so honestly we're well within those. So, but if Congress wanted to to do that, certainly something that you look at.

- I said in the future, I didn't mean to suggest, yeah.

- Liza, do you wanna weigh in?

- We've covered 12333 Part. That's part Chris said, you know, our 250-year history, we haven't had Congress set into that, but on a collection within the United States that's occurring, that's something Congress consider we take whatever is .

- So in the 250-year history, we actually didn't even have a award required to collect America's phone calls in the United States until 1967. So basically we're talking about a few decades in which the Fourth Amendment understood . And the 1978, when Congress passed FISA, it created a certain geographic limitation on FISA's reach. So to oversimplify, necessarily, FISA applies when the government collects information from you, USA companies or inside the US. When the government collects information oversees, it usually operates pursuant to claims of inherent executive authority as regulated by EO 12333 and various other executive branch policies. This distinction is extremely significant because there are seemly few legislative limits that apply to EO 12333 caution and absolutely no judicial review. The protections that are in place in these executive policies are less robust than the ones that are in place under, even if they're more robust than other countries. So this geographic limitation might have made some sense in 1978 when surveillance inside the US usually meant surveillance of Americans, surveillance overseas generally meant surveillance of foreigners. But as we know today, communications are rooted and stored around the world in locations far removed from the point of origin or receipt. And in fact, the fact that foreigners communications were being stored inside the United States and the European government was being required to get a probable cause order to ask system was one of the main reasons why the government sought to modernize FISA in 2008, to the Section 702. But the government paid a lot less attention to the flip side of this problem, which is that Americans, purely domestic communications and Fourth Amendment protected information like the old location information is routinely rooted and stored overseas in ways that in some cases you can keep them outside of FISA's protections and expose them to EO 12333 surveillance. Now, Congress did extend FISA to cover intentional targeting of Americans who are themselves overseas and EO 12333 policies generally prohibit targeting Americans or intentionally collecting fully domestic communications. But there are evidence and exceptions to both of those, and perhaps more to the point, they have very little practical effects, those limitations, when the government engages in bulk collection without hurting anyone, which is allowed under EO 12333 but not under Section 702. And we learned last year that CIA's multiple bulk collection programs that are pulling in American data and the CIA's running backwards searches to access that data. Even when EO 12333 surveillance is targeted, not in bulk, it will pull in the communications of Americans who are in contact with targets, just like Section 702. There's no difference there. However, unlike Section 702, there are no court ordered minimization requirements, no court ordered US person query requirements, no judicial oversight to enter compliance with the rules that exist. There's really just no justification today given the technological way we communicate for giving Americans constitutional rights less protection simply based on the geographic of where our digital data happens to reside at any point in its global travels. And so, yes, I think Congress should make sure that any surveillance that results in the collection of Americans communications and Fourth Amendment protective information needs to happen pursuant to statute authority and which judicial oversight. There's no problem with the President having inherent constitutional authority that conducts surveillance of foreigners overseas, but the second that starts to put Americans' information, the Supreme Court has made very clear in Fundi that to fight the president's constitutional powers over foreign affairs, even in war time, anytime Americans individual liberties are at state, all of the branches of government have a role to play. And that's the case for culpable state surveillance today, the way it operates.

- Great, thank you very much. There's a lot on the table, and I'd like to open the floor to about five minutes that we can take questions from individuals. I'll note to my introduction to Foreign Intelligence law students as well as my Advanced Foreign Intelligence law students exams open May 2nd. But this is your chance to ask people who really know what they're talking about. So just let me throw that out there for all these students out there. We're go ahead and take the first one.

- Is that okay?

- That's fine. Anybody can ask questions. I particularly encourage April, my advanced board Intel law class, as well as the intro to , as if you'd like to ask the questions, please do.

- [Student 1] for the panel. This is the first and the only time I probably for this panel. I have quick questions for the . There's a lot of discussion about the warrant requirement, which is something that Congress is gonna be sitting for US person for 702. Both of you at the end, Brad and Mike, suggested that, you know, this would be very unworkable, it could create all sorts of delays in accessing the data. And I just wanted to know if FBI or DOJ had at any point actually done an analysis or a study of that issue and found that there would be complications. I mean is this sort of just a, I guess for lack of a better word, a hunch that this would create lots of problems understanding that there have been many times that the data is data. You know, it just sort of strikes me, similar to arguments made when the Act provisions expired in 2020, there were lots of arguments made that, you know, this going to slow down our investigative authorities and that will lead to a lot of problems. And now we're in a position where the administration basically doesn't wanna renew those last provisions or at least Section 210 recognizing that it just doesn't hold enough value. So I just wanted to know more about why are you so, why is the concern about why the requirements is so high in this , you say about that? And then quickly also for Chris. I know the administration has very interested in classifying more examples 702 value and recently there has been disclosures that are alleged have been made by a Massachusetts International Guardsman. Many of those documents that are now the public domain, FISA being the source, many if not most, perhaps all of them seem to come from 702. Just wondering if the administration might at some point acknowledge that those are example, are the value of 702 in a context? Or .

- Super quick. There's not like a study in the . It's based purely on, I would say two factors. One is the volume. So it's just self evident that we could not possibly process from a peak of 2000 to 210,000, that's just not doable, so we don't need a study to do that. Second is that we collect against a lot of foreign targets on, again, that's reasonably likely to obtain foreign intelligence. If you change it to a probable call standard that someone is, let's say an Asian of foreign power, just to give you an example, Alex is a operator, right? And we have information he's trying to send or ship something bad to Iran, or we have something, we wanna target him. We don't know that he's working for Iran. We can't prove he's an agent of a foreign government. We can't prove that he's a terrorists in the terrorist group, but we still very much wanna know what he's doing. Or you know, Chris is in in touch with a terrorist and they're having a conversation with the scene being code. We don't know whether Chris is in the terrorist

organization or not. We can't make a PC showing, but we very much wanna know, and 702 gives us that flexibility. And if you change it to a PC standard in report, we can't do the volume and we can't get the standard. That's it.

- Chris, I mean, yeah, Mike.

- Oh, thank you. So yeah, great question. So the way I see it, yeah, and I agree with Brad, we don't like to have statistics for a systematic analysis to really back this up. But when we look at how we're using our queries and how they're contributing to our operational actions and our investigation and our analysis, I think there getting two probable facts if we were have a warrant imposed, one is the delay. So we see many cases, the information that we are receiving from our databases is already in our possession, is time sensitive. So we are reviewing this information or finding operational actions that will allow us to to boom, as we say, where if there were a delay, those we would dismiss those operational actions or there would've been ongoing harm if we were unable to warn or assist a victim. And so there is a cost to imposing a delay on these while we're waiting again to access information that's already that's not in our possession. The second part is though the probable cause, as Liza noted, this will result in fewer queries if you're required to seek a warrant every time you're doing a query for a US person term. In some categories of queries that the Title I would be completely unachievable when we're looking to identify victims so that we can figure out where they are down warland or when we are looking to identify information of paying the victims so that we can gain a greater understanding of the threat to them so that we can help them defend themselves in the most informed way as possible. So one additional effect to that, as we're seeing theoretically fewer of these, what we will be doing is reverting to manual review of this data that we are authorized to review in its entirety. And that is gonna result in missing connections where we're going to have information that would allow us to understand and applaud that's going to be spread across several different accounts that a single analyst may not be reviewing all of them, or a large period of time where we may have important communications with foreign intelligence target overseas that occur over a course of months and you can't really understand the nature of the threat without pulling all of those together and looking at them at once.

- Thank you. Chris, speak up.

- Very quickly. So I think we know that to get pre-authorized, we're gonna to make our case to, in the first instance our representatives and some not on classified basis, but ultimately we're gonna to make the case of American people and that's gonna require new classifying information. You started trying to do that. I think the AG and DNI letter that my boss sent the member of the Congress in February some initial information. You know, I think this is something hard to do, so you have to do it carefully because our adversary study what we say about this, try to identify it, power of intelligence activities. So we're constantly trying to balance providing information to American people while with the need to and methods. On your second question, I think you know what the answer is, except with my colleagues from the Department of Justice and the FBI here. I mean, .

- [Student 2] So my question primarily for Brad and Chris. So I meant, I noticed in a lot of your answers about, you know, why by all this activity, K 702 or other bulk data kinda large. A lot of it has to do with practicality, A lot of it has to do with competition, or you know, a lot of the people have looked at this and said it's okay, or said it not said that it wasn't okay, right? A lot of these negative responses. I'm wondering is there an affirmative case for this activity, right? That with our right to be secure in person House and all that good stuff, is there an affirmative constitutional argument for this stuff that that doesn't just say, hey, nobody says it's wrong or this other things, you know, that says it's okay? And last caveat, if you could frame your response in a kind if answer.

- Sure, our students . This is the alternative.

- Sure, so recognizing that we're running out of time and there's people on the stand that are probably not gonna agree with everything I say, but I think that there's, you know, 702 is a program that focuses on non-US person, or overseas for communicating foreign intelligence. I think that, you know, if you look at classic Youngstown framework that Justice Jackson established when the president, This is an area where the president has inherent authority to conduct activities overseas. It's been bolstered by Congress passing statute that authorized it. I think that the executive branch has the strongest footing to engage in those sorts of activities. I think that Brad went through this sort of logic. So the vast majority of 702 doesn't deal with incidental question of US persons, it deals with targeting non-US persons located overseas. And I think that that's pretty squarely constitutional. I think Liza raised some constitutional concerns about US person queries. I think Brad explained the executive branch logic for why that's lawful. I think there's a number of cases, a number of areas where when the lawfully acquired intelligence, and I think everyone agrees we're part of the lawful, we're allowed to look at that information for lawful purposes as much what certainly do under 702. Now there are distinctions between people who try to sanction this and the other Congress where we engage in those activities. But I think, you know, today, Congress on three occasions and the fifth got a number of occasions have found it to be lawful.

- Really quickly, sorry. The notion that collected it lawfully, which by way and loss of certification they're only targeting foreigners, you can then use it for any lawful purpose. Is literally the opposite of minimization, right? Minimization is minimize your use of it. And minimization is not just in statutory requirement, it is a constitutional one. Youngstown is a separation of powers case. It did not involve the Fourth Amendment. If Congress and the executive branch fully agree with each other that they should violate Americans' Fourth Amendment right, we still can't do it, so. Things are moving on, I'm so sorry. sense. But great questions, Trent. Thanks. Brad, if you wanna ? You're good. All right, unfortunately, I'm so sorry we have run very, long run this panel. The purpose of this panel was to set the table, so to speak, to lay it all out there, what the issues are. I hope that you share my view that this was from .