U.S. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

(PCLOB)

PUBLIC FORUM ON FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA) SECTION 702

Thursday, January 12, 2023

A P P E A R A N C E S

SHARON BRADFORD FRANKLIN
Chair, Privacy and Civil Liberties Oversight Board

GENERAL PAUL M. NAKASONE
United States Army
Commander, United States Cyber Command
Director, National Security Agency/Chief, Central Security Service

JULIAN SANCHEZ
Cato Senior Fellow

JERAMIE SCOTT
Senior Counsel, Electronic Privacy Information Center

APRIL DOSS
NSA General Counsel

CHRISTOPHER FONZONE
ODNI General Counsel

CINDY COHN

Executive Director, Electronic Frontier Foundation

MIKE HERRINGTON

Senior Operations Advisor, FBI

DR. JEFF KOSSEFF

U.S. Naval Academy

DR. JONATHAN MAYER

Princeton University

P R O C E E D I N G S

MS. FRANKLIN: Hello, I'm Sharon Bradford Franklin, Chair of the Privacy and Civil Liberties Oversight Board. Together with my fellow Board members, Ed Felten, Beth Williams, Travis LeBlanc and Richard DiZinno, I'd like to welcome you to today's public forum.

Today's forum will help to inform the Board's oversight of Foreign Intelligence Surveillance Act, Section 702. Section 702 authorizes the government to target non-Americans located outside the United States, and to collect the content of their communications such as e-mail and phone calls. The government may also collect the information of U.S. persons through what is called incidental collection when they are in communication with these foreign targets.

Our role as the Privacy and Civil Liberties Oversight Board is to review federal counterterrorism programs to ensure that they include appropriate safeguards for privacy and civil liberties. Since Section 702 is a program with multiple purposes that

include counterterrorism, the PCLOB has long conducted oversight of Section 702 surveillance. In fact, dating back to 2014, the PCLOB conducted its first review of surveillance conducted under Section 702 and issued a comprehensive report on Section 702. Indeed, that report is still considered the most comprehensive unclassified description of the Section 702 program.

In its report, the Board found that the Section 702 program was valuable, but also identified certain aspects of that program that raise particular privacy risks, including the potentially large scope of incidental collection of U.S. persons' communications, the use of about collection to acquire communications that are neither to nor from targets of surveillance, and the use of queries to search for the communications of specific U.S. persons within the information that has been collected.

That report set out 12 recommendations to resolve these issues, most of which have been implemented by the intelligence community, but a number of which have not yet been incorporated into the law and the program's procedures. As people

watching this program, that are public forum are likely aware, Section 702 is scheduled to sunset at the end of 2023 unless Congress Acts to reauthorize the statute. To carry out our oversight role, the Board plans to release a new report on Section 702 to inform the upcoming public and congressional debate.

This new report will update the PCLOB's 2014 report and provide additional recommendations in light of new developments over the past several years. With Section 702 authorities set to expire at the end of 2023 as well as international debate regarding U.S. intelligence collection practices in recent years, now is a critical moment to review current policies and practices under the law and consider potential additional reforms that would strengthen protections for privacy and civil liberties.

Today's public forum is designed both to inform the Board and the public as we engage in oversight of the government's use of Section 702. The forum will start in a moment with a keynote speech from General Nakasone, Director of the National Security Agency and commander of the U.S. Cyber

Command. It will then be followed by two panels.

Before we begin, I want to thank all of our panelists and speakers for joining us today, as well as our tremendous staff for all of their incredible work in planning today's forum and making it possible for us to come together today online. And in terms of logistics, I want to note that today's event is being recorded and the recording will be posted on the PCLOB's website. So I want to turn now to General Nakasone for his opening keynote remarks.

General Paul M. Nakasone assumed his present duties as commander, U.S. Cyber Command and director, National Security Agency and chief of the Central Security Service on May 4 of 2018. He served as commander of U.S. Army Cyber Command from October of 2016 to April of 2018. And previously he led the Cyber National Mission Force at U.S. Cyber Command. He is a native of White Bear Lake, Minnesota, and he is also a graduate of Saint John's University in Collegeville, Minnesota, and he holds graduate degrees from the U.S. Army War College, the National Defense Intelligence College and the University of Southern

California. So I now turn it over to General Nakasone for his keynote. Thank you very much for joining us.

GEN. NAKASONE: Thank you, Chair. On behalf of the intelligence community, I want to thank the Privacy and Civil Liberties Oversight Board, as well as those watching today for your interest in one of the U.S. government's most important foreign intelligence authorities, Section 702 of the FISA Amendments Act. The authority will sunset on December 31, 2023, unless Congress passes legislation to reauthorize it. Without Section 702, we will lose critical insights into the most significant threats to our nation. Our role today in talking about this authority is to help inform the forthcoming congressional debates.

You may be already familiar with the legal authority. For those who are not, a brief history, FISA, the Foreign Intelligence Surveillance Act dates back to 1978. Title VII, which includes Section 702 was added as part of the FISA Amendments Act of 2008. The additions to FISA were made in part to address changes in communications technologies, and the

growing global use of U.S. communication services, including some of the highest priority foreign intelligence targets. This legal authority allows the intelligence community to collect the communications of many of our most critical foreign intelligence targets located outside the United States, who use these U.S. infrastructure and services to communicate.

FISA Section 702 is irreplaceable. It is focused and limited, yet agile enough to address national security threats in an ever-changing technological and threat environment. It allows the intelligence community to acquire the communications of specific foreign actors overseas and use those details to identify terrorist plots, track spies, identify cyber-attacks and try to stop them, as well as provide U.S. policymakers with the information they need to understand a wide range of national security threats.

As someone who was in the Pentagon during the attacks of 9/11, I have a personal perspective about how this authority has helped secure the nation in the years since those attacks. As the commander of U.S.

Cyber Command, the director of National Security Agency, I have seen firsthand how FISA Section 702 has continued to provide critical intelligence that has kept our country and our allies safe and secure. Since the initial enactment of 702 in 2008, our threat environment has evolved substantially.

Our focus has shifted from counterterrorism to strategic competition. In the two decades since 9/11, we have seen the People's Republic of China evolve as America's primary geopolitical challenge. The PRC is the only competitor with both the intent to reshape the international order and increasingly the economic, diplomatic, military and technological power to advance that objective.

Meanwhile, Russia continues to pose an acute and ongoing threat to regional security in Europe. We've also seen the nature of conflict change drastically, where cyberspace is a battleground and cybersecurity has become one of our most pressing national security concerns. And as we have seen in the last year, the world has moved into an era where the shift from competition to crisis to conflict can

occur in weeks or days, or even minutes, rather than years.

To address these evolving challenges and continue to keep our nation secure, the intelligence community needs authorities that are technology-neutral and agile. FISA Section 702 is just that. This authority plays an outsized role in protecting the nation, providing some of the U.S. Government's most valuable intelligence on our most challenging targets. It provides unique information with minimal risk.

In addition, when we look at the National Security Agency's overall reporting intelligence from FISA Section 702 accounts for an oversized portion of reporting relative to its cost. This authority provides the U.S. government irreplaceable insights, whether we are reporting on cybersecurity threats, counterterrorism threats, or protecting U.S. and allied forces.

FISA Section 702 has helped us to understand the strategic intention of the foreign governments we are most interested in, the People's Republic of

China, Russia, Iran, and Democratic People's Republic of Korea. We have learned about espionage plots to obtain sensitive U.S. technological information. We have used information from FISA Section 702 to prevent weapon components from reaching hostile foreign actors. We have identified threats to U.S. troops.

We have discovered sanction evasions and disruptive foreign cyber-attacks, and intelligence acquired under this authority has stopped significant terrorist plots, saving American lives. I want to repeat that, we have saved lives because of 702. Last month, I was part of a panel at the Reagan National Defense Forum with Senator Angus King about hybrid warfare with other top military, government and industry leaders.

Senator King discussed how difficult it is to talk about successes in the intelligence community since successes often means that terrorist plots were foiled or cybersecurity vulnerabilities were patched and nothing happened. As the senator noted, how do we demonstrate to the public the fact that the dog didn't bark in the night. It's difficult to provide you with

concrete examples of how this authority has helped protect the country because so many of our successes are just that, preventing the dog from barking in the night.

We also have to limit what we share publicly because our foreign adversaries are paying close attention to how the intelligence community and most specifically the National Security Agency function in hopes of learning our tradecraft in evading detection. But it is important for the public to understand why this authority matters. So where we can declassify stories that tangibly demonstrate its impact on our security, we will.

Let me start with an example from the early days of 702. In 2009, NSA discovered information in 702 data, indicating an al Qaeda courier in Pakistan was in communications with an unknown individual in the United States. We passed this information to the Federal Bureau of Investigation who found that the individual Najibullah Zazi and a group of co-conspirators had imminent plans to detonate explosives on the subway trains in Manhattan. The attack was

prevented. Zazi and his co-conspirators were arrested and pled guilty, or were convicted of their roles in the planned attack.

Again in 2014, FISA Section 702 provided the intelligence community key insights into ISIS planning and senior members of the terrorist organization, including ISIS leader Haji Iman, ultimately leading to the removal of Iman preventing attacks. And again, as Senator King mentioned, the dog didn't have to bark. The information we get from 702 today is no less critical even as our focus has shifted towards strategic competition. This authority continues to provide critical intelligence to our policymakers.

Let me tell you about a few of the intelligence community's most recent successes. The U.S. government identified multiple foreign ransomware attacks on U.S. critical infrastructure in 702 data. This intelligence position the government to respond to and mitigate these events, and in some instances, prevents significant attacks on U.S. networks. In another recent example, the intelligence community used information from 702 discover -- to discover that

a foreign adversary had used a cyber-attack to acquire sensitive information related to the U.S. military.

And harkening back to the counterterrorism origins of the authority, FISA attacks 702 information contributed to a successful U.S. Government operation against one of the last remaining 9/11 architects, Ayman al-Zawahiri. These are just a few of the ways this authority has helped keep this nation safe. Stories like this are typically classified. There are countless others that we cannot share without putting the nation's security and classified sources and methods at risk. But I hope these examples give you a sense of just how vital Section 702 is to our national security.

So I've talked about how this is a critical authority and a unique authority for the U.S. Government's foreign intelligence mission. But the PCLOB is tasked with ensuring we are also protecting the rights of U.S. persons. Civil liberties and privacy are central to the implementation of FISA Section 702. The law was designed with safeguards to

protect the rights of the American people and our allies. To that end, the collection must be focused on individual targets, meeting specific criteria that must be documented and verified by those within and outside the intelligence community. Section 702 cannot be used to target Americans anywhere within the world, or any person outside the United States, regardless of nationality, no exceptions.

Excuse me. Let me say that again, Section 702 cannot be used to target Americans anywhere in the world or any person inside the United States, regardless of nationality, no exceptions. The government is also prohibited from targeting a foreign person abroad to learn about an American. Any information unintentionally collected is handled consistent with specific court-approved procedures intended to protect the civil liberties and privacy of U.S. persons and persons inside the U.S. By executive order we extend comparable protections to foreigners.

This authority has layers of civil liberty and privacy protections embedded throughout from annual training to the use of the authority that I

took again just last week, to policy controls on when and how queries are conducted to technical controls on who has access to the data and how it is secured.

Here at the National Security Agency, these safeguards are built upon a strong culture of compliance with a dedicated internal compliance group focused on identifying the sources of any possible incidents, and approving the protections in place. If there's an incident, NSA analysts report it and it is investigated by our compliance group. And after the investigation is completed, our training policy and technical controls are updated as needed.

What is most important from my perspective is that these safeguards assure privacy protection at the same time do not hamper our ability to produce foreign intelligence. Oversight and transparency are also baked into the law. All three branches of the U.S. Government have a role in the oversight of Section 702. In the legislative branch, the congressional intelligence and judiciary committees also provide stringent oversight of the program, routinely reviewing the government's use of the authority.

Within the executive branch, the Department of Justice and the Office of the Director of National Intelligence look at all 702 targeting, review potential compliance incidents and oversee other aspects of the program.

And of course, all of you as members of the PCLOB play an important role in the ongoing oversight of the program, particularly as it releases to the board mission to ensure that the Federal Government's efforts to prevent terrorism are balanced with the needs to protect privacy and civil liberties.

In the judicial branch, the Foreign Intelligence Surveillance Court plays a crucial role in overseeing NSA's activities under FISA Section 702. The FISC is comprised of Supreme Court-appointed Article III judges, and provides an expressed oversight in NSA's use of the authority.

In my personal opinion, the court applies great rigor in carefully considering all information bearing unlawfulness of the government's activities authorized by Section 702. It conducts a comprehensive review of the program every year, as

well as on a continual basis ensuring incidents of noncompliance are addressed.

Over the next year, we in the intelligence community will be working with our partners to ensure the immense value of FISA Section 702 and the civil liberties and privacy protections built into the authority are clear to Congress and the public. There will be conversation and debate. We welcome that. Events such as this are an opportunity to engage directly with people who care about these critical issues.

So under Section 702, both national security and civil liberties and privacy are preserved and protected. It is an and, and not an or that connects these two important goals. Neither is compromised for the other.

702 authorities provide exquisite foreign intelligence that is focused on non-US persons outside the United States, and specific invaluable insights that protect our nation, intelligence that cannot be obtained through other means. These authorities are executed by trusted intelligence community personnel

that are rigorously trained and certified, self-report when and if they make errors and operate under oversight from every branch of our government.

This oversight provides a verification necessary to demonstrate the intelligence community's lawful and appropriate use of Section 702, allowing us to carry out our crucial work while ensuring our rights as American citizens are protected. Thank you very much for the opportunity to talk with you about this important topic. I look forward for our forthcoming discussions.

MS. FRANKLIN: Thank you so much, General Nakasone. Really appreciate your remarks and your taking the time to join us here today. So we are going to turn next to our first panel, and I just have a few housekeeping notes for those watching -- watching.

For each panel, we will first hear brief opening statements from each panelist, and then my fellow Board members and I will take turns asking questions of the panelists with each of us asking one question at a time and following that answer, moving

on to the next Board member. And we will cycle through as many times as we have time during the time for that panel.

So, turning to our first panel, if they can all come on screen with their cameras, that would be terrific. The panelist will make opening statements in the following order. First, we will hear from Christopher Fonzone, who is general counsel for the Office of the Director of National Intelligence, or ODNI. We will then turn to Julian Sanchez, who's a former senior fellow at the Cato Institute.

We will next hear from Jeramie Scott, senior counsel at the Electronic Privacy Information Center. And the final panelist to make brief opening remarks will be April Doss, general counsel of NSA. So, again, brief opening remarks by the panelists turning first to Chris Fonzone. Thank you.

MR. FONZONE: Thank you, Chair Franklin. Can you hear me? Excellent. Well, thank you Chair Franklin and all the members of the Board for inviting me here today. I very much appreciate the opportunity to be here with my fellow panelists to talk to you

about Section 702.

Today's discussion is an extremely important one as it implicates some of our most vital interests and our most cherished values. Indeed, I doubt there are many people who appear on the screen today or who are watching from home who would disagree with either of the following two statements.

The United States, like all or nearly all other nations, needs to collect foreign intelligence in order to fulfill its obligation to keep its people safe and secure. And the second statement, our country's commitment to protecting individual liberties limits what the Government may do in the name of national security.

Yet, even as simple as it is to agree on these basic principles, both of which we have long recognized as being part of our Constitution, it can often be difficult to work through how to, as I know my fellow panelist April is fond of saying, weave them together.

How should the government be allowed to collect foreign intelligence? When should it be

prevented from doing so? When should it be required to satisfy some legal burden of specific need to an independent court? What happens in an emergency when lives are at stake? These are not easy questions and there are no obvious easy answers.

Luckily, however, this is an area where we are very much not writing on a blank slate, for the three branches of our government have long worked together to develop a framework for how to advance our national security needs while protecting civil liberties – with a key part of this framework being the Foreign Intelligence Surveillance Act.

President Carter recognized this when signing the original FISA in 1978. "One of the most difficult tasks in a free society like our own," he wrote in signing statement, "is the correlation between adequate intelligence to guarantee our nation's security on the one hand and the preservation of basic human rights on the other."

FISA, in President Carter's view, appropriately accounted for both of these interests. As he put it, FISA "sacrifices neither our security

nor our civil liberties and it assures that those who serve this country in intelligence positions will have the affirmation of Congress that their activities are lawful."

Of course, the passage of the original FISA did not end debate over these issues. Indeed, in the 40-plus years since FISA's passage, both technology and the geopolitical landscape have continued to change, and Congress has on multiple occasions returned to FISA, amending the statute to recognize new realities.

Most importantly, certainly for our purposes, in 2008, Congress enacted Section 702, which recognized that, due to changes in telecommunications infrastructure, foreign intelligence targets - such as proliferators, hackers, terrorists and spies - often rely on U.S. telecommunication services.

With Section 702, Congress thus authorized the government to seek a court order to acquire the communications of these foreign intelligence targets from U.S.-based telecommunications companies, while at the same time requiring safeguards that protect the

privacy and civil liberties of U.S. persons.

Interestingly, President Bush's remarks on signing the law that created Section 702 made a strikingly similar point to the one President Carter made 40 years earlier. Specifically, President Bush said, "This law will protect the liberties of our citizens while maintaining the vital flow of intelligence."

To be sure, the enactment of Section 702 did not end the debate over how we should collect foreign intelligence while protecting privacy and civil liberties. And material and important modifications have been made to that Section 702 program in the 15 years since it became law. For example, we've increased transparency around the program and put in place additional protections. And, as Sharon alluded to at the outset, the Board has played a vital role in coming up with these additional reforms. But notwithstanding these changes, the core of the program Congress created 15 years ago remains the same.

And while the fact that we have - that we're here today, of course, indicates that the debate

continues - there are three key points about Section 702 that are very much worth emphasizing.

First, the Section 702 program is lawful, as it is clearly authorized by statute, and courts have repeatedly found it to be constitutional. Indeed, this is something the Board recognized when it last engaged in an exhaustive review of the Section 702 program in 2014 and, in the years since that review, the case has only grown stronger.

This is because since the Board's last review, Congress has again reauthorized the authority such that Section 702 has now been enacted and reauthorized three times. Moreover, since the Board's last review, Federal courts have continued to confirm the board judgment as to Section 702's legality and constitutionality.

Which leads to the second point: the Section 702 program is extremely valuable and effective. I won't go into too much detail here, particularly since the Board reached this conclusion during its 2014 review. But General Nakasone's opening remarks provide additional details about the importance of the

program and how it provides critical intelligence on a range of national security challenges from counterterrorism to cyber to strategic competition to many others.

And General Nakasone's remarks only build on the remarks of many other IC leaders, including the DNI, who have emphasized how Section 702 provides critical intelligence.

Which brings me to a third and final point: Section 702 protects privacy and civil liberties. Again, General Nakasone has detailed many of the extensive protections Section 702 has -- puts in place. I know April Doss, who is joining me on this panel, and a colleague of mine from the FBI, who will be here on the next panel, will do the same. So I'll not try to repeat what they will say.

Rather, I will simply say a few words about ODNI's oversight role, which reflects the work it does, integrating the intelligence community and its statutory authorities and capabilities. Specifically ODNI's oversight efforts largely focus on promoting inter-agency coordination, prioritization, and

harmonization, particularly with respect to program-wide modifications.

This means that among other things, ODNI conducts in consultation with the Department of Justice reviews of Section 702 taskings, coordinates the provision of IC documents and briefings to Congress in consultation with DOJ, and leads, in consultation with DOJ, the Government's efforts to provide the public with information about Section 702 activities, including releases of FISC opinions, joint assessments, and the release of the annual statistical transparency report.

Of course, as prior statements have made clear, ODNI's work is only part of a detailed compliance regime, the upshot of which is that, as President Obama said in 2014, "The men and women of the intelligence community . . . consistently follow protocols designed to protect the privacy of ordinary people. They're not abusing authorities in order to listen to your private phone calls or read your e-mails." These statements were true then, and they're true now.

To be sure, the intelligence community is not perfect. As President Obama also recognized in the 2014 remarks, "Mistakes are . . . inevitable in any large and complicated human enterprise." But the important point is that when the intelligence community makes such mistakes, we own up to them. We disclose them as appropriate to the FISC, to the Congress, and to the public, and we set out to fix them.

Which leads to my final point, which I'll keep short.

I recognize that reasonable minds can disagree about these issues. I also know based on my time in government, that time in government is often full of the varied joys and frustrations of trying to develop practical solutions to the messy business of weaving together interests, diverse interests like the need to collect foreign intelligence and the need to protect individual liberties.

Viewed through this lens, I really do think 702 is a thoughtful solution to a complex issue, and I hope these short remarks have helped even a little bit

to illuminate why. Thank you and I look forward to the discussion.

MS. FRANKLIN: Thank you. We'll turn next to Julian Sanchez.

MR. SANCHEZ: Thanks, Sharon. And I'm grateful to have been asked to join this hearing. So, you know, I assume during these panels, we're going to have a lot to say in the weeds about the various compliance issues that have arisen over the course of the 15 year history of Section 702. But I hope you'll indulge with me if I lead not with a discussion of the weeds, but with a somewhat more radical critique of Section 702.

And that's that, you know, if we look at in effect how it operates, we see that in or each of recent years, the FISC has issued each year either one or two broad authorizations for 702 acquisition. And under each of those authorizations, the intelligence community has exercised its discretion to designate each year more than 200,000 individual foreign targets.

And under the aegis of that authority though,

the targets are of non-U.S. persons located at the United States, we know that a substantial number, certainly in absolute terms, even if a small as a percentage of the total take, substantial number of U.S. person communications, certainly when their one end of an international communication, but also we know for many years in practice and despite in explicit statutory prohibition, even many tens of thousands of wholly domestic communications were acquired as a result.

And if we sort of step back and say, well, what does this look like collection on this scale, where the decision about what to collect is delegated to executive branch officials with only this sort of programmatic authorization directly by the judiciary, I think, you know, the one clear answer is that these sound a heck of a lot like general warrants.

Now if there's a point on which Fourth Amendment scholars are virtually unanimous and there aren't many, perhaps, but this is one. It's the original function of the Fourth Amendment, the original motive behind the Fourth Amendment was

outrage over the general warrants and roots of assistance that were prevalent during the colonial era. And, you know, this is understandably sort of fallen into the background of Fourth Amendment jurisprudence.

We think today of the Fourth Amendment primarily as a guarantor of an individual right to privacy against unreasonable searches in effect typically enforced by the exclusion of improperly obtained fruits of such searches from criminal prosecution.

But if we look, you know, closely at the explicit wording of the Fourth Amendment, we get a somewhat different picture, a guarantee of a right to be secure, not just to individual persons, but the people collectively, even though in many other places in the bill of rights, the framers are happy to use individual language.

Indeed, the original monoclausal structure of the Fourth Amendment arguably does nothing but prohibit general warrants. That original language changed the last minute by a motion by Elbridge Gerry,

said that the right of the people to be secured in their person's houses, papers, and effect, shall not be violated by warrants issuing without probable cause or particularity.

And the change by Gerry to a dual clause structure was meant to emphasize even more strongly that this was a prohibition on such general warrants even issuing. And I think this is significant because it gives us an understanding of what the Fourth Amendment is trying to do that views the right protected by the amendment as something that is violated not at the time when a search is executed, but when a particular kind of authorization, when a particular delegation comes into existence.

And this is something that is reflected in a lot of the founding era rhetoric around the Fourth Amendment and against risk of assistance and general warrants. So, James Otis, a huge influence on Madison's drafting of the Fourth Amendment, argued against the resistive decisions that every households who are in the province will necessarily become less secure than he was before this writ had any existence

among us.

James Pemberton writing on behalf of the Quaker community of Philadelphia denounced general warrants for conferring powers that in any free society would be reprobated as overturning every security men can rely on. And more than two centuries later, I would note the idea that discretionary surveillance can impose disparate burdens on minority religious communities remains, alas, all too relevant.

So this is a collective or structural concern that's reflected in both the original wording of the Fourth Amendment, which identifies the issuing of non-particularized warrants as the moment at which the people's right to be secure is compromised and in the more familiar current version reflecting Gary's (phonetic) insistence on a more emphatic prohibition on the issuance of such non-particular warrants.

And I think if we re-center that idea, the idea that the Fourth Amendment is first and foremost about barring that kind of broad delegation of authority to the executive branch, we get a somewhat different view of Section 702. So consider the sort

of a mainstay of 702 apologetics, right?

The people who enjoy a right to be secure against unreasonable searches are the American people. 702 permits only the targeting of foreigners located abroad, who enjoy no such protections. So there can be no fundamental constitutional objection to the orders that 702 authorizes.

I think, you know, even though of course, you know, errors in implementation may themselves entail Fourth Amendment violations in practice. But I think, you know, by parallel reasoning we could say the general warrants of such concern to the framers would have been unproblematic because they didn't target anyone, I think the defect in that kind of defense is obvious in light of what I've said.

The Fourth Amendment is not a guarantee against unreasonable targeting, but against unreasonable searches and separately against even the issuance of discretionary non-particularized warrants, independent of the execution of that search.

Title I of FISA, FISA Classic (phonetic) reflected this understanding by requiring a warrant

for the interception of wire communications with one domestic endpoint, even if the domestic endpoint was not the target of collection. To be sure the discretion afforded to intelligence agencies collecting communications under the aegis of 702 is procedurally fettered rather than plenary.

But nevertheless, the statute contemplates the acquisition of U.S. person communications on U.S. soil on a programmatic rather than a particularized basis. And I think, you know, the fundamental question from a constitutional perspective has to be not who is targeted, but who's communications are searched and collected.

Now an obvious objection to this sort of analysis is, well, the FISC has demonstrated its willingness repeatedly to find Fourth to identify Fourth Amendment violations by the intelligence community in the execution of 702. It's identified quite a few. So why should we think that the FISC would overlook this supposed more fundamental defect that I'm arguing for? And I'll suggest two reasons.

The first is that the Fourth Amendment has

been sort of a victim of its own success, right? Clear rules do not tend to generate case law and the prohibition on general warrants is sufficiently clear-cut. Although we don't find a lot of occasions in our Fourth Amendment jurisprudence for the courts to emphasize it, it has faded into the background, whereas the role as a kind of regulator of criminal procedure has come to the forefront.

And second, I think the fact of the rules of standing under which American courts operate requiring a showing of individualized concrete harm, and the fact that Fourth Amendment litigation is overwhelmingly centered on questions about the admissibility of evidence in criminal prosecutions, creates a kind of distorting lens, right, where we emphasize the individual aspect --

MS. FRANKLIN: Julian?

MR. SANCHEZ: Yeah.

MS. FRANKLIN: Thanks. I'm sorry. I'm going to need to ask you to stop there. We need to keep the openings relatively brief so that we do have time for --

MR. SANCHEZ: Yeah.

MS. FRANKLIN: -- for questions. Thank you.

MR. SANCHEZ: So I just want to suggest that that this has created a distorting lens that disconnects the Fourth Amendment in -- as it exists in current case law from the thing that the framers of the Constitution were most centrally concerned about. And I hope we can get into the weeds of specific clients issues.

MS. FRANKLIN: Thank you. Okay. We're going to turn next to Jeramie Scott for brief opening remarks. Thanks.

MR. SCOTT: Thank you, Chair Franklin, and members of the Board for holding this forum and inviting me to participate. EPIC has a long history of engaging with the PCLOB and on these issues, particularly on Section 702 of the Foreign Intelligence Surveillance Act. 702 continues to implicate serious privacy and civil liberties concerns and there are numerous issues to raise, one of the most persistent being the warrantless backdoor searches. I'll use my opening remarks to highlight

three other issues I hope the Board will look into.

One, the scope of abouts collection. Two, the use of 702 collection in cybersecurity investigations. And three, the need for greater transparency ahead of the reauthorization debate. The PCLOB should investigate the scope of abouts collections, about collection sweeping communications that merely reference a target and consequently it can end up acquiring wholly domestic communications.

As a PCLOB in the Foreign Intelligence Surveillance Court have both emphasized, the sheer breadth of abouts collection and the extent to which incidental collection is part of the parcel of abouts collection results in substantial privacy violations for the individuals whose personal information the government incidentally collects. The NSA previously failed to bring it abouts collection activities into compliance with statutory and constitutional requirements.

And for years NSA personnel recorded data collected to the Section 702 upstream program using U.S. person identifiers despite the express

prohibition against the use of these identifiers and NSA's own minimization procedures. In 2017, opinion deemed these queries "significant noncompliance" and a "very serious Fourth Amendment issue."

Ultimately, the NSA determined that cannot remedy the noncompliance and therefore decided to end abouts collection and purge all previously collected upstream data. But it's not clear that some type of abouts collections is not occurring today. In a October 2018 FISC opinion, there appears to have been a disagreement between the Government and (inaudible) in that case about whether the current limitations on abouts collections apply to downstream acquisition.

Given this disagreement, it is crucial that the PCLOB investigate and clearly define the current scope of abouts collections, especially given the history of persistent and significant noncompliance relating to abouts collection. The PCLOB should also review the use of 702 collection in cybersecurity investigations. The Board's previous report did not address the use of 702 in cybersecurity.

Since that report, the Intelligence Committee

has dramatically increased the use of Section 702 in the cybersecurity investigations. While the Government claims that Section 702 has played an important role in cybersecurity investigation, there is not enough public information to cooperate whether Section 702 is necessary to accomplish these goals and whether special safeguards are necessary in the cyber context.

The use of Section 702 as part of cybersecurity efforts raises privacy and civil liberties concerns given the potential breadth of collection and coring. According to the ODNI's statistical transparency report in 2021, the FBI conducted branch queries related to "Attempts to compromise U.S. critical infrastructure by foreign cyber actors." These queries include approximate 1.9 million in query terms relate to potential victims including U.S. persons, more than all report inquiries over the previous year.

Given this exponential increase, the PCLOB should investigate and report on the use of Section 702 in the cybersecurity context, such reviews within

the scope of the PCLOB, because National Security Agency has asserted that cyber-attacks are frequently a vector for attacks with terroristic motives, and therefore claim that cyber is an integral part of U.S. counterterrorism programs. U.S. Government officials have repeatedly emphasized the growing threat of cyber-enabled terrorism.

These officials have also emphasized the need to meet cyber-enabled threats with the same approach as traditional counterterrorism using a whole of government and all tools approach, including reliance on an intelligence tool. Additionally, according to the White House National Security Council, "Reliant on legal authorities that make theoretical distinctions between on-detect terrorism and criminal activity may prove impractical." All the more reason for the PCLOB to take a comprehensive review of the use of 702 and cybersecurity investigation.

It is vital that the public understand the scope of surveillance systems used in cybersecurity investigations, how the data collected is used and whether additional privacy and similarly protections

are necessary to ensure that these investigations -- investigative tools are not abused.

Last point I'll make is on the need for greater transparency measures. Despite the progress that has been made, the U.S. Government has not provided the classified information about Section 702. This lack of clarity hinders vigorous public debate on the benefits and costs of these programs. Therefore the PCLOB should push for greater transparency ahead of the reauthorization debate.

In particular, the PCLOB should once again seek the release of a declassified estimate of the number of U.S. persons whose communications have been incidentally collected pursuant to Section 702, an estimate members of Congress and privacy and similar groups have called for numerous times, a number the Government previously said it -- previously said it would provide before doing an about-face and saying they could not provide it because of privacy and security concerns.

Additionally, I urge the PCLOB to recommend the further declassification of other influential FISC

documents and information that has bearing on the public and congressional debate on the reauthorization of 702. Thank you again for the opportunity to participate in this panel. And I'd be happy to answer any questions.

MS. FRANKLIN: Thank you. So the final panelist to make brief opening remarks before we turn to Board member questions is April Doss. I can't hear you. Can others hear? You're not muted.

MS. DOSS: How's that?

MS. FRANKLIN: Great. Thank you.

MS. DOSS: Wouldn't -- you know, the technical problems came from the NSA. Chair Franklin and esteemed Board members, thank you. Thank you so much for the opportunity to address and discuss FISA Section 702 with you on this panel. My name is April Doss, and I've been NSA's general counsel since May 2022.

Prior to becoming NSA's general counsel, I worked in academia, private practice and on the Hill. But I also previously worked at NSA in a variety of attorney and non-attorney positions for 13 years.

Throughout my tenure at NSA, I've witnessed firsthand the twin and deeply interwoven successes of the 702 program in producing critical foreign intelligence for the U.S. and her allies, and in protecting the privacy rights and civil liberties of persons in the U.S. and around the world.

National security law is often thought of as a balancing of the national security interests of the U.S. as a whole against the rights and liberties of individual people whose privacy might be impacted during national security operations. However, rather than accomplishing one at the expense of the other, NSA has woven privacy and civil liberties protections into the way in which the agency executes its core national security responsibilities as signals intelligence and cybersecurity.

NSA's signals intelligence or SIGINT mission involves the use of electronic surveillance to collect information about the capabilities, intentions and activities of hostile foreign powers, international terrorist groups, malicious cyber actors, and other foreign entities or their agents to protect the U.S.

and its interests while ensuring that the legal rights, freedoms and civil liberties of Americans remain fully protected.

As General Nakasone said in his opening remarks, Section 702 may not be used to target anyone located inside the United States, nor may the statute be used to target an American anywhere in the world. No exceptions. Rather Section 702 of FISA provides a court-supervised regime that permits the intelligence community to obtain the compelled assistance of U.S. telecommunications providers to target foreign persons located outside the U.S. who possess or are expected to communicate foreign intelligence information that satisfies the carefully vetted intelligence requirements of U.S. policymakers.

For completeness, I also note that a separate legal regime embodied in Executive Order 14086 provides comparable protections to foreign persons, because privacy interests might be impacted by NSA signals intelligence activities, to include the agency's 702 activities. It's not sufficient, however, for me as the lawyer who works behind the

closed doors of NSA to simply declare that we're doing enough.

We must show and explain to the American people how the Government not only strives to achieve its national security interests, but how protection of constitutional rights and civil liberties is woven into the very fabric of NSA's use of the authority provided by 702.

In particular, the statute requires court-approved procedures and continuing oversight by all three branches of government to ensure that the intelligence community's use of the authority remains lawful. To its credit, this oversight regime has resulted in the identification, reporting and correction of compliances incidents, as well as periodic adjustments to the statute and to its implementing procedures.

For example, during the last reauthorization of Section 702 in January 2018, Congress added a new requirement for court-approved procedures to govern intelligence agencies queries of law 702-acquired information.

Even though 702 has been in use for over 14 years, it's not surprising that the law remains a topic of intense interest, especially during a period when it's again due to sunset unless reauthorized by Congress. So with that in mind, and recognizing the importance of brief remarks, I'd like to take just a few moments to dispel some myths about the 702 program, and then briefly discuss NSA's culture of compliance. Each decision to target a person under Section 702 is an individualized one, made on a case by case basis and subject to rigorous review.

Prior to initiating collection, pre-targeting justifications are reviewed by at least two different people beside the original analyst. Those checkers evaluate the information offered and the reasons provided by the analyst to confirm that the information gathered demonstrates the subject at the targeting as a non-U.S. person outside the U.S. and who possesses or is likely to communicate foreign intelligence that is responsive to those intelligence needs.

After collection is begun, as analysts must

document their post-targeting analysis on a routine basis. If an error is discovered, analysts must self-report that error, so it can be tabulated and ultimately forwarded to external overseers. But self-reporting is not the only checking mechanism. Compliance officers, auditors, lawyers and investigators continually review and re-review targeting decisions and make sure that analysts acts appropriately or in the case of a compliance incident that the incident is promptly reported and addressed.

In recent years, these compliance incident reports have been made more accessible to the public, as demonstrated by the thousands of pages of court decisions and other materials that the intelligence community has declassified and released over the past several years. This overall increase in transparency demonstrates the extent to which the compliance regime is functioning effectively and robustly.

The Foreign Intelligence Surveillance Court takes its role in the FISA process extremely seriously, requiring all incidents of 702 noncompliance to be reported immediately to the court,

whether they involve U.S. or non-U.S. persons, and it regularly mandates the government to correct incidents of noncompliance to the court's satisfaction.

Perhaps the most difficult part to convey through facts or figures or statistics is NSA's culture of compliance. This culture of compliance stems from a deep respect for the U.S. Constitution and adherence to the rule of law, which is woven into everything that we do. Even after many years at NSA, there's one anecdote that stands out for me as representative of that culture of compliance.

It was 2005 and I had just started a new position in NSA's Office of General Counsel, where I would be advising analysts on intelligence law. As I was awaiting my first assignments, my supervisor handed me a stack of thick paper bound volumes. These were the complete five volume report at the Church Committee, the precursor to the Senate Select Committee on Intelligence, documenting its findings from the mid-1970s investigation into spying on Americans by the U.S. intelligence community, and the 1950s, '60s and '70s.

My new boss told me to read the reports and understand that history with a particular eye to the parts that focused on NSA. Although it had been 30 years since that report was published and almost 30 years since FISA had been enacted, reading those reports was part of my on-the-job training for the work that I would be doing. Stories like this are common at NSA across all organizations.

NSA's memory of past events has created a profound respect for mechanisms of accountability, supervisors, senior analysts, lawyers, compliance officers, technical specialists, and others make sure that all of NSA's formal compliance programs are supplemented with a living history and institutional memory in which a commitment to protecting privacy and civil liberties forms the bedrock of everything we do.

MS. FRANKLIN: Thank you.

MS. DOSS: (Inaudible).

MS. FRANKLIN: If I could -- if I can ask you to please wrap up. We -- board members are -- there are five of us more -- to ask more questions. Thank you.

MS. DOSS: Thank you. Thank you again, for inviting me to speak at this forum. And I look forward to a thought-provoking discussion.

MS. FRANKLIN: Thank you. Thank you to all our panelists. And sorry, with five of us and time being short, we're going to cycle through the board. We're going to switch our order for the two panels. So hopefully, we all have a chance to ask multiple questions. And we'll go one question at a time. For this round, we're first going to get a question from Travis LeBlanc.

MR. LeBLANC: Thank you very much, Chair Franklin. And thank you to all the panelists for joining us today. I appreciated your remarks as well as those of General Nakasone. Very much appreciate everyone being here today. There is no doubt Section 702 collects a vast amount of information as publicly relayed in the Board section 2014 -- in the Board's 2014 report on Section 702. In that same report, the Board noted that some of the information in -- under Section 702 includes U.S. person communications, or information of or concerning U.S. person information.

Today, Section 702 authorize executive branch officials to make targeting decisions on specific selectors without any judicial oversight. There is no individual or particularized basis for the targeting decisions overseen by an independent magistrate or judge. Mr. Sanchez, do you believe Congress should require the intelligence community to obtain a FISA order or warrant to run queries on U.S. persons under Section 702?

And if so, do you believe that the Constitution requires an order or warrant for such queries? I recognize the significance and import of this issue. And while directing the question to Mr. Sanchez, invite any panelists to respond as well.

MR. SANCHEZ: You know, I do and in light of certainly of the -- the enormous scale of collection. And in particular, given the sort of dual-hatted role of the FBI, which has access to these -- this intake database. So we have this sort of enormous scale of collection nominally for foreign intelligence purposes. And we see a pattern of very large-scale querying by FBI on the order of, in some cases,

millions of queries per year, sometimes in very large batches of whose ability to satisfy even the internal querying standard is dubious.

I think it suggests the need to involve a magistrate for those purposes. Two reasons, in particular I'd say one, after the 2018 imposition of requirements for FBI analysts to return to the FISC when they need to run queries for purely criminal investigative purposes, we find reports after the fact that query seemed to have continued for those purposes without obtaining the required authorization from the FISA court. And also because, you know, the FISC itself repeatedly, after being often belatedly notified about compliance issues have said that they've found what appeared to be on the FBI side, either widespread misunderstanding of or indifference to the fundamental querying roles and key terms such as likely to return by information related to foreign intelligence, that had been essential to the querying policies since the inception of the -- of those programs, you know, more than 14 years ago.

So I think, you know, what it demonstrates

pretty well, is it delegating this kind of decision-making authority to agents of the executive branch with oversight only after the fact and kind of on the honor system has not worked out very well. I think we've sort of tried compliance whac-a-mole for long enough. And, you know, the evidence is that the issues keep arising.

MS. FRANKLIN: Thank you. So the next question is from Beth Williams.

MS. WILLIAMS: Great. Good afternoon, and thank you to all of our panelists for being here today. My questions for Mr. Fonzone. Some commentators have recommended that the administration should be open to accommodating the concerns of numerous members of Congress about the improper use of intelligence authorities for partisan reasons, specifically with regard to crossfire hurricane.

It's my understanding that the improper use of authorities related to that investigation did not implicate Section 702 authorities. Can you comment on whether that is accurate? And can you also comment on what protections exist or should exist to ensure that

Section 702 is not weaponized (phonetic), either wittingly or unwittingly, in service to any partisan purpose?

MR. FONZONE: Sure. Thank you. Thank you, Board Member Williams for that question. Yes. First, I can confirm that the high profile discussion of a FISA compliance incident with respect to crossfire hurricane did not involve the Section 702 program.

I also can confirm that the IC is – and I would ask April to weigh in here, as she talked about it - and I'd say it's culture of compliance.

I think that's a culture of compliance that exists across the intelligence community, and the intelligence community is very much focused on being scrupulously apolitical in how it wields its authorities. I think we recognize the power of those authorities and that they have to be wielded in a way that can maintain the trust of the U.S. people. So I think leads to your last point, which is, although I think that the IC already operates in a scrupulously apolitical way, the DNI has made clear that we're open to discussing reforms with Congress that would improve

-- that would preserve the program's efficacy while adding to civil liberties and privacy protections.

And if there are reforms of that nature, that would address the concerns that members of Congress have to make clear the fact that's already true, which is that the IC operates apolitically, I think we'd be open to having that discussion.

MS. FRANKLIN: Okay. So the next question is my turn. So I'm going to turn to April Doss, please. So as you're well aware, before the spring of 2017, as part of upstream collection, the NSA conducted what has been called about collection where NSA collected not only communications to or from a target, but also communication about targets, such as where a target's e-mail address appeared in the body of an e-mail.

And in 2017, NSA announced that it had suspended that collection, essentially noting that the number of compliance incidents and the challenges in complying with the rules, the value of the about collection was not sufficient to overcome those. Then when Congress reauthorized Section 702 in January of 2018, it required that if NSA wants to restart about

collection, the government must first get approval from the FISA Court and then must also notify Congress.

To date, as we understand it, NSA has not restarted about collection. What can you tell us regarding whether NSA has any plans to resume about collection or what the standards or reasons would be for NSA to seek to restart about collection or whether NSA would oppose a permanent end to about collection?

MS. DOSS: With respect to the last part of your question, of course, NSA is delighted to take part in any classified and unclassified conversations with the Board. And certainly with the larger set of stakeholders, as we look at what reauthorization could potentially look like. As Chris mentioned, certainly, the intelligence community is looking to work actively with the Hill. We will be looking to the administration's position on this as on all other matters. And NSA's role was simply to be informed that discussion.

I would note that, you know, in General Nakasone's remarks, you know, he pointed to how

quickly the intelligence environment can change. He referred -- he gave the example of how quickly we can move from competition to crisis to conflict. And I think that it'll be important as we have those conversations about what additional reforms to the statute might look like that those conversations take into account the agility that the intelligence community will be able to need to retain in order to carry out new programs or new techniques, if needed. And as properly authorized as you pointed out, of course, most importantly, NSA is not currently engaging in any abouts collection. And if it had an intention to do so would go to the FISC, would notify Congress.

So that is the status that we're in. And of course, we would welcome the conversation in classified settings, with the Board, with ODNI and with the Department of Justice and others, on what the implications of that kind of statutory change could potentially be.

MS. FRANKLIN: Thank you. The next question is from Ed Felten.

MR. FELTEN: Thank you. And let me join my colleagues in thanking all of the panelists and General Nakasone for your remarks and your appearance and willingness to answer our questions today. I have a question for April Doss, which relates to the question of how NSA might be able to estimate the prevalence of U.S. person information in Section 702 collection.

This was a recommendation of the 2014 PCLOB report on Section 702, as you know. And as you also know, there's been a bunch of back and forth with Congress and others about this question. And my question for you is not -- today is not to debate the ins and outs of this. But simply to ask, what might NSA do? What might Congress do? What might we at the PCLOB do to move this issue forward? In light of the obvious value to Congress and the public from having insight into the extent of incidental collection of U.S. person information and the practicalities of the issue. What might be done to move this issue forward? And I think you're muted.

MS. DOSS: Thank you for that question. We

welcome discussion on any viable solution that's accurate, repeatable and focuses on foreign intelligence. Of course I know that in the next panel there'll be one of the presenters, one of the co-authors of the paper about One Proposed Approach (phonetic).

You know, in the past several years, NSA has provided the congressional oversight committees and the PCLOB with detailed explanations of methods that we have tried to use to estimate incidental collection, what metrics were produced and why those failed to produce an accurate or reliable metric.

As we've undertaken efforts over the years to try to do that, our efforts have been guided by three principles. First, that the approach should produce a metric that's meaningful and reliable. The approach would need to be replicable and mathematically sound. It would need to make clear what's being counted and what's not being counted. And it would need to produce a number that makes a genuinely useful contribution to the public discussion on 702 reauthorization.

Second, of course, the approach would need to safeguard civil liberties and privacy. As you know that's been one of our chief concerns is how to do that counting without creating a focus on U.S. person information, which, of course, is not our role. We are a foreign intelligence agency that stands at the shores of the nation and looks out.

And then third, of course, the approach has to be feasible, and shouldn't unduly divert resources from mission-essential functions. Those three principles have guided all of the approaches we've taken. And again, we welcome any discussion about viable -- potentially viable solutions that would be accurate and repeatable and focus on the foreign intelligence.

MS. FRANKLIN: Thank you. And next, we'll turn to Rich DiZinno.

MR. DiZINNO: Thank you, Chair Franklin. And again, I join my colleagues in welcoming all the panelists, and thank you for your time again. My question is for April Doss. April, thank you, again, for being here.

We've heard some discussion about the evolving cybersecurity threat and addressing that threat using Section 702 authorities. As we all know, the origin of intelligence collection activities that have since been codified under Section 702 arose in the aftermath of the 9/11 attacks. And the original sort of use case for operationalizing type of collection that's been since codified was to address that post 9/11 threat.

Without obviously getting into classified details, can you talk about the cybersecurity threats that we face as a country? How the use of Section 702 surveillance is being used to help meet those threats? And can you also touch on the differences in implications on privacy and civil liberties? Namely, as 702 surveillance authority is applied to address cybersecurity threats as opposed to sort of "Traditional terrorist threats," what are the relative impacts on privacy and civil liberties concerns in those two different contexts?

MS. DOSS: Thank you for that question. I think, you know, as we look at the mission impact,

General Nakasone, just a few minutes ago, gave some examples of some of those key intelligence threats to the U.S. national security, threats to critical infrastructure, and the ways in which 702 has helped to counter those, for example, through identifying foreign ransomware attacks on critical infrastructure, and cyber-attacks designed to acquire sensitive information related to the U.S. military.

If we look at the structure of the law itself, when Congress passed 702 in 2008, that decision was really driven by changes in global telecommunications infrastructure. Those changes remain equally relevant today. And one of the things that I think we can see echoed in the director's remarks a few minutes ago is that this authority has proven to be remarkably adaptable, and remarkably versatile. The authority is underpinned by the ways in which the telecommunications infrastructure had made the old Title I FISA framework, not obsolete, but less applicable to certain types of intelligence activities.

So Title I and the probable cause to believe

that an entity is an agent of a foreign power and those Title I warrants remain a core backbone of FISA. But the changes in telecommunications infrastructure that were taking place by the early 2000s drove this change to recognize that the intelligence community needed an additional set of tools. And what we found, what the director alluded to, is that these tools have been highly effective against a variety of targets.

In addition to counterterrorism, has been highly effective in looking at matters relating to cybersecurity and relating to broader national interests, and the kinds of intelligence priorities that we have in strategic competition with some of those key foreign adversaries.

So we would really welcome an opportunity to talk with you in more detail in a classified setting about how this looks in the cybersecurity context, and then how that might be -- how that might be conveyed appropriately in unclassified ways to provide additional context or clarity or transparency for the public at large.

MS. FRANKLIN: Thank you. I don't know how

many full cycles we will get. But we're going to keep going until the time is up for this panel. So back to Travis LeBlanc.

MR. LeBLANC: Thank you. I have a question for Mr. Fonzone. On Subsection F2 of I think Section 1881 FISA, requires the Federal Bureau of Investigation in criminal, non-national security investigations to obtain an order from the FISC prior to making U.S. person queries. I believe this is the provision that Mr. Sanchez was referring to earlier in his remarks, in which he I believe suggested that this authority has not been used by the FBI. Is that true? And if so, why not?

MR. FONZONE: So I think the -- we will have a colleague of mine from the FBI on the next panel. I think a question like this directed to the FBI's activities under the statute is probably best directed to him, Board Member LeBlanc. I'm happy to talk a little bit about why the FBI may conduct a U.S. person queries and some of the things ODNI has said about that in the past. But I think the specific question with respect to the FBI's behavior under that

statutory provision is probably best directed to my colleague from the FBI in the next panel.

MS. FRANKLIN: I'm going to let Travis go again, if you want to quickly since you didn't get it.

MR. LeBLANC: Sure. I will go again.

MS. FRANKLIN: Oh, you have to be quick.

MR. LeBLANC: I'm very quick all the time. Jeramie, Mr. Scott, you have several times in I believe your remarks mentioned that you believed it was important that there be safeguards that you would like to see implemented in the context of cyber. And I'm wondering if you have any thoughts on the kinds of safeguards that you believe should be implemented around the use of Section 702 in the cyber context?

MR. SCOTT: Thank you, Board Member LeBlanc, for the question. Let me first, you know, as I alluded to, we need actually more information about how cyber is being used in the first place to adequately narrow down what type of protections may need to be in place. Some of the issues there is kind of the scope of collection that's happening under cyber. And then how that information is being used

after the fact. Just like you have incidental collection generally with 702, that information is used.

Post-collection, there needs to be, I think, a review of how that information from the cyber context is being used and probably needs to be a narrowing of how that information is being used. And so it's only used for the kind of specific cyber context. And it's not then being used beyond that context, because just like the 702 in general, with the cyber, there's -- often it's an incidental collection of information from U.S. persons, including communications.

And there's -- and it's sort of a black box right now, I think, to the public, in terms of the scope of cyber, the privacy and civil liberties implications of cyber. So I think some of the same kind of protections that we see generally need to make sure they're applied to the cyber context, whether it's memorization (phonetic), whether it's the narrowing of the use of that data. Or sometimes perhaps even though requirement, a new requirement for

a warrant to search that information as discussed earlier in 702 in general.

MS. FRANKLIN: Thank you. Beth -- back to Beth Williams.

MS. WILLIAMS: So this question is for April Doss. April, for Americans who were very concerned about privacy threats, and there are many Americans who are, can you describe what you see is the threat to U.S. person's privacy from hostile foreign actors? And can you share if and how does Section 702 assist the United States in protecting the privacy of U.S. persons from foreign actors?

MS. DOSS: Thank you for that question. It is such an important one, you know, at the beginning of the day, at the end of the day, 702 is all about protecting the U.S. and her allies. And that includes protecting the U.S. people from all threats.

And when we use 702 to protect -- to identify and protect specifically against foreign threats, absolutely, we are looking at what some of these adversary nations are doing to try to gather information about American targets for

counterintelligence purposes. We are using it for force protection purposes. 702 is critical to support to military operations. It is critical to understanding the ways in which foreign adversaries are carrying out a whole host of activities that raise privacy and civil liberties threats to the American people.

And here, again, we would be happy to share additional information in a classified setting around what those threats look like and work with you to determine how best to increase transparency on the ways in which 702 is a key protection for the public against foreign threats to the nation, including the security of individual Americans.

MS. FRANKLIN: Thank you. Okay. So the next question is from me. And I'm going to turn to Julian Sanchez. So you spoke in your opening remarks about your concerns about overbroad collection under Section 702, without having any, you know, particularized findings about targets. Some of the changes that some civil society advocates have urged are to narrow that scope of collection by either requiring that targets

be an agent of a foreign power or narrowing the definition of foreign intelligence that can be subject to 702 collection.

We have had some change with regard to the new executive order that President Biden issued in October on enhancing safeguards for United States signals intelligence activities, which specified that all signals intelligence can only be conducted pursuant to a specified list of 12 legitimate objectives.

I'm wondering in this context if you have any particular recommendations you would urge with regard to targeting under Section 702, to address some of the concerns that you made? What specific reforms would you want PCLOB to recommend in this regard?

MR. SANCHEZ: Sure. So to say a couple of things. So, first, yeah, I think insofar as the FISC itself has discussed the foreign intelligence sort of carve-out from the warrant requirement in terms of collection directed at suspected agents of a foreign power, I think that's a disconnect between the sort of parameters of the space in which the executive branch

has a broader authority to act with more limited supervision and the statutory text.

So to the extent that FISC itself has said, you know, the conditions are less stringent in cases involving not surveillance of any international communication, but specifically surveillance targeting agents of foreign power, those parameters should be reflected in the statutory contours. And maybe that in terms of specific authorizations issued by the FISC, that is reflected. But I think, you know, if it's important enough to be part of the parameters of the less stringent requirements for judicial oversight, that ought to be reflected in the statute.

Another thing I'd say is, you know, to the extent that the public pitch for 702 was really initially about, you know, as we all kind of think back and recall, you know, 2005, 2007, 2008, it was really centrally about an issue that had arisen with trends in communications, right? The argument that was made to the public and to Congress was there is a problem with asynchronous Internet communications such that what is fundamentally a foreign to foreign

communication transiting United States looks when you carve it into asynchronous pieces, like two one-end domestic wire communications, right?

The e-mail goes to Google. And then the e-mail goes from Google's somewhere else as part of a separate wire communications. There were instances where FISC judges were treating that essentially as two one-end domestic communications. And we needed a fix for that.

And I agree we needed to fix for that. But the solution we ended up with was significantly broader, where we didn't just say, look, you know, we need to understand what is fundamentally a transiting communication or areas where, you know, we may not know in advance the location of one endpoint of the communication. And what we got instead was a fix that also moved one end domestic communications within the potential ambit of 702 that had traditionally required a more individualized FISA warrant when they were known to be one end domestic wire communication. It's like one thing we can do there is bring, you know, what was intended as a fix to that particular kind of

problem much closer to that and segregate the issue of, you know, genuinely international communications transiting through the U.S. from collection of communications where we have a known U.S. participant or endpoint, ideally, you know, at the collection stage and then certainly in particular at the querying stage when that's not feasible.

MS. FRANKLIN: Thank you. Turning back to Ed Felton.

MR. FELTON: Thank you. My next question is for Jeramie Scott and it relates to Abouts Collection. In your opening statement you mentioned a FISC proceeding raising questions about the boundaries of what constitutes Abouts Collection and thank you for raising that issue for us. But I'd like to ask a question Abouts Collection more generally and in particular given that NSA stopped the Abouts Collection almost 6 years ago now. But NSA has also stated repeatedly that there is value in retaining the option to restart Abouts Collection should conditions change. And given as well that there is a requirement in the current statute to notify -- that NSA notified

Congress before resuming.

I just like to ask what you -- for your opinion on that regime of allowing a restart with notification to Congress. How would you suggest Congress might approach the question of what to do about Abouts Collection in -- as it considers the statute?

MR. SCOTT: Board Member Felton, thank you for the question. I mean, first, I would like to see a permanent ban on Abouts Collection by understanding that, you know, there may be value that I'm not exactly privy to. I would also like to see that if Abouts Collection began again, an automatic trigger for review by the board itself, not just to inform Congress, but an actual look at how this is being implemented and, you know, reviewing of some of the issues we've seen before with Abouts Collection. It's obviously, you know, constitutionally bumps up against or that Abouts Collection bumps up against constitutionality because of its, you know, collection of information incidentally of U.S. persons.

So, I would like to see if that ever happens,

Abouts Collection begin, an automatic review by the PLCOB or another independent oversight entity for that reason, because it poses so many issues with respect to privacy and civil liberties. And to my point that I made earlier in my opening remarks, right now, it would be helpful for the board to review the kind of disagreement that was in that opinion where the (inaudible) actually thought that what was happening, what the NSA was doing, actually triggered the kind of requirements of Congress related to Abouts Collection. And obviously the government disagreed and the FISC ruled in the government's favor. There's obviously a disagreement there that would be helpful for an independent oversight board to look at and make an informed determination on and present some of that information to the public, hopefully.

MR. FELTON: Thank you.

MS. FRANKLIN: Thanks. Okay. So, we're just going to have time to finish out a second round of questions. So, Rich DiZinno, hopefully have a quick question and answer and then we'll conclude this panel.

MR. DiZINNO: Sure. Thank you, Sharon. I guess, I'll turn back to Abouts and ask you, April, again, in terms of at the time that NSA ended the practice of Abouts, NSA made that decision in the midst of some public discussion, although limited in an unclassified fashion some of the complications involved in that decision. My understanding is that those balancing factors included operational difficulty, compliance issues that arose as a result of that operational difficulty and weighing the overall benefit of the intelligence value gain from using that method of collection. Can you talk about that and talk about sort of those countervailing factors that NSA evaluated in making that decision?

MS. DOSS: So, I think you've identified exactly those factors that were taken into consideration. You know, when I mentioned earlier NSA's culture of compliance, we really weave together this commitment to Foreign Intelligence Collection and the commitment to Protection of Privacy and Civil Liberties. And we try to continuously improve our compliance mechanisms and programs. And we try to

take lessons learned from programs where we've had to carefully assess what is the intelligence value and how does that weigh against the risk to privacy and civil liberties. And so the Abouts Collection, as you pointed out, was an instance where in weighing all of those factors. The course of action that was most consistent with all of those values and aims for the government was indeed to cease the Abouts Collection.

So, as we try to -- and we try to take that approach to all of our activities to say from a compliance perspective, what do we have in place in terms of training of people, in terms of policies and processes, in terms of technical compliance measures? When we're looking at any mechanism, any particular approach to implementing 702, we look at how do we weave together the intelligence activity with the compliance activity and where we find that as in the instance of Abouts that the weighing of those factors was proving challenging. We self report that, we work with the Board, with our congressional overseers, we work with DOJ, we work with ODNI, to determine what is the best course forward. So I hope that helps answer

the question.

Again, as has been pointed out, Abouts Collection certainly is paused. We would of course notify the FISC and Congress if there was an intention to resume it and of course we're quite happy to continue having much more detailed conversations with you all at a classified level.

MS. FRANKLIN: Okay. Thank you very much to all of our panelists. Very much appreciate all of your remarks and your answers to our questions. And I'm going to say thank you for joining us.

And we're going to welcome in our second panel. So, if our panelists for the second panel can come on camera. We are, as with the first panel, going to begin with brief opening remarks by each of the panelists. And I'm going to urge you to please be brief, so we can make sure to have time for questions from all of the board members. There are five of us who are all eager to ask you all questions. And we're going to, again, cycle through each board member, asking one question at a time. We're going to reverse the order and I will note who is going to be asking

the next question each time.

So, we're going to hear from our panelists for the opening remarks in alphabetical order.

First we will hear from Cindy Cohn, who's Executive Director of the Electronic Frontier Foundation or EFF. We will next hear from Mike Herrington, Senior Operations Advisor at FBI, then we'll hear from Professor Jeff Kosseff, of the U.S. Naval Academy. And the last speaker for opening remarks will be Professor Jonathan Mayer of Princeton University. So, turning first to Cindy Cohn. Thank you.

MS. COHN: Hi. Thank you very much, the Board, for the opportunity to share EFF's views on Section 702. We want to especially thank the Board for its past work on 702, nearly a decade ago now. It was critical to us as an organization that was struggling hard to get the American people and the judiciary to even understand that the Section -- what became the Section 702 program existed happened. And it was a critical moment in order to bring this program, which, you know, we should all be reminded,

occurred without legal authorization for many years under some semblance of the Rule of Law.

To the end, we hope that the Board can reanimate its role in shedding much needed light on this large and very expensive program, including not just how 702 is being used in practice, what kind of mission creep has occurred from the original antiterrorism justification. I heard strategic competition just now as yet another thing that gets layered on top of what originally was supposed to be narrowly laser focused on stopping terrorism. And how U.S. persons and non-U.S. persons are impacted by it? And especially, I hope, articulating the severe, if not fatal, barriers to real accountability and oversight programs that occur under 702 today, especially in the context of individual is seeking to redress for the way the program has impacted them.

We believe that such an independent articulation is crucial to congressional consideration of whether to renew 702. And if it is to be renewed, any changes to it. Without that there's a very real risk that renewal will be based, once again, on

largely one-sided limited disclosures of information from the obviously self-interested IC. I don't mean that in a way to say that they are wrong, it is their job to try to make sure that these authorities continue, and that they can continue on what they're doing, that's their job. I understand being somebody's lawyer. But that means that there needs to be a third-party that is impartial that can evaluate those claims and not just one sidedness here.

Past experience shows that these kind of disclosures have not been sufficient to give the American public or Congress a clear-eyed view of what's going on. And they shouldn't be -- continue to do this as we head towards renewal, much less protecting the public interest.

Additionally, while there are a lot -- there are many problems with 702 itself, and I will talk about some of those, I really want to urge the Board to consider how governmental secrecy now renders moot many of the accountability and oversight mechanisms for national security surveillance that exist on paper in FISA, as well as in the U.S. Constitution. As the

-- this board is well aware, EFF's highest priorities for the last 2 decades has been ensuring that individuals can seek judicial accountability for violations of their constitutional and statutory rights committed through the government's warrantless foreign intelligence surveillance inside the United States. And we have led to key litigation specifically about 702 surveillance happening versus AT&T, which is about the surveillance that existed before it came under 702 authority, and then 1702 was enacted, Jewel versus NSA, because Congress in its wisdom granted something called Retroactive Immunity to the telephone companies to try to protect them from the rampant legal violations that had occurred prior to Section 702's passage.

I think we have to be honest at this point, that the U.S. has de facto created a national security exception to the U.S. Constitution. And this isn't solely or to me even primarily about legalities. The American people and indeed people all around the world have lost the ability to have a private conversation over digital networks.

702 is a mass monitoring infrastructure that subjects people's communications to NSA review, whenever the internet happens to route their communications through key infrastructure points, mainly on or near the U.S. borders. This impacts, admittedly, millions of Americans and also untold numbers of non-Americans, the numbers of which as you know, we cannot even tell you because they can't even figure it out. But these people are impacted solely because they use the internet in ways that pass through these monitoring stations. This surveillance is suspiciousless and it's warrantless. And any analysis of the NSA's surveillance that starts after collection is missing this critical piece, which I think is important for civil liberties as (inaudible) were just basically understanding what's really going on.

So, regardless of what happens after this and digital monitoring and collection, this is a fundamental change in the rights of all people around the world, including Americans to have a private conversation and should be recognized as neither

necessary nor proportionate under international Human Rights Law. You know, this stretches far beyond the narrow special needs doctrine exception to the Fourth Amendment that we've seen so far in Fourth Amendment Law. I'm happy to go in that more detail, but that will take way longer than 5 minutes.

Additionally, it's now clear that Americans have no avenue to remedy this problem, and that the IC has obfuscated and blocked transparency into its activities such that due process, separation of powers and other core American values are at risk. They're simply not available in the context of the NSA spying. And of course, it's clear that the fruits of this surveillance don't just stay with the NSA, as wonderful as I'm sure those individual people are. The fruits also stretch over to the FBI, which means they are available for prosecution and indeed have been used for prosecution in situations in which, as far as I'm aware, no defendant has ever been given access to the information that went into their prosecution.

So, I want to talk about a few things that I

think this that this Board ought to honestly be honest about and recognize. First, this is mass surveillance, not targeted surveillance. The sheer numbers and admitted mechanisms of upstream removes the basic ability for people to have a private conversation. This is mass surveillance, regardless of how targeted things are once it gets initially collected or reviewed.

Second, let me see if I can move more quickly. Treating the monitoring of traffic as a transit keys infrastructures, if it is the same thing as listening in on Carmela Soprano because the government has targeted her husband, Tony, is simply ridiculous. And it shouldn't be that something that's countenanced by this panel.

Second, robot searching as searching. The IC's central claim is that human eyes are required before Americans are considered to have their rights impacted by what they're doing. Under both the first and the Fourth Amendment, this position must be rejected, robot searching as searching.

Third, judicial reviews of protocols and

their implementation is not the same as actual judicial review of individual cases involving people, whether in civil litigation or criminal defense. And aligning those two things, I think, is a mistake and one that you shouldn't replicate. Just because somebody in a black robe is involved doesn't mean that you have judicial review, as enacted in the constitution and law.

And fourth, given the massive scale of this surveillance, it is not surprising that it simply cannot be done within the boundaries of even the limited accountability measures that Congress is implicated or that the Agency has positioned for itself. In short, surveilling the whole world or even the portion of the whole world whose internet traffic transits the U.S., it's a hard thing to do. That's the reason that there are multiple pages of compliance incidents that were gathered by our friends at the Brennan Center, and that those things are going to continue. This is -- this scale is too hard to do well and we need to recognize in a way that respects people's human rights and I think it's time that we're

honest about that and put on the table, the idea that maybe if something is really this hard, it's not something that we should try to do.

MS. FRANKLIN: Okay. Thank you. I'm going to need to ask you to wrap up there, so.

MS. COHN: Okay. Well, I tried to stay (cross talk).

MS. FRANKLIN: So we have time for questions. Thank you.

MS. COHN: Thank you.

MS. FRANKLIN: Thank you. Okay. Turning next to Mike Herrington for brief opening remarks, please.

MR. HERRINGTON: All right. Thank you. Good afternoon. And thank you, Chair Franklin, and other members of the Board for the opportunity to contribute to this important discussion. As an FBI agent who has investigated cyber national security cases since before FISA Section 702 was created, I've personally used both it and traditional FISA as a case agent in a wide variety of leadership roles. So, I've seen firsthand the value this authority brings to the FBI's

mission to protect the American people and uphold the constitution.

From the FBI's perspective, the primary national security threats to the homeland now reside outside the United States. We must collect outward to protect ourselves inward. And there's no more agile or efficient tool to do so than 702. This agility is particularly important in a technology environment where foreign threat actors can move to new communication accounts and infrastructure in a matter of hours, if not minutes. Section 702's precision lets us home in on only the information necessary and relevant to investigating and countering foreign threats.

To more concretely illustrate its value, let me tell you a few stories about how the FBI uses Section 702 to protect the homeland. In particular, I'd like to focus on the importance of querying Section 702 data for terms related to U.S. persons or USPER queries, a topic which I know has seen a lot of interest recently. While these are hypothetical scenarios, they're closely based on actual cases where

we've used FISA 702 and USPER queries to protect Americans from three of our biggest national security threats.

First, terrorism. The FBI receives a tip that a foreign terrorist organization is targeting a particular U.S. person. So we regularly query Section 702 data for that potential victim's identifiers and in one of those queries, find specific plans to target him through an unwitting associate. Because of those queries, we're able to get both U.S. individual's specific information to protect themselves before the terrorist take action.

Second, counterintelligence. The FBI finds a foreign spy possesses identifiers for dozens of U.S. persons. We query those identifiers against Section 702 data to determine which of those individuals might be actual or potential victims, in need of defensive briefings or other protective measures and which might be accomplices or co-optees in need of further investigation. The queries allow us to efficiently and selectively review foreign communications to answer that question instead of using other possibly

more intrusive, techniques to accomplish the same end.

Third, cyber. A U.S. company suffers a breach and the FBI has a reason to believe it maybe the work of a foreign cyber actor. So, we query identifiers related to the company, including employees whose accounts may have been targeted in the incident. In a situation where every passing minute could mean irreparable damage or loss of data, these queries allow us to quickly determine attribution, identify adversary footholds on the network, and share specific information about the cyber group with the company, allowing them to uncover the full extent of the breach and evict the bad actors.

So, as you can see from these three examples, querying our lawfully acquired and held FISA information is crucial to finding threat intelligence in a targeted and efficient manner, so we can act on it quickly enough to prevent damage before it happens. Now, many of you may be tracking the FBI's compliance challenges related to us for queries of Section 702 data, such as those noted by the Foreign Intelligence Surveillance Court, in its since-declassified November

2020 opinion.

While it's important to note that the Court did not hind unlawful purpose or bad faith, the high rate of non-compliance found by the Court and other oversight bodies over the past couple of years is nevertheless unacceptable. As Director Wray has said publicly, he's "hell bent" on doing whatever it takes to fix our compliance, and that's a feeling all of us in FBI leadership share.

So, what have we done about it? After a hard look at the types of errors that we were seeing, the FBI implemented a series of major reforms throughout 2021 and 2022 to address their root causes. We made changes to our database systems to enhance understanding and compliance, including switching the default setting, so users must affirmatively choose to have their queries run against FISA data. We instituted pre-approval for certain categories of queries, in some cases requiring the Deputy Director of the FBI to personally approve queries before they are run.

We clarified our guidance to the workforce on

query standards and created new, improved and mandatory training on those standards. While initial indications from these reforms are promising, we're committed to continuing to take whatever steps we must take to get it right. To that end, I would highlight one more important reform, the creation of a new Office of Internal Audit solely focused on evaluating our FISA compliance and recommending reforms on an ongoing basis.

Finally, I want to make sure we don't lose sight of the fact, as we contemplate renewal of this important authority, that we will need it not to counter the threats of the last 5 years, but those of the next 5 years and beyond. As foreign terrorist organizations reconstitute and pose a resurgent threat to the homeland, as foreign cyberattacks continue to escalate in sophistication and frequency, and as we enter into an era of heightened strategic competition, the foreign intelligence we depend on Section 702 to collect will become even more crucial to protecting the United States and its interests. And loss of this vital authority would leave us vulnerable to all of

those threats as they grow in intensity over the coming years. Thank you.

MS. FRANKILIN: Thank you. We'll next hear from Jeff Kosseff.

MR. KOSSEFF: Thank you, Chair Franklin and members of the board. Thank you for the opportunity to discuss Section 702. The views that I expressed today are only mine and don't represent the Naval Academy, Department of Navy, Department of Defense or any other party. So, that said, I first want to express my appreciation for the absolutely crucial work that the Board has done over the past decade in gathering information about 702 and clearly explaining to the public how the program works. Such objective narratives are precisely what we need at this time.

So, I began examining 702 in 2015, when my then colleague at the Naval Academy, Chris Inglis, invited me to write a paper with him for a series about 702. I devoted a great deal of time to reviewing public material about how the program operated, including this board's excellent report, as well as the Court opinions that assess the program.

In the 2016 paper, Chris and I concluded that 702 is constitutional and reasonable under the totality of the circumstances based on what we knew from the public record. Now, the public's knowledge of the facts of the 702 program have evolved since 2016. And those facts have challenged me to reconsider whether I personally think that the program is constitutional. While I continue to believe that the program is absolutely essential for national security, and that many of the programs are very well managed to protect privacy, I have very deep concerns about the FBI's access to 702 data and in particular the U.S. person it bear issue.

This started with the October 2018 FISA opinion finding, "The government has reported a large number of FBI queries that were not reasonably likely to return foreign intelligence information or evidence of a crime." The Court noted some instances in which FBI employees and contractors queried 702 data for personal reasons. And the Court found that the querying was unreasonable under the Fourth Amendment and came up with a cure involving documentation.

Now, I questioned whether those changes fully addressed to those concerns, particularly after the December 2019 Court opinion that found, "Widespread violations of varying standard" by the FBI, including queries about people who visited FBI offices for purposes such as performing maintenance. Then we had the November 2020 opinion released to the public in April of 2021, where the FISA Court found additional problems, including the use of information to screen applicants for the FBI Citizens Academy program.

Now, I'm glad to hear today about the 2021 and 2022 reforms, but after these three FISA Court opinions in a row that documented compliance failures, I personally, I'm not prepared to believe all of the problems are fixed. I hope that they are, but I think we need far more information and that's where the Board can help. These problems are particularly concerning to me, in light of last year's disclosure by the DNI that the FBI had conducted up to 3.4 million U.S. person queries in 2021.

Now, that could be overstating the number, but I can just say when I first looked at this program

back in 2015, I never would have imagined it was that many U.S. person queries, and I hope the Board will find more -- gather more information on those numbers. Now all of this raises serious questions about the FBI's ability to self-regulate its access to 702 data under the current governance framework. Now, I'm not one for conspiracy theories about surveillance, I've been more than willing than most people to assume that the FBI and other agencies are properly accessing 702 data.

Nearly 6 years ago, I testified to the House Judiciary Committee that I believed 702 was constitutional and that its national security benefits far outweigh privacy concerns. But at a certain point, we must stop giving the nation's largest law enforcement agency every benefit of the doubt. The FBI cannot play fast and loose with American's most private information, this has to stop now. And if the FBI cannot stop itself, Congress has to stop in -- step in.

Now, the Fourth Amendment is not our only safeguard against government privacy intrusions.

While it provides vital protection, statutes can fill in the gaps if we determine that certain practices are unacceptable. We have the Stored Communications Act and the Wiretap Act. Local governments are restricting law enforcement's use of facial recognition. Given the repeated findings of these compliance problems, Congress should consider imposing more statutory limits on the bureau's ability to query 702 data.

One option would be to require a warrant for the FBI to query 702 information about U.S. persons. Of course, Congress would need to consider the trade-offs in imposing such a requirement. The DNI states that a warrant requirement would -- could hamper the speed and efficiency of operations and I don't trivialize those needs.

I'm sure there are many cases in which easier querying of 702 data would benefit national security. But the question for Congress is not whether warrantless government querying would have some benefits, because of course they would, but whether those benefits outweigh the privacy intrusions of the

warrantless queries. And I don't pretend to have an answer to this difficult policy question, particularly because the amount of public information that we have about 702's operation is limited, with the most valuable data scattered across redacted Court opinions that are publicly released months after they're written. So, as you prepare your next report, I hope that you can help to provide a more complete picture of how the FBI query 702 data and the benefits that 702 provides.

Now, I want to conclude by saying, I don't want my criticism of this aspect of 702 to be seen as a call to allow 702 to expire. 702 is absolutely vital to national security, and we must preserve it. But we must do so in a way that protects our fundamental civil liberties. Thanks for inviting me to speak. And I look forward to your questions.

MS. FRANKILIN: Thank you. And the final panelist to offer a brief opening remark will be Jonathan Mayer.

MR. MAYER: Thank you. Thank you, Chair Franklin, and members of the Privacy and Civil

Liberties Oversight Board for convening this important and timely public forum on Section 702. Section 702 is among the most effective and most contested surveillance authorities available to the U.S. intelligence community and PCLOB is playing a central role as Congress considers reauthorization this year. I offer that view from firsthand experience.

Before joining the Princeton faculty, I served as a staff member in the Senate, where I worked on the Intelligence Committee and Judiciary Committee bills that culminated in the FISA Amendments Reauthorization Act of 2017. That legislation implemented modest reforms and set the current sunset date of December 31, 2023. That most recent reauthorization process was difficult for members and staff. Foreign Intelligence Surveillance is a complex area of statutory and constitutional law, and IC practices are both technically sophisticated and often classified.

As an example, there was a legislative staff briefing on Section 702 in the weeks before reauthorization. We were about 30 minutes in and had

reached the Q&A section. A senior legislative staff member in the senator -- in senator's office who is responsible for advising the members vote on reauthorization, raised their hand and earnestly asked, what's Section 702. So, you have your work cut out for you. I commend the board and staff for taking a fresh look at Section 702 in this year's reauthorization cycle, and for aiming to release the report in the spring.

Should that target date for a formal report slip, I would strongly encourage you to provide whatever substantive input to Congress that you can in the coming months. In the last reauthorization cycle, committee bills form the framework for reauthorization policy debates. Once those base bills were developed, it was difficult to make changes. So, I want to emphasize in the clearest possible terms that for PCLOB to best serve Congress and the American people, you must move quickly.

In the balance of my opening statement, I'd like to emphasize a foundational issue for Section 702. How does the surveillance authority affect

ordinary Americans? When the IC conducts Section 702 surveillance, it incidentally collects communications to or from people in the United States and U.S. persons abroad. These are persons who are not targets of Section 702 surveillance, who could not lawfully be targets of Section 702 surveillance and were otherwise protected by a warrant requirement under FISA and for persons in the United States under the Fourth Amendment of the Constitution.

Current law allows the IC to query this incidentally collected data with the U.S. person identifiers for foreign intelligence and law enforcement purposes. For 15 years, members of Congress on both sides of the aisle and civil society groups from across the political spectrum have repeatedly called on the IC to quantitatively estimate the extent of Section 702 incidental collection. Section 702 also includes a conditional requirement for the IC to estimate incidental collection.

The IC for its part has closely considered this issue and has not identified an estimation method that it finds feasible. As the board wrote in its

2014 report on Section 702, the volume of incidental collection is one of the biggest open questions about the program and a continuing source of public concern. The unknown and potentially large scope of the incidental collection of U.S. persons communications, the Board explained, pushes the program close to the line of constitutional reasonableness. But because of the impasse over estimation methods, lawmakers and the public do not have even a rough estimate of how many communications of U.S. persons are required under Section 702.

I'm here today because I believe there is a possible path forward to resolving that impasse. When I served in the Senate, the DNI noted in a public hearing that the IC would welcome outside technical assistance about how to estimate incidental collection. My research group at Princeton took up the challenge broadly engaging with experts, stakeholders from government, industry and civil society. We spent several years developing a new estimation method. And we published our primary research article this past August.

The project is, to our knowledge, both the only peer reviewed scientific proposal for estimating incident collection and the only detailed alternative to the sampling and manual analysis methods that the IC has consistently declined. I want to specifically acknowledge my co-author (inaudible) and -- well, the views I offer at this public forum are solely my own, the research that I'm describing here is very much a collaborative effort.

The key idea in our proposal is that communication services such as webmail providers and telephone carriers maintain highly accurate country level location data in the ordinary course of business. The IC could match its own dataset about Section 702 collection with these external location datasets, and compute aggregate estimates of incidental collection. Let me briefly touch on why, as I understand the IC's experience, estimating incidental collection is so difficult. An estimation method must protect intelligence sources and methods and must respect privacy and civil liberties. It must comply with the law. It must impose a limited burden

on IC capacity. It must rely on high quality data. It must be transparent and repeatable. It must use cryptography standards approved by the IC. It must account for differences in data formatting. And it must account for change over time. I elaborate on each of these requirements in my prepared statement.

And in short, I believe that our proposal for estimating incidental collection under Section 702 appears to satisfy each and every one of these criteria. While I'm heartened by the earnest response we've received, I also fully acknowledge that taking steps forward will not be easy.

And so, in closing, I'd like to suggest that as the Board moves forward with Section 702 oversight, I encourage you to consider assessing how the IC is implemented and could implement the statutory provision that conditionally requires an estimate of incidental collection. Thank you again for convening this public forum. And I look forward to your questions.

MS. FRANKLIN: Thank you. Okay. So, we're going to reverse the order of the Board members and

questions. So, we'll turn first to Rich DiZinno.

MR. DiZINNO: Thank you, Chair Franklin. And this question is directed to Mr. Herrington. There's been a lot of discussion in this forum and outside of this forum about the compliance issues that FBI has faced with respect to U.S. person queries. These compliance issues are very concerning, especially with respect to the implication for and the impact on the privacy and civil liberties of U.S. citizens. You mentioned some of the changes that the FBI has made to improve privacy and security in your opening statement.

Can you go into a little bit more detail regarding the reforms that had been made? And in particular, can you explain how we, how Congress, how the American people can be reassured that these significant compliance issues will be, if not eliminated, then at least drastically reduced? And then separately, I'd like you to address, please, the impact of additional restrictions on U.S. person queries in the form of a warrant requirement? Meaning, what impact would that have as a process

matter and what impact that would have as an operational matter, in terms of the FBI's ability to do the kinds of things that you described in your opening statement?

MR. HERRINGTON: All right. Thank you, Member DiZinno, for that question. So, it's a lot of important issues and I do think it's worth exploring this issue further than I was able to in my initial remarks. First, let me run down through some more specifics on the reforms that we've implemented. First, you know, we identified several areas where our databases were, you know, not configured in the most advantageous way. And in particular, the one that I noted where we've changed the default, so that in some of our databases that are running against multiple datasets, a user with access to FISA data will no longer have to unselect when they run a query, that it will run against FISA data. In fact, they have to affirmatively select, and in doing so, you know, think about whether that query meets the query standard.

So that is one thing that resulted in a lot of queries that we had had that may have not been

intentionally run against FISA data. And in some -- in many cases, those still met the justification standard, regarding the query standard, but in many cases they did not. And so that resulted in issues of non-compliance. We've also identified two specific areas where we need pre-approval for queries. One is batch queries in 100 or greater terms in one single query. And another is querying, you know, sensitive terms such as those related to, you know, an elected official or a journalist or a member of the press.

In the first case, an attorney must approve that. And that's because just due to the number of terms that are implicated in a batch query. If that justification was not met, then it would have a greater privacy impact. In the second case, I think it's obvious, you know, why we would need preapproval for targets that are for terms that are related to people in particularly sensitive situations, including, you know, some of the concerns about politicization of intelligence tools.

And then the last is one thing that we found is that a lot of the compliance incidents related to

failing to meet the query standard were due to a lack of understanding of what that query standard was, and in fact, you know, due to lack of clarification or communication of that. So, as I said, we clarified that to make sure that it is clear that we are not to be using it in some of the vetting incidents that were cited, you know, in an earlier statement, and unless they affirmatively meet the reasonably likely to retrieve foreign intelligence information or evidence or a crime standard.

And also we have included very concrete examples in that training so that we can better convey that standard to our workforce, and we've also made it a mandatory annual requirement to retain access to the database. So, I would note that, you know, the compliance incidents that have been made public to this date predate all of those changes. So, I would say it is important to, once we start making public the result of oversight that postdate those, that we compare and view the results of those changes, which as I said, are promising, you know, from our perspective, although defer to DOJ and ODNI to provide

more detail on that point.

Finally, on the impact of a warrant requirement. That would depend greatly on the legal standard applied. I'm assuming, based on the discussion here, that what we're talking about is a probable cause standard. Now, you know, I'm not a lawyer, but I know the FISC has repeatedly held that querying data that is lawfully collected and held by the government is not a Fourth Amendment search, although I've heard various views regarding that in the discussion here. But I want to focus more on an operational impact. And I see two major impacts. One is that the process would become so burdensome, that it would really be tantamount to a de facto ban on querying USPER terms against this dataset. And the second one is that it would really prevent us from connecting the dots, and would in fact go towards rebuilding the wall that the 9/11 and Fort Hood Commissions identified in their studies that prevent the effective connecting of the dots and sharing information among agencies.

So, to understand the first point, I'd like

to consider the hypotheticals from my remarks. First, you know, in many cases, we can't wait the weeks or months for the results that would be required to actually seek an order from the FISC. And that could prevent us from, for example, mitigating an ongoing cyber intrusion or preventing a terrorist attack before it happens or could even delay valuable defensive briefings that we're giving to somebody who is being targeted by a foreign spy.

Also, there are some cases, in lot of cases, important cases, we wouldn't really have enough information to meet a probable cause standard. Think about those hypotheticals which represent actual, important use cases. The fact pattern in a lot of them doesn't support a probable cause finding on those specific terms, that would nevertheless be valuable in those situations in part because many of them pertain to actual or potential victims. And also another important point there, if we do have probable cause for a particular USPER term or individual, we would likely be well beyond the point in the investigation where a query would even be valuable or useful. And

instead, we would likely seek a warrant to conduct an actual Fourth Amendment search on the relevant person, account, or et cetera.

At the end of the day, we receive tips about threats and have a responsibility to follow-up on them. Our agents and analysts have a discretion about how they use their time and in doing so and how they can best use their time. So, you know, using -- given -- putting -- imposing this onerous requirement would mean that many more of them would just resort to manual review of the data, instead of seeking an order for a query which they are permitted to do. They can manually review line by line everything in this data. That would be more resource intensive to be sure, which I understand is not a compelling argument to many. But any -- the fact remains that, you know, any agent analyst who is reviewing 702 data line by line is not doing other things to protect Americans. But more importantly, that could have the opposite effect on privacy than is intended by emplacing this requirement.

Manual review, line by line would be less

targeted and selective in reviewing that data. And also, we might have to use other investigative techniques, instead of querying, which might be more intrusive, to answer a question that simple query of 702 data may have been able to answer without going into that more intrusive technique.

MS. FRANKLIN: Thank you. I'm sorry. We do want to get to other board member questions. Just -- it's a very, very important topic, but I do thank you.

MR. HERRINGTON: Yes. Thank you.

MS. FRANKLIN: I'm turning to Ed Felten.

MR. FELTEN: Thanks. My question is also for Mr. Herrington. In your testimony, you gave several examples of querying -- how querying 702 data helped the FBI protect Americans from foreign threat actors. And I couldn't help but notice that in each of your examples, the FBI was querying for U.S. person as a victim or potential victim of a foreign bad actor, rather than querying U.S. persons as potential perpetrators of crime.

So, in light of your examples, is it fair to say that a primary use or primary value for the FBI

mission of Section 702 of U.S. Person queries comes from searches related to potential U.S. victims, rather than perpetrators? And what statutory or procedural safeguards exist to protect the privacy of U.S. persons in this scenario of a search of that U.S. person as a potential victim?

MR. HERRINGTON: Thank you, Member Felten, for that question. So, I did focus my scenarios which, again, are hypothetical scenarios, but based on, you know, actual facts of cases on that because I do think that that is one area that is a very important use of this tool, and one that's particularly important for the FBI in our mission to protect Americans and, you know, notify and warn and protect victims. I -- I'm not sure the word primary would apply there because I don't have statistics as to what proportion of our queries actually apply to actual or potential victims, rather than, you know, actual or potential subjects of an investigation. However, it is very -- it is a very substantial and important purpose for this.

And in terms of protections for U.S. persons

whose terms may be queried as actual or potential victims. You know, there are several layers of civil liberties protections baked into FISA and into Section 702. In particular, you know, in our minimization procedures, our querying procedures, our targeting procedures, and at the end of the day, any of these queries has to meet the query standard, which is reasonably likely to retrieve foreign intelligence information or evidence of a crime.

MS. FRANKLIN: Thank you. All right. So, I get the next question and I'm going to turn to Cindy Cohn, please. So, you spoke a little bit about some of the longstanding lawsuits that EFF has brought and the barriers you face during the state secrets privilege. And one of those, as I understand it, the underlying claim that you have been seeking to litigate, but have not been able to litigate involves upstream collection under Section 702 and how EFF challenges under -- under the Fourth Amendment, that this would violate the Fourth Amendment and raise certain privacy issues. Could you speak to both the -- the legal claim, but also just from a privacy

interests perspective, what risks EFF sees with upstream, even with Abouts Collection suspended? You're on mute. You're on mute.

MS. COHN: Wouldn't be a meeting if I wasn't on mute. Hi. The EFF believes that all people, including Americans, have the right to have a private conversation in the digital age and that it should not be subjected to review, even robot or momentary review by law enforcement without meeting some standard and -- and the intelligence community. I mean, I think that we have to center what we're trying to protect here, which is the ability to have a private conversation and the ability to associate with others without governmental review in the first instance. I think that's what, you know, Mr. Sanchez was talking about when he was talking about general warrants and writs of assistance, but the Fourth Amendment as a whole. I also think that's embedded in our basic privacy law, whether that's the Wiretap Act or otherwise.

So, the risk is that the human right to be able to have a private conversation or privately

associate is something that we all should enjoy, and that it has gone away. Secondary risks include the kinds of things that we've been talking about, about the, you know, the ongoing difficulty of the intelligence community in the FBI specifically to actually even do what they said they were going to be able to do in a very limited way. The worst case scenario is a criminal prosecution of someone that's based upon evidence that they cannot interrogate, which we have seen, you know, courts refuse to really pay attention to, but I think is a serious problem. And the fact that we have on paper, the idea that you should be able to confront your accusers and the evidence arrayed against you, but we have several cases now where that has not actually existed, that we know about, and I suspect untold others that we don't, given some of the techniques that have been uncovered about how law enforcement and national security will hide the use of intelligence collected information for prosecutions. I think that's the worst case scenario is that people are going to jail without being able to confront their accusers and the evidence against them.

As I mentioned, and I've said a couple of times, I think there's also First Amendment implications here. We talk a lot about the Fourth Amendment, and those are important. But we also have a right to associate in this country without being tracked and without our associations being tracked. And that's another issue that EFF has tried to bring up in litigation and has ended up stymied, but a -- but stymied for reasons that don't have to do with the merits of the claim. And I think it's important for us as a society to recognize that the kinds of contact tracing tools and other things that are being deployed and used against U.S. persons have implications for the ability to people to associate as well as for -- for the -- the basic privacy rights.

MS. FRANKLIN: Thank you. Over now to Beth Williams.

MS. WILLIAMS: All right. So, this question is for Mr. Herrington, and thank you to all of our panelists for being here. You know, you mentioned the wall, Mr. Herrington, and that's actually what I was hoping you could talk a little bit more about, because

after September 11th, both the 9/11 Commission, and the Inspector General at the Department of Justice concluded that the wall that had been erected between national security intelligence investigations and criminal cases prevented the sharing of information that two of the terrorist hijackers were in the United States. And as a result, many of the reforms after 9/11 were geared toward more information sharing among the intelligence community.

You talked a little bit about your concerns about this. Can you talk -- can you explain why you're concerned about why certain changes to Section 702 might be rebuilding this wall? And, you know, if those are concerns, is there another way to solve some of the FBI's compliance problems in order to better protect privacy and civil liberties without rebuilding those -- those bureaucratic hoops that prevented us from stopping September 11th?

MR. HERRINGTON: All right. Thank you, Member Williams. It's a great question. I appreciate the -- the opportunity to respond to that. So, I would say, it's important to note here that, you know,

we have already kind of self-imposed, and for good reason, some restrictions on our sharing of information between agencies as it pertains to the Section 702 program specifically. And that is that -- the FBI only receives a relatively small portion of the total 702 collection, I believe it was about 4.4 percent in last year's ASTR that was reported, because we limit our access to that collection to only those targets that are relevant to a full predicated national security investigation, so that we can use this in a more targeted manner to fulfill our mission, which is to protect the Americans or to protect Americans and uphold the Constitution.

So, just referring back to my hypotheticals, I think that's the best way to illustrate the danger of, for example, a warrant requirement, and how that might constitute rebuilding the wall. So, in the first one, like, if a terrorist organization were targeting a particular individual, what if the team who's reviewing that manually, because they don't have the ability to query that, does not know that a subject who is monitored by another field office is

involved in that and that other subject has key information that would help prevent the -- the threat. They would not find that in their manual review of their own select targets that they know to review.

Also in the cyber example, what if we thought it were one particular cyber group that may have done this based on our best guess, but it actually turned out there was another one. And because we didn't query our holdings writ large, we didn't find that information and we're unable to establish attribution. It would be pretty much infeasible to review the totality of our cyber related investigation every time that there's a cyber incident, even if you're only considering those that do meet the query justification. So, those are some of the concerns that we have as constitutes rebuilding the wall.

Now, in terms of what we might accept short of a warrant requirement. I'm not really in a position to get to specific proposals today, but I would echo General Nakasone's remarks by saying that FBI is committed to keeping Section 702 a tool that preserves and protects both national security and

civil liberties and privacy. And we look forward over the coming months to discuss potential reforms that allow us to do both even better.

That being said, I do have a few points to make on the topic. First, as I discussed, we've already implemented significant reforms to our USPER query compliance. And we did that by looking at the areas where the FISC and other external oversight bodies found that we fell short, allowing us to identify the root causes and tailor those reforms specifically to directly address those causes. So, I think there's a few important criteria that we keep -- should keep in mind when evaluating proposals for reforms. The first pertains to that point, is the proposal reform based on analysis of actual shortcomings in the authority and is - is it specifically tailored to fix the root causes. The second, and as we've emphasized in the run up to prior reauthorizations, it's important this authority -- authority remain technology neutral to avoid being made obsolete by new advancements in technology. So, does the proposal reform preserve the authority's

technological neutrality? And third, does the proposed reform preserve the efficacy of this important authority? And does it curtail that efficiency in significant ways?

So, those are some of the questions that we would consider when we're looking at proposed reforms. And we'd certainly be more inclined to support proposals that meet those three criteria. They're guided by analysis of where specifically improvements are needed. They keep Section 702 technology neutral, and they preserve the efficacy of this vital authority.

MS. FRANKLIN: Thank you. Over to Travis LeBlanc.

MR. LeBLANC: I have a question for Professor Mayer. Thank you for joining us today and providing your analysis and proposal on the incidental collection of U.S. person information. You're not only an accomplished academic, but you also have critical experience working in the U.S. Senate, particularly during the last reauthorization. With an eye towards your legislative experience, do you

recommend that Congress clarify its legislation and/or mandate NSA provide an approximate count of U.S. person information? And additionally, do you have other recommendations for 702 reforms that you would encourage the board to propose in its updated Section 702 report?

MR. MAYER: Well, thank you for the question, Board member LeBlanc. I think before getting to the issue of whether statutory changes are needed, with respect to estimating incidental collection, I think it's worth trying without statutory changes. In our analysis of the applicable law for the proposal we have developed, we do not see at this stage legal barriers to implementing the proposal. Those may arise. There may be other barriers that arise. And if that's the case, I would also like to see Congress move on that issue in advance of reauthorization. And I think it would be unfortunate to have another cycle of reauthorization where we don't have access to this important information. So, that would be my hope with respect to estimating incidental collection.

You asked about other aspects of the

reauthorization. And without going into any deliberations from the -- confidential deliberations from the last reauthorization, I would call the board's attention to two provisions that have already come up. One about Abouts Collection and the other about U.S. person queries. There was discussion in the prior panel about the Abouts Collection provision that Congress added to Section 702 in the most recent reauthorization. And the discussion about that provision was largely; one, about legislative procedure. Under the current provision, Congress gets notice about the upcoming resumption of Abouts Collection, and then it's up to Congress what to do about it.

And so in essence what that provision does is it flips the default for how Congress might act on Abouts collection. Instead of Congress having to affirmatively authorize about this collection, you know, the President then signing that bill. In this case, Congress gets noticed, and then it's up to Congress if it wants to essentially opt out of that new form of Abouts Collection. And it's difficult to

see that happening on any quick timeline. And, of course, this is presupposing that the intelligence community has decided to do this and that intelligence community reports to the President. And so we're not talking about a situation which not only Congress would have to pass legislation, declining to allow that Abouts Collection, but actually have to override a veto. So I think that it is difficult to see that provision having much substantive impact. And my recommendation for consideration there would be to just flip the default back the other way. So, if the intelligence community has a proposal for resuming the Abouts Collection, there was nothing stopping the intelligence community from approaching Congress with that proposal and seeking legislation to authorize that proposal.

The other provision, and the last provision I want to touch on is around US person queries. Again, this has come up already today. This is the provision 702 F2, which provided for judicial review of results of certain FBI U.S. person queries. That part of FISA was introduced as a compromise, as an alternative to a

requirement for a warrant to conduct U.S. person queries or to review the results of U.S. person queries. And there was pervasive confusion at the time about the difference between the warrant proposal and this proposal.

And I just want to close by emphasizing how narrow this provision is in ways that I think were -- it is fair to say were not evident to many members of the congressional staff at the time. First, this only applies to queries that are not designed to find and extract foreign intelligence information. It is often the case that there is some foreign intelligence component to U.S. person queries. And second, the query has to be performed in connection with a predicated criminal investigation. That is a particular stage in a criminal investigation. There are other types of queries potentially by the FBI that would not be predicated criminal investigation.

And then last, that investigation has to not relate to national security. And it's almost a little bit tautological to find a query in Section 702 data where there isn't something touching on national

security there. And so, again, there's a lot of confusion among staff about these limiting principles. And I think the Board could do a tremendous service in helping Congress and the public understand those principles. Thank you.

MS. FRANKLIN: Thank you. Okay. We're going to turn back to the top of the order and I'm going to ask my fellow Board members, if we can try to keep our questions concise and our panelists also to please keep answers concise, hopefully, we can make it through the order again. Back to Richard DiZinno.

MR. DiZINNO: Thank you, Chair Franklin. Back to you, Mr. Herrington. You mentioned in your opening statement having experience using, "Traditional FISA as well as using (inaudible) authority as a case agent." In terms of compliance and abuses, we have seen and there has been reference in this form to the Crossfire Hurricane investigation and the DOJ IG report relating to that, those issues that were brought up.

Can you just talk briefly about and describe the differences between Title 1 and the abuses in the

context of Crossfire Hurricane and Title 1/traditional FISA versus Section 702, including very briefly the broad purpose and the difference in purpose of each authority and some of the privacy and civil liberties issues that each authority implicates?

MR. HERRINGTON: Yes, thank you, Member DiZinno. You know, I would say that they're both very important authorities, but are targeted at very different things. I don't want to get too deep into the Crossfire Hurricane case, or the OIG report on that other than to say that we fully accepted their recommendations and have, you know, implemented several reforms based on and responsive to those investigations or those recommendations.

So, Title 1, FISA is, you know, meant to target specifically agents of a foreign power. And so -- and it also has a heavy probable cause requirement to it, as many of you are aware. And that results in a rather long process, particularly when you're talking about situations as in my experience in cyber ones where you are dealing with how to implement collection using a, you know, technologically

sophisticated actors who may -- and also actors who may be moving from account to account very quickly, faster than that we can apply for a FISA Title 1, in some cases.

So, it's a very limited tool in many respects, that 702 provides a great deal more agility and efficiency in targeting those foreign actors who may be, you know, moving more quickly, and therefore, or using many more, you know, using many more accounts. So, it's just a much more efficient and quicker way to do -- to look into those activities, and answer questions that we have about, you know, threats that we're seeing, you know, in a much more quick manner and do, you know, although we definitely use FISA Title 1 to obtain, you know, information that allows us to prevent attacks, just the agility of 702 is valuable in doing that in an even more agile manner.

You know, one thing that I would say about the…the… circling back to the Crossfire Hurricane is that, you know, we are required to provide information to support, a lot of inculpatory information and one

of the failures, there was a failure to include more exculpatory or information that was casting doubt on those findings. And so we've implemented changes to make sure that we are including that information in the future.

MS. FRANKLIN: Thank you. Now to Ed Felten.

MR. FELTEN: Thanks. I have a question for Professor Mayer. First, I want to thank you for your work, for your research on methods for estimating the prevalence of U.S. person information in Section 702 collection. I think it's important to move the debate forward on that issue. And also mindful of your suggestion that there are things that might be done in advance of the reauthorization deadline to provide useful information for Congress on this question.

But I want to ask sort of more generally about this question of estimating U.S. person information. And it seems to me that on this topic, we often let the perfect be the enemy of the good. That is we -- we often and I think sometimes agencies will set a very high bar in terms of the precision of what they're asking for or in terms of minimizing or

requiring absolutely zero encounter of U.S. person information in the process.

So, I guess, I'd like to ask your opinion about this, in particular, you know, are there simple statistical estimation methods involving, which you mentioned, involving manual evaluation of a small sample that would be viable for agencies. And number one -- and number two, to the extent that U.S. person information is indeed very rare in the collected data, isn't it the case that examining a small sample should encounter little or no U.S. person information?

And then finally, to the extent that there's concern about the analysts encountering U.S. person in this information, in the process of an estimation, are there things that could be done by Congress or others to clarify that -- that in the big picture there, it's extremely valuable to understand how -- what the impact is already on U.S. persons and how we could minimize that? So, in general, I'd like your opinion about sort of how to move forward and how we can avoid making the perfect the enemy of the good in this space.

MR. MAYER: Well, thank you for the question, the multi-part question, Board Member Felten. Before getting to that, it occurs to me, I didn't quite give a fulsome answer to Board Member LeBlanc on the 702 F2 provision. And I just wanted to close that out by noting that I would encourage the Board to consider the limitations on 702 F2. And given that they're so significant right now, potentially consider recommending revising those limitations on 702 F2 orders.

With respect to the estimation issue, there are a couple of straightforward methodological directions. One would be for agencies within the intelligence community to attempt estimates based on the data that they hold and based on data that they could obtain, whether through web searches or commercial data providers. Another possible approach would be for companies that receive Section 702 orders to attempt estimates based on the orders that they -- as to the directives that they've received.

Those methods may well be viable. There has clearly been a difference of opinion between the

intelligence community and stakeholders, including members of Congress on both sides of the aisle who have advocated for those types of estimation methods. My own view is that there is a potentially viable path forward there in that the privacy implications, while not insignificant, could be managed through procedures developed by the intelligence community, perhaps with input from PCLOB and Congress. But I recognize that there is a reasonable difference of opinion about those particular directions.

And I would say, the data access issue here is just as significant as the privacy issues. If you're going to estimate incidental collection, you need to be able to match up information about Section 702 collection with where people are located or their nationality. And that's not easy data to come by. And there are some real questions about the commercial data in this space. And so in thinking through the viability of the more straightforward methods, I would encourage the Board to think about that data access issue alongside the privacy implications.

With respect to what the privacy implications

for Americans are, I think it's very difficult to estimate. It may well be that it's a relatively small amount of a sample. And -- and so that would, you know, certainly mitigate privacy concerns around these approaches. But we know that we don't know. So, I'm afraid I sort of can't give more of an answer than that. And that's for managing the privacy impact. As I mentioned, you could imagine very carefully drawing intelligence community procedures around how that analysis is done, how the data is used. Same for any other stakeholders involved in the process and PCLOB and Congress could be involved there.

So, again, on balance, I think there may well be a path forward there. But I take it face value, the IC's reluctance, and they've been very consistent in that reluctance.

MS. FRANKLIN: Thank you. Back to me. I'm going to ask the last question because we're almost at the end. But I want to make sure to ask the question to Professor Kosseff, thank you for joining us and for your patience as we cycled through the other panelists. But I wanted to ask you, you argued that

the significant number of compliance incidents with FBI and the U.S. person queries shows that Congress should consider imposing statutory limits on the FBI's ability to query Section 702 data. Can you elaborate at all on what changes you would recommend for Congress?

MR. KOSSEFF: Well, I think part of that really depends on what you find. I'm fairly open. I think, between the compliance incidents and the number, the up to 3.4 million is what's really stuck with me, that is not something I ever would have imagined years ago. But I think probably the -- it could range from a warrant requirement for queries to, I think, also looking at limiting the purposes for U.S. person queries, and saying you can't do it for criminal investigations. I mean, I think, or there can be disclosure requirements or additional procedural requirements.

My concern about procedural requirements is that we've imposed some, both sort of administratively and legislatively, and they're not working very well, at least from what we know. So, I feel like we need

to figure out something that will make -- will stop this mission creep, frankly.

MS. FRANKLIN: Okay. Well, thank you. Thank you so much. And I want to, again, we are at time, I want to thank all of our panelists for participating today, for sharing your thoughts, for sharing a written opening statement with us, which I believe we will be able to post on our website.

Also for those watching, we will have this available. The recording will be available on our website. So, hopefully additional folks will be able to watch at that time. And thank you again to everybody. This will be very valuable to us as we continue to move forward with our review and preparation of the Board's upcoming Section 702 report to inform the debate over reauthorization.