THE BROOKINGS INSTITUTION

FALK AUDITORIUM

A CONVERSATION WITH ASSISTANT ATTORNEY GENERAL MATTHEW OLSEN ON THE REAUTHORIZATION OF FISA SECTION 702

Washington, D.C.

Tuesday, February 28, 2023

WELCOME:

CAMILLE BUSETTE
Interim Vice President and Director, Governance Studies; Director, Race, Prosperity, and Inclusion Initiative, The Brookings Institution

OPENING REMARKS:

MATTHEW G. OLSEN
Assistant Attorney General for National Security, The United States Department of Justice

FIRESIDE CHAT:

BENJAMIN WITTES (Moderator)
Senior Fellow, Governance Studies, The Brookings Institution; Editor-in-Chief, Lawfare

MATTHEW G. OLSEN
Assistant Attorney General for National Security, The United States Department of Justice

* * * * *

Camille Busette: Good morning. I'm Camille Busette, the interim vice president for governance studies here at Brookings, and I am delighted to welcome you to a conversation with Assistant Attorney General Matt Olsen on the reauthorization of Section 702 of the Foreign Intelligence Surveillance Act, otherwise known as FISA. Thank you for joining us in-person and virtually. As usual, a huge thank you to our AV, events and security colleagues here at Brookings. For today's event, we will first hear from Assistant Attorney General Matt Olsen, and then he will be joined for a conversation by my colleague, senior fellow Ben Wittes. Audience Q&A will follow.

You might be wondering why we are having a conversation about Section 702 of the FISA Act. Section 702 is a key provision of the Foreign Intelligence Surveillance Amendments Act of 2008 that permits the government to conduct targeted surveillance of foreign persons located outside the United States with a compelled assistance of electronic communications for providers to acquire foreign intelligence information. The government uses the information collected under Section 702 to protect the United States and its allies from hostile foreign adversaries, including terrorists, proliferators and spies, and to inform cybersecurity efforts.

Section 702 of the Foreign Intelligence Surveillance Act is set to expire on December 31st. This is this is one of the main legal engines of US intelligence collection, and its potential expiration is, for many in the intelligence community, a five-alarm fire akin to the debt ceiling crisis. Within, with an ongoing war in Europe and Chinese surveillance balloons floating around, you have recent examples of why intelligence collection is very much part of the national dialogue today.

However, the politics of reauthorization are complicated; while Congress has reauthorized Section 702 twice before since its original passage, we are, as you know, in an age of deep polarization. Congressional Republicans have become skeptical of the government's administration of FISA as a result of the Russia investigation and the perceived misuse of FISA to obtain information on President Trump. In addition, Section 702 has also always had a liberal and civil, civil libertarian detractors who see it as authorizing mass surveillance and believe the program allows for backdoor searches of Americans without a normal warrant.

So with that background, it gives me great pleasure to introduce Assistant Attorney General Matt Olsen. Matt Olsen is the assistant attorney general for national security. In that capacity, he leads the Department of Justice's mission to combat terrorism, espionage, cybercrime and other threats to the national security. From 2011 to 2014, Olson served as the director of the National

Counterterrorism Center and prior to leading the National Terror Counterterrorism Center, Olsen was a general counsel for the National Security Agency. For eighteen years, Olsen worked at the Department of Justice as a career attorney and in a number of leadership positions. He served as an associate deputy attorney general for national security and was special counsel to the attorney general. In 2006, Olsen helped establish the National Security Division and served as the first career deputy assistant attorney general for national security. Please join me in welcoming Assistant Attorney General Matt Olsen.

Matthew Olsen: Thank you. Thank you very much. All right. Thank you very much, Camille, and good morning to everybody. Thanks especially to Brookings for hosting me today and to my friend Ben Wittes for organizing this event. I'm looking forward to what I know is going to be a lively discussion. I know that we have a number of folks here and we have a number of folks online joining.

So, look, as many of you know, the National Security Division, which I lead at the Justice Department, was created in the wake of 9/11. It was created to unify all of the Department of Justice's national security efforts. We investigate spies and terrorists. We go after nation state threats, those who would bring malign foreign influence to the United States. We enforce sanctions and export control laws and much more. But the national security division is also responsible for the Foreign Intelligence Surveillance Act. We are the lawyers who represent the government before the Foreign Intelligence Surveillance Court or FISA court, and we oversee the use of FISA authorities. I've been on this job leading the national security division for just about a year, and I've worked in the national security field, as we just heard from Camille for much of my career.

People often ask me what keeps me up at night, and that's usually a hard question to answer. We have so many threats that we face from nation state adversaries, terrorists, malicious cyber actors, it's hard to pinpoint just one threat. But right now, I can say without hesitation the answer to that question, what keeps me up at night is thinking about what's going to happen if we do not renew Section 702 of the Foreign Intelligence Surveillance Act. This law will expire at the end of this year if Congress doesn't act to reauthorize it. And if 702 expires or is watered down, the United States will lose absolutely critical insights that we need to protect the country.

Let me back up a little bit. Section 702 is the law that enables the United States government to obtain intelligence by targeting non-Americans who are overseas and who are using US-based communications services. Its value simply cannot be overstated. Without 702, we will lose

indispensable intelligence for our decision makers and our war fighters, as well as those of our allies. And we have no fallback authority. We have nothing to go back to that would even come close to making up for that loss.

So that's why this morning, the attorney general and the director of national intelligence sent a letter urging Congress to swiftly reauthorize 702. And in that letter, they emphasized that there is simply no way to replicate 702's speed, agility, reliability and insights. Section 702 enables the United States to gain intelligence about our most, our most pressing threats. Today, we are relentlessly focused on serious threats, such as the Chinese government's efforts to spy on us and to steal our sensitive technologies; Iran's sanctions evasions; North Korea's nuclear program, and Russia's invasion of Ukraine.

Let me stress the threat we face from China in particular. At this moment when China is ramping up its efforts to spy on Americans, we should not, we must not blind ourselves to that threat by allowing 702 to expire. The bottom line is that Section 702 gives the intelligence, it gives us the intelligence that's necessary for us to stay one step ahead of our adversaries, and we cannot afford to let it lapse. So it is time to sound the alarm. We must act with urgency and that is why I am here today.

So a little bit of background. Both the intelligence and law enforcement communities need to partner with Congress on this. And we must make the case to the American people directly. So I see the urgency of this moment from my current position in the Justice Department. But I also recognize the critical value of 702 from working for over two decades in national security, that includes as a lawyer in the Justice Department and the FBI. Shortly after 9/11, I saw how the statutory framework that was in place at the time couldn't keep pace with the evolving threats and evolving technologies.

When I first came to the national security division when it was created in 2006, I was part of the team that helped craft 702, which was first passed in 2008. I then went on to become the general counsel of the National Security Agency, where I oversaw how NSA implemented the statute. I saw in practice both the power of the statute as a collection tool and the rigor of the oversight procedures that were built into it. Then as my time as the director of the National Counterterrorism Center, I was a consumer. I received the intelligence from 702, and almost every day it provided insights that supported our ability to combat terrorism. So historically, 702 has faced sunset twice in the past ten years, and both times Congress voted to reauthorize it, both times with strong bipartisan majorities.

So while now 702 is more essential than ever before, that broad bipartisan consensus that supporting it has supported it in the past has frayed in recent years. If we are going to preserve this vital tool, it is incumbent on us in the executive branch to do more than just to demonstrate that 702 is immensely important to national security. We also must earn and sustain the trust of the American people and of Congress. And we, we have to demonstrate how the intelligence and law enforcement communities are striving to uphold the confidence that has been placed in us. All right.

So the good news is that it at its very core, FISA's privacy and oversight framework is designed to do exactly that, to sustain public confidence through rigorous and regular scrutiny by all three branches of government. Going back a little bit. Historically, FISA was created to constrain government surveillance activity in response to concerns about surveillance abuses. When Congress enacted the original FISA in 1978, in response to the landmark Church Committee report, it marked the first time that the government surveillance for foreign intelligence was subject to affirmative judicial review. This was unprecedented, not just in the United States, but anywhere in the world. And in the 45 years since it was enacted, FISA has proven to be remarkably durable. Its basic structure has effectively balanced operational needs with requirements to obtain court authorization and congressional approval. And when necessary, Congress has amended the law to account for changes in technology and to enhance privacy and oversight.

So Section 702, now moving forward a bit, 702 was the product of just one such amendment. When FISA was originally passed— I want to talk a little bit about why it was, why we adopted Section 702— when FISA was originally passed, Congress intended for the law to regulate surveillance activities conducted within the United States. But with the advent of the Internet and as the technology supporting international communications evolved, FISA’s very terms required the government to seek individualized court orders and to do so even when the target of the collection was a foreign person based overseas. And this situation became increasingly untenable in the aftermath of 9/11 as we ramped up our efforts to dismantle al Qaeda and disrupt foreign terrorist threats. And I saw this firsthand as an official in the newly created National Security Division.

So let me be a little more specific. Here was the problem. NSA would be tracking a possible terrorist located overseas, not a U.S. citizen, not someone located in the United States. But that person also happened to be using a U.S. based e-mail service provider. And because that provider was in the United States, traditional FISA requirements, the definitions in FISA meant that we had to

establish probable cause that the possible terrorist was an agent of a foreign power before we could get access to those communications.

And this just wasn't operationally feasible. Often, we couldn't, we didn't know enough about the overseas individual to make that kind of a showing. And even in cases where we could get enough information, the process of obtaining individual court orders, pulling that information together, applying to the FISA court in every instance took too long and it often required months of effort. It's simply not something that we could do at operational speed, let alone at the speed required to disrupt a cyber-attack. It's not what Congress had intended. And this arrangement actually made no sense as a constitutional matter.

Probable cause, as you guys know, is a standard that protects the rights of Americans and others inside this country. The Supreme Court has long held that the Fourth Amendment does not apply to non-U.S. persons who are outside the United States. So we needed to update FISA to reflect this legal and technological reality and the nature of the threats that we face while still protecting the rights of Americans, and Section 702, Section 702 was the solution to that problem. And here's the key point. 702 only, it only authorizes intelligence collection targeting non-U.S. persons who are outside the United States, and in such cases, the law provides the legal framework for the government to compel the assistance of U.S. electronic communications service providers.

So Section 702 strikes an important balance. The government is not required to obtain court orders for each target, not required to obtain individual court orders. But— and this is critical— the program is subject to judicial oversight and approval. So the FISA court approves and ensures that the collection under 702 is reasonably designed to target only non-U.S. persons overseas, that the program is tailored for specific intelligence needs and that it is consistent with the Constitution, the Fourth Amendment in particular. And in fact, every court, every court, including the FISA court that has looked at 702 over the years, has found it to be constitutional. And there are strict limits on handling any information that is incidentally collected about U.S. persons. So it targets people overseas, but it can collect information about U.S. persons incidentally.

Section 702 prohibits on its terms the intentional collection of U.S. persons communications. But U.S. person information can be incidentally collected in a few ways. One is when a foreign target overseas is in touch with a person in, a U.S. person in the United States. Second, when say two foreign persons overseas, one of whom is a target, discuss a U.S. person during their

communications. So these are a couple of ways in which U.S. person information can be incidentally collected.

So this overall framework has worked remarkably well over the past years. And in the 15 years since its enactment, Section 702 has become what I think is the intelligence community's most valuable national security legal tool, its most valuable tool. And we must retain it to confront the evolving threats that we're facing in the years ahead. So let me pause here and, and offer a couple of hypothetical scenarios in which 702 could prove crucial to put some specifics on the table.

Suppose the FBI gets information that an individual overseas, someone overseas appears to be recruiting employees of a U.S. semiconductor company, possibly for the purpose of gaining access to sensitive U.S. technology for military purposes. An analyst at the FBI with that information could target that overseas individual's e-mail under 702. And this would help us figure out what technology they may be seeking to take, whether it might be used to advance that country's military. That's one example.

A second is, suppose a foreign partner tells us that an overseas individual is attempting to sell weapons to a rogue nation that's under U.S. sanctions. We get that information from a foreign intelligence partner. Under 702, we could move quickly to acquire that overseas individual's communications to gather more intelligence about his or her activities, who that person is dealing with, even, even if there was not probable cause to believe that that person was acting as an agent of a foreign power.

A third hypothetical. Suppose a foreign partner captures a terrorist on the battlefield. Not an uncommon scenario. That person who's captured on the battlefield has a phone. And our foreign partner gets a list of e-mail contacts from that terrorist's phone. With that information, with that list of email address, addresses, intelligence analysts here, our intelligence analysts could use 702 to gain insights about other people that terrorist is in contact with, understand that network, and that would help us disrupt ongoing or future plots.

So in each example that I've just offered, 702 would provide critical insights early at the early stages of an investigation, and we could then follow up, follow leads and get more information. And here's a key. In each example, it would be either impractical or actually quite impossible to seek an individualized court order based on probable cause. So those are hypothetical examples. Now, let me give you some real-world examples. Famously, in, Section 702 was used to foil a plot in 2009, an

active plot to bomb the New York subway. NSA analysts relied on 702 to target an email address used by a suspected al Qaeda courier in Pakistan, and they discovered a message that was sent by someone in the United States seeking information about how to make explosives. The FBI identified that person in the United States from 702 as Najibullah Zazi and was able to disrupt his plot in time to save possibly countless lives.

And then moving forward just this past summer, 702 collection contributed to the successful operation against Ayman al-Zawahiri, who had served as al Qaeda's leader since Osama bin Laden's death. 702 has also played a key role in countering threats from China, as well as other countries, Russia, Iran, North Korea. We've used it to identify and disrupt hostile foreign actors' efforts to recruit spies in this country or to send operatives into the United States. And we've relied on 702 to mitigate and prevent foreign ransomware and other cyber-attacks on U.S. critical infrastructure. We've also used Section 702 to get information on efforts to evade U.S. sanctions, enabling us to prevent components of weapons of mass destruction from reaching foreign actors and our adversaries.

So those are actual real examples of the ways 702 has been used recently and in the past. In short, 702 is a tremendously powerful tool which makes it all the more critical that we maintain the trust and the confidence of Congress and the American people. And that's the challenge that we face today. So how do we do that? How do we maintain that trust? Well, we build trust through judicial and congressional oversight, as well as through our own oversight and accountability procedures within the executive branch. And we do it as well by being as transparent as we can possibly be about how the law is used and when we make mistakes.

Agencies that use Section 702 have internal compliance procedures. DOJ and the Office of the Director of National Intelligence conduct independent oversight to assess a number of things, collection decisions, they review queries, they examine the dissemination of Section 702 information or intelligence that may contain U.S. personnel information, and they address incidents of noncompliance so that we don't repeat them. In fact, the oversight attorneys in the National Security Division, which I lead, review every single targeting decision that's made, 100% of them. Still, in recent years, DOJ and ODNI have found serious compliance issues with FBI's queries of FISA collection for information about U.S. persons. And these problems were reported to the FISA court and to Congress and the court had described, has described them in public opinions.

And I want to spend a few minutes talking about those issues right now. Look. Every compliance incident matters, of course, but incidents that involve U.S. person information are especially troubling and especially damaging to public trust. Congress authorized the government, it authorized us to collect foreign intelligence under 702 obtaining individuals, without obtaining individual court orders, without individual court orders, because 702 targets our non-U.S. persons outside the United States. And we've used this tool to collect intelligence because of the need to protect national security. But we still need strong guardrails when intelligence agencies review this data for information about Americans. We need those guardrails.

To be clear, it is critically important that the government is able to review the data that it collects, to query the data. When we examine 702 information using a query term with a name of a U.S. person, for example, we are trying to identify in certain cases, U.S. victims of foreign hacking or spying. And that's what lets us warn and protect those individuals. If we're trying to keep Americans, protect if we, if we were to keep Americans from, if we were to keep protecting Americans from escalating cyber and espionage threats, we need to maintain the capacity to, capacity to conduct U.S. person queries.

So this is especially true for the FBI, which is responsible for protecting the homeland from national security threats emanating from overseas. So the Zazi example that I mentioned a few minutes ago shows how important it is that we are able to connect the dots between foreign-based threats, those emanating overseas and individuals in the United States. Look, this was a key lesson of 9/11 and we simply can't forget it. So let me now offer a couple of hypotheticals, focusing on the querying of U.S. person identifiers.

Here's one. Suppose a Chinese citizen overseas is suspected, based on intelligence reporting, of plotting to assault dissidents living in the United States, dissidents who are speaking out against the PRC government. The investigation may reveal that the Chinese citizen is in frequent contact with a person and associate inside the United States. At this very early stage of an investigation, FBI analysts are quite likely to want to query the 702 databases, the information we have that's been collected under Section 702, data that's been lawfully collected using the name of this U.S. based person.

Another example. Suppose the FBI learns that a foreign actor has hacked into an American energy company and exfiltrated data. The FBI again, quite likely is going to want to immediately query

its Section 702 holdings using that company's name or other U.S. person information to figure out a number of things, the scope of the breach. What happened to the data? Whether there were other U.S. victims. These are all logical and lawful investigative steps. They also directly implicate the rights of Americans, so we need to be exceptionally careful. And unfortunately, unfortunately, in this highly sensitive area, we've made mistakes in recent years that have undermined that core public trust.

Now, many of these mistakes resulted from misunderstandings by FBI personnel about the rules that govern how you conduct a U.S. person query and in other instances, personnel, FBI personnel queried FISA information inadvertently without realizing that the 702 data sets were included in the query as a default. And understanding that context is, context is very important as we look to fix these issues. But at the end of the day, the mistakes are not acceptable. They aren't acceptable to us, they're not acceptable to Congress, they're not acceptable to the American people, and they shouldn't be. So we've known we've had work to do, and we've implemented key reforms to address these errors.

One is that we've changed the default settings. We've changed the default settings in FBI systems so that you have to affirmatively opt in to query 702 information. It's changed so now it requires an affirmative step to opt in to search using an, a U.S. person query. We've also required FBI personnel to record specific written justifications before they access 702 information using a U.S. person query. We've also imposed pre-approval requirements for certain types of sensitive U.S. person queries or large, large-scale questions. And we've improved guidance and training for all FBI personnel. And this is important. We are already seeing concrete improvements as a result of these efforts.

There's been a dramatic decrease, a dramatic decrease in the total number of U.S. person queries since the FBI adopted these reforms in 2021, along with a significant reduction in the number of inadvertent queries of the Section 702 databases. And we've made these changes. We've made these advances without undermining the fundamental value of Section 702. But I want to be clear. This is about more than just imposing a checklist of new requirements. Our fundamental task is to ensure that we are building a culture of compliance, a culture that recognizes the harm that's caused by even the smallest mistake.

So, look, there are going to be mistakes. Any, any program as complicated as this that involves human beings who are trying to work on tremendously difficult systems under time pressure,

we are going to make mistakes. But the reality is that every mistake undermines public trust and confidence in how we use these tools. So here's the key point for me. All of us in these jobs, we need to recognize that the American people are entrusting us with the immense responsibilities of keeping them safe and protecting their liberties. I feel honored by that. I feel the weight of that responsibility. And I know my colleagues in the FBI and across the intelligence community approach their jobs in exactly the same way.

Just as we are determined to protect the American people and to defend our Constitution, so too, are we determined to be worthy of the trust that's placed in us every day. The stakes are incredibly high. Repressive authoritarian regimes like China and Russia, Iran, North Korea, they pose a range of threats to our countries and to our allies, while terrorist groups continue to plot violent attacks in secret. And these are not just threats to our, our safety and security. They are threats to our freedoms, they are threats to our democracy, and they are threats to our fundamental American values here and around the world.

So it's against this backdrop that renewing 702 is a national security imperative. It is a national security imperative. That's really beyond dispute. And going forward this year, we share that responsibility with Congress to preserve it. This requires us in the executive branch to be strong partners with Congress and to be as transparent as we can possibly be with the American people, welcoming hard questions, being open and candid about the mistakes we make, even when we're relentlessly focused on trying to fix them and fundamentally fulfilling our role as stewards of this public trust. This is what the American people expect and it's what they deserve. So thank you for being here today. Ben, I look forward to answering your, answering your questions and the questions of others. Thank you very much.

Benjamin Wittes: Is this live? Yes, it is. So I would like to cover three broad areas today. The first is the importance of 702 and the range of uses of 702, the second is the compliance issues and that you referred to and the matters that are, are addressable and not addressable. And the third is the politics of reauthorization. So let's start with the, with the importance of the program. We used to talk about this program almost exclusively in counterterrorism terms. Today, the national security adviser issued a statement that while I don't have the exact words of it in front of me, make clear that this is a pivotal authority with respect to collection against both China and Russia.

So I want to start with the question of, you know, how much is this a counterterrorism authority versus a general collection authority that has application to great power conflict?

Matthew Olsen: So that is a really good insight, and I think it reflects, the answer's reflected in the statement that came from the White House today by the national security adviser, as well as the letter that was released this morning from the attorney general and the director of national intelligence. So, look, the short answer is when, when Section 702 was passed in 2008, we were you know, we were focused on al Qaeda and our counterterrorism efforts. And the central goal of Section 702 was really focused on those threats.

Today, we face a much different threat environment that is and certainly does include our, you know, terrorism challenges. But it is as much or maybe more focus now in terms of the threats we face on a number of nation state adversaries and the usual list, North Korea, Iran, Russia, and particularly China. So that, the good news, I think, is that Section 702 was agnostic as to threats when it was adopted, and it has proven to be extraordinarily valuable now, today in addressing the wide range of threats we face, because it does focus simply on those who are overseas, who are not U.S. persons, who may have foreign intelligence information.

So, so it has proven to be effective across the board on the range of threats that we face today. And in fact, going forward, as we can't necessarily sit here today and predict what we're going to be thinking about five years from now when we're sitting in these chairs, but it is built to be adapted to those threats in the future, because it includes, crucially, the speed and agility to move against these various threats.

Benjamin Wittes: So I think it was during the last reauthorization the government put out the, I thought, remarkable fact that 702 was the single largest contributor to the president's daily brief, which certainly I found arresting at the time, and I remember it so much. Is that still true? I mean, when we think about presidential decision making, is it fair to say that 702 accounts for not necessarily the majority of the information that's presented to him, but a plurality of it with respect to other legal authorizations?

Matthew Olsen: So it, I sit every morning with the attorney general and the director of the FBI and receive the briefing that is, you know, akin to the PDB, includes the PDB. And it is clear to me from that briefing that Section 702 is, plays a substantial role and contributes significantly to the intelligence that leaders around the community, including the president, receive every day, whether

it's the most important or most significant, I think it's hard to measure that, that exactly. But it certainly is, it is a critical one. And it strikes me, having served in a number of different roles, that there's no more important legal tool for the collection of critical intelligence.

Benjamin Wittes: So when we distinguish here between legal tools and, and other tools, I assume the distinction that you're making is that when, when we collect, based on General 12-333 authorities, they're not attributed to a specific law, right. But when you collect under 702, you're, you actually have to invoke 702 to do it. Is that the distinction that you're making?

Matthew Olsen: That's the distinction that I make. Now, I think that's a lawyer's way of thinking, but it's certainly the case that when it comes to surveillance collection, 12-333 is the basic backdrop of the president's authority. Section 702 is a statutory authority that must be invoked, as you say, in order to rely on it. But then there's obviously a number of, you know, the broad range of ways in which the intelligence community collects information, whether it's through human sources or by sharing from other services.

So when I say it, the most important legal tool is because I see it just about every day, I see the collection being used and we are a part of that in the Justice Department. But I see it both being invoked but also contributing to finished intelligence products that are, you know, critical to our understanding of the nature of the threats we face.

Benjamin Wittes: All right. So I want to ask about some specific state actor collection. And I want to work off of some of the hypotheticals that you used. With respect to China in particular, there have been a number of substantial cybersecurity events that the intelligence community has responded to. Major incidents, major investigations. My assumption is that you are saying to us that 702 is central to those operations. Is that fair?

Matthew Olsen: Yeah, I'll be just direct. Absolutely. Section 702 is critical to our ability to understand the nature of the cyber-attacks that we face on a consistent basis from nation states, whether that's China, Russia, Iran, 702 is one of the key ways that we understand the types of threats we face.

Benjamin Wittes: And with respect to China in particular, is it fair to say and so the examples that you used, you involved threats to U.S. intellectual property and technology theft. I assume that was not an accident, that that's the hypothetical that you use because there you have, you have a US-based actor, you have a foreign actor that's attacking that actor, that's, and you often have data being

stored in the United States. So these are going to be tricky to collect without recourse to something that lets you get domestic data.

Matthew Olsen: That's exactly right. So if you imagine a cyber-attack emanating out of China that attacks a U.S. company, for example, whether it's for espionage or for, or for, for a destructive purpose, right. The, what you, the elements of Section 702 are, are it's important understand how 702 works to understand why it's so, what's so useful in that scenario, whether it's China or another country. One is that the attack emanates from overseas, two, that the, the victim is in the United States and three, it's often the case that US-based communication service providers withhold information that would be useful or critical in understanding the nature of that threat. And Section 702 is this single tool that allows us to get access to that. Without Section 702, we simply don't have a means to collect information, certainly not at the speed of a cyber-attack that would allow us to understand it and potentially mitigate it in time.

Benjamin Wittes: All right. The second, second country that Jake Sullivan mentioned this morning was Russia. We have had a major, major set of intelligence successes vis a vis Russia. All I think involving signals intelligence, which is in the run up to the Ukraine invasion, and after the Ukraine invasion, just based on the newspapers, we seem to know a lot about Russian intention and that seems to have played a substantial role in the behavior of the president of the United States who went out and said the Ukraine invasion is going to happen, it's going to happen imminently, you know, and put the prestige of the United States on the line. Without asking you to comment on any specific intelligence or operation, is it fair to say that that set of state, that that presidential behavior might have been different in the absence of 702, that the quality of the information he received might have been different?

Matthew Olsen: So I'm going to answer quite generally. Again, sort of falling back into the way Section 702 works, which is it does provide us with this unique capability to target individuals overseas on our key set of threats. And of course, among the threats that we are concerned about, as I mentioned, not only terrorism but Russia and Russia's invasion in Ukraine. And look, I, I said in my remarks, we need to be as transparent as possible, but we also have to be cautious about the things I talk about, we talk about in how Section 702 is used.

You know, as, as we lean in to be transparent, we can't topple over the guardrails that disclose sensitive information. So we have to be cautious. And so my answer is a little opaque on that

one, Ben. But I think it's important to basically step back and understand we're talking about spies, hackers and terrorists. And when we don't have Section 702 to go after those groups, those individuals, we blind ourselves and unilaterally would blind ourselves to those key threats.

Benjamin Wittes: All right. So let me, I'm not going to push back hard on this, this, but I am going to push back a little bit. Two Russian commanders are texting with each other on Telegram, which does not transit the United States, as I understand it seems to me 702 has little to say about that. But if the same two Russian commanders were to use some other platform, that data would transit the United States, 702 may have a lot to say about it. Is that fair as a matter, just as a matter of characterizing the law?

Matthew Olsen: I think as a matter of characterizing the law, it's fair to say that the scenario where you have a foreign actor overseas, again, whether that's somebody in Russia, somebody in China, somebody in Iran, and they are using a US-based service provider to communicate and whether they're communicating with another member of their group, another associate, you know, another member of their government or somebody in the United States, if they're using U.S. service providers, Section 702 is the unique law that gives us the ability to, to gain that intelligence.

Benjamin Wittes: All right. One more important before I kind of move on to the, the, the problems. On cybersecurity, a huge amount transits the United States just because so many of the service providers are American providers or are interfacing, excuse me, regularly with American providers. Is it reasonable to say that the cybersecurity arena is particularly vulnerable to a lapse in 702, or are, or are all of these different areas kind of equally vulnerable?

Matthew Olsen: I think it's, I think it's fair to focus on the, on this, the nature of the cyber threats we face that come from other nation states as a, as a critical part of the overall value of 702. One of the reasons I say that is what Section 702 provides— and it has been an argument for 702 since its inception— is speed and agility, the ability to move from one, you know, one target to another, to do so very quickly, to do so at an early stage in an investigation. We may not know a lot of information, but we know enough to know that there's a threat that's coming from another country, it's coming into the United States and it's using U.S. infrastructure or US service providers to, to, to enable that threat.

And really, the cyber example is a very good one, because in some ways, if you think about Section 702, it is fit for purpose for that type of threat. You know, the argument was made in the

context of terrorism because we were focused on one terrorism target communicating with another or potentially communicating with somebody in the United States, overseas. And it was also important there to have that speed and agility. But now sort of, you know, an order of magnitude more significant is the, the speed of cyber-attacks and understanding how those can, the need to be fast and agile in how to respond is even more important, I think, in that context. And I think that's why the argument for 702 is very strong here.

Benjamin Wittes: So a skeptic would respond to all of this by saying, okay, fair enough, 702 produces a whole lot, but you know, it only dates from 2009 and the United States had pretty robust collection against terrorists and foreign target, foreign state actors before 2009. So just as the government always overstates the importance of the, the thing that it wants Congress to do, there's a kind of an overstatement going on here, the world wouldn't end if we returned to 2008 in collection. And so I just want to posit simply, why is that wrong?

Matthew Olsen: So that's fundamentally wrong. In 2008 and, and post-2001, we were losing insights. And we were losing insights for the crucial reason that the way communications worked had changed so that we were under, for surveillance purposes, under FISA, we were having to get individual court orders for non-U.S. persons overseas because they were using US-based service providers, providers and FISA required us to get individual court orders. So our insights were going down during that time frame.

It was only after the passage of, of 702 that we reformed FISA, modernized it in order to respond to the changes in technology that have allowed us to keep up with those threats. So it is, it is a basic misunderstanding of how FISA works, but also how technology has changed to assert that we could just go back to, you know, pre-2008 or pre-9/11 time period and do just as well. I mean, it's not even close. We would literally be blinding ourselves to some of the most crucial threats we face if we were to allow this law to lapse.

Benjamin Wittes: So just to push from the point of view of the same skeptic, you know, you guys, I was up here with, with Jim Comey when he was, said the FBI was going to go dark and, and, and, you know, it didn't really happen or maybe it did happen, and the world went on. And now, you know, you said we're going to go blind. And so the skeptic will say, oh, I've heard this before. I'm not, I, I'm, I'm much less worried about it than, than Matt Olsen is and, you know, is, you know, on a, on a kind of 1 to 100 scale of dire, how dire is this?

Matthew Olsen: You know, I think it is very dire. And that's why I said I want to sound the alarm. And it's not just me, right? It's the attorney general and the DNI. It's Avril Haines and Merrick Garland, and it's the national security adviser today making the case for the importance of reauthorizing Section 702 saying that it is an urgent imperative for our national security and being willing to talk more about the ways in which it's used. For example, disclosing the fact that 702 was part of the information that we had that allowed us to carry out the operation against Ayman al-Zawahiri, the leader of Al Qaeda, and then explaining a number of other ways in which it is used, whether it's cyber-attacks or foreign espionage.

So, you know, the number of, of, it's in some ways hard to quantify that, whether it's on a 0 to 100 scale or not. But I can tell you from my own career, going back to my time at the FBI in the mid-2000s to today, I have seen the way in which 702 has become increasingly important. Increasingly, the tool that enables us to collect information that we have no other way of getting. And that's why I use the term that we would be blinding ourselves to some of the key threats that we face.

Benjamin Wittes: All right. So I want to turn to the sort of problems of the, of the program. And, you know, one of the oddities of this program is that you stress how important it is, and I share your alarm at the possibility of its demise. On the other hand, you also just stood at the program, at the podium and said proudly that the number of 702 U.S. person queries has dropped dramatically. And that actually coincides with a dramatic decline in the number of Title one FISAs over a long period of time as well. And so I want to ask, what is the relationship between, how is it possible that the program could be growing in importance, even as it and FISA in general are being used less and less? Why, why is that not in conflict with, with itself?

Matthew Olsen: All right. So we ready for a little FISA 101 here with this very astute group?

Benjamin Wittes: Yes, absolutely.

Matthew Olsen: So I think that's a good question. And I think it's important to kind of break it down. So you have used the term traditional FISA or Title one FISA. So when we talk about traditional FISA or Title one, we're talking about FISA as it was originally intended to target people in the United States or U.S. persons here for, with individual court orders based on probable cause. Section 702 as we've talked about is a carve out to that which allows the government to target people outside the United States who are not U.S. persons without getting those individual court orders.

And you're quite right, the number of the former traditional or Title one FISAs has gone down significantly over the past several years. And there's a number of reasons for that, and one of the reasons directly answers your question. One reason is we see fewer counterterrorism targets. That's one of the reasons for the decline. But the I think the biggest reason for the decline is that Section 702 has proven to be the more effective and more capable tool and the one of choice for intelligence analysts.

So the drop in Title one FISA, FISAs is explained in large part by the use of 702 as the better tool, the more agile and more effective tool in conducting intelligence collection when it's available. In other words, when we can use it to target somebody who's outside, who's outside the United States, who's not a US person, and therefore we're not having to go to the FISA court in every case to get to to show probable cause and get a court order.

Benjamin Wittes: All right. So that is music to my ears, because I listen to that and say, hey, the availability of this less intrusive authority for purposes of a U.S. person whom you're not targeting with it, but is incidentally collected against, minimizes the use of the more intrusive authority where you're actually targeting that U.S. person. But I can see the ACLUs response, on the other hand, which is to say, ah, Matt Olsen just admitted that the government's doing backdoor searches against U.S. persons, piggybacking off of 702 and you can see, he's just proven what we've always said, which is 702 allows the surveillance that would otherwise be done with Title one FISA, which has a higher standard of review.

So I want to, I want to ask you is, you know, one of the big traditional left and civil liberties criticisms of 702 is that it enables what they call backdoor surveillance. To what extent is there any validity to that criticism? And, and, and if it's not valid, how do you square that with what you just said?

Matthew Olsen: So I don't think it's a valid criticism and I don't think the term is apt, backdoor surveillance. So, so, yes, Section 702 is, has been used increasingly, again, to target non-U.S. persons overseas. It expressly prohibits using the tool, using that authority to intentionally target anyone in the United States. So by its terms, it cannot be used in the sense that you're describing as a search for U.S. person information. That said, it is true that there are times when targeting someone overseas will also collect information about a U.S. person. If there's a person overseas who's in touch with me in the United States and that, that communication is collected under 702, it will collect,

incidentally, my communications as well. But there are strict restrictions in place about how my information can ever be reviewed or disseminated.

So I don't think it's a backdoor search. I think it's, in fact, how Section 702 is intended to be used. In other words, targeting the person overseas, collecting their information. If, as a result of that collection, somebody in the United States is identified as being in contact with or perhaps conspiring with that person overseas, whether it's to spy, to conduct a cyber-attack, to conduct a terrorist attack, then the FBI— and this is, I think, exactly what we want— the FBI pivots and decides the person in the United States, in my scenario, me is an appropriate target of a title one or traditional FISA and has to go to the FISA court to establish probable cause to collect against me.

Benjamin Wittes: So one of the things I've always thought about the backdoor search argument is that you actually, if your overseas targeting is good, you're going to get a lot of incidental collection against U.S. persons. You target person X because you believe that person is running spies in the United States. And you know that there's communication that's stored on a U.S. server. So you target that person, and it turns out your thesis is right. So he's in touch with all kinds of U.S. persons, which then causes you to collect, incidentally, on those people. And then you figure out which one of them is you want to target. If your overseas targeting is bad, then you may actually have, you may gather much less U.S. person data because you may be targeting a pizza delivery salesman in Karachi and it's not it's just not very you know, he doesn't have any U.S. person contacts.

And so one of the things that I've always been a little bit concerned about, about the U.S. person incidental collection is people take the number of U.S. persons collected against as this kind of talismanic sign of civil liberties intrusion. And it seems to me, it seems to me that that may well be wrong. It may be that if you're doing your targeting under 702 well overseas, you end up with more, not less, domestic incidental collection.

So, you know, you guys have released some data over the past few years about the number of U.S. persons affected. And the number is large just in terms of, you know, raw numbers of people who've been subject of incidental collection. How should we read that? You know, some of those numbers are really big. Should we or shouldn't we treat that as, to some degree, a metric of civil, civil liberties concern?

Matthew Olsen: So the, some of the numbers we've released have been, have shown the number of times, for example— and I think this goes to your question— the number of times that the

US government, particularly the FBI, conducts a search of 702 data using a U.S. person identifier, right. And if you think about like this cyber example, so say there is a Chinese cyber, a malicious actor who is, you know, who is carrying out some sort of cyber-attack against a U.S. company.

One of the things and we see that by 702 collection right where we're on that overseas individual in China, say who's using a US-based service provider. If we're able to collect that communication, and it may be that part of that collection includes the cyber-attack information targeting a U.S. company or that's involving a U.S. company. So if the FBI has that information, it can then search through its 702 data. One of the first things it's going to want to do, you know, the minute it understands what's happening, is to look through its holdings, which would include 702 collection with the name of that U.S. company. That's a U.S. person identifier. There may be individuals at that company that would be useful to search.

So in this case, there's no other way to search for that information. If you have to show probable cause, for example, that the company is an agent of foreign power, they're not right they're a victim in that case. So what the FBI is going to want to do is quickly search through its holdings and identify, you know, that with the identification of the company in order to understand the nature of that attack on that company. So that's the kind of information that's been released and the number of U.S. person queries. And in time, that number has been very high. I did say today, and I'm that that number has gone down significantly since we've imposed some additional requirements and procedures on the manner in which and the circumstances under which the FBI can search its 702 data.

Benjamin Wittes: But if you were I mean, again, I don't know that I want that number to come down, right? So if you have an overseas entity that is attacking, that is, you know, conducting cyber-attacks against U.S. persons and you've captured, say, a million, a million identifiers of people to whom they've sent malware, you want that now you want to search every one of them, to, you're going to, you may have to notify them that they've been the subject of of attacks. You may have to, right it, it seems to me that there are good protective reasons why the government may engage in, you know, the search of a U.S. person identifier at or may have collected that identifier to begin with, right.

And so I guess I'm, I'm always concerned when I hear people say, wow, there were 1.3 million searches. I think that's the number from one year of you know, and my reaction to that is,

yeah, but how many of those were, were, you know, because we were trying to collect on the individual and how many of them was because we were protecting them from, from, from, you know, malicious activity.

Matthew Olsen: So I tend to agree with you on, on how I think about this challenge. Not everybody has that same perspective. They see that number and they think it's a large number and they think backdoor searches or violations of, of Americans privacy and civil liberties. I think it's really important to stress that, again, this is information that we're talking about that's been collected under 702 that the FBI is searching with a U.S. person identifier to find connections. And often, as is in the case where the number was so large, was to understand the victims in a cyber-attack who have, who may have been hit. And so, you know, an IP address, for example, can be a U.S. person identifier.

So I think it's crucially important that we have that capacity, and we have that capacity to search that data without a higher standard or certainly going to a court for approval. But, but, look, we also it did make mistakes and I talked about that. And one of the reasons that we made mistakes is that the system was set by default for analysts to search in section 702 data, even when that wasn't their intended goal, even when they didn't fully explain the nature or the reason for making that search.

Benjamin Wittes: And I want.

Matthew Olsen: That's why— if I could just finish that thought— that's why when I say the number has gone down, I don't, I think the number has gone down in a way that is consistent with the actual need to continue to conduct those searches.

Benjamin Wittes: So I, I want to turn to the politics of reauthorization. But before I do, I want to ask you about the compliance issues. These are areas where, unlike these, these metrics discussion, there's no doubt these were mistakes, there's no doubt that they were improper, in some cases they were inadvertent, in other cases, they reflect gross misconduct on the part of the, of the analysts in question. And they come you know, there is this long now string dating back to 2010 of major compliance questions where as best as I can reconstruct they look like you guys catch the FBI in some misbehavior, you guys report it to the court, the court goes ballistic about it. And the result is a dialogue between the court and the bureau or the NSA with you guys as a kind of intermediary and oversight mechanism.

I have to say, when this last round of compliance issues arose, I was really frustrated and, you know, kind of like, how many times do we have to go through this process before the FBI developed some kind of organic compliance culture. And you're in a weird position here because you represent them before the court, but you also are riding herd over them in, within the executive branch. Why shouldn't I kind of throw my hands up and say, to hell with the bureau on this? They just don't seem to learn.

Matthew Olsen: So, look, we're all in this together. The Department of Justice, the rest of the intelligence community, and we have to get this right. And by that, I say, I mean we have to focus on both the structural changes that we need to make to ensure compliance, as I said in my remarks, there are going to be mistakes, we are going to make mistakes in a system that's complex that's run by human beings. We are going to make mistakes, but we need to also have a culture, in addition to structural changes, we need to have a culture of compliance that does not accept those mistakes and does everything we can to fix them.

So we've had a number of mistakes, I know I read on Lawfare when I was out of government, when your frustration, Ben and I and you know, some of those mistakes that you wrote about in Lawfare and others related to, as we've talked about, traditional FISA, Crossfire hurricane, right. And those were compliance issues, they were they were accuracy issues, they were issues around the, the completeness of the FISA applications that we're presenting to the court. And we've taken a number of steps to increase the national security division in the DOJ's oversight over those issues, completeness and accuracy of the applications that were submitted to the court.

But we've also made mistakes, particularly in the, in the effort to query 702 data. And there I am very confident in the changes that we've implemented structurally where we've changed the default settings. So basic change, we changed the default settings. So an FBI analyst has to affirmatively opt in to search 702 rather than it's searching 702 by default. We changed the rules and the training to make sure that analysts understand what it means to search and that what the standard is for searching US, using US person queries that there has to be a reasonable likelihood that it will return foreign intelligence information or evidence of a crime. And that that justification— and this is critical— that justification has to be articulated affirmatively by the analyst.

And it's these changes that have accounted for a significant drop in the number of US person queries, my judgment is that that's because in, before many of those searches were or those queries

were inadvertent, not something that the agent or analyst really meant or intended to do. But big picture and I come back to this culture of compliance, we still have work to do. We have work to do to maintain the trust of the American people in how we operate this program. But I think that's changing. I do think that we're making progress there. And that's why I'm, you know, as I said, I'm confident that we're going to get this law reauthorized this year.

Benjamin Wittes: All right. So I actually was asking not about the Crossfire hurricane stuff, but the but the 702 compliance issues. But and the 215 ones that preceded them. But I actually, Carter Page gives a very good opportunity to transition here to the politics of reauthorization. So, first of all, you mentioned that the Crossfire hurricane compliance issues don't involve this program. And so in some sense, they're beyond the scope of this discussion. That said, they're not beyond the scope of the discussion because they hugely conditioned congressional willingness to give you guys or even let you guys keep the authorities that you have.

So let's, let's, let's start, let's, let's take a moment and pause over Carter Page. And, you know, you cannot say the letters FISA in any degree of acronym, pronunciation or spelling the whole thing, you know, calling out the entire name of the statute without an intense eruption on Fox News and on the Hill about Donald Trump and spying on campaigns and Carter Page. And so, first of all, like, spell out for us very clearly why that is not the issue that we're talking about when we're not here having a broad conversation about FISA and compliance, we're talking about a specific program, to what extent are any of the issues other than politically— I'm going to come back to the politics— to what extent is this even related to the conversation about Crossfire hurricane?

Matthew Olsen: So you notice when I talked about those issues from Crossfire Hurricane, I did not make the point that that's not Section 702, and I didn't.

Benjamin Wittes: No, but I did.

Matthew Olsen: You did. But and I understand that it's a different part of FISA. It's a different section of FISA. It's a different title. But it is so much part of the challenge that we face. So, yes. Crossfire Hurricane, Carter Page, totally separate part of FISA and totally separate types of issues with the ways in which the Department of Justice and the FBI did not comply with the requirements of the statute from 702. But the reason they're so connected, and I don't just say on the politics, I think on the trust question that we you know, those mistakes that we made will cost us with the American

people and with Congress. And so I don't distinguish between the two in trying to make the case for 702. I think we have to be.

Benjamin Wittes: So you're okay with Jim Jordan going off about Carter Page when you try to bring up 702?

Matthew Olsen: Look, I think it's incumbent on us with every member of Congress to explain the value of 702 and explain how we're addressing the concerns that that that member of Congress may have. And I trust, I trust every member of Congress to understand this fundamental point, and that is that national security transcends politics. National security is more important than what political party you belong to, and that national security is not a game where we use politics to score points. So I trust that every member of Congress agrees with me on that point, and that when we have this conversation about the value of 702 and the steps we've taken to ensure compliance, it's going to be a good faith, honest conversation. We may not agree in the end on the balance, but it's going to be a conversation that's based on putting our national security first.

Benjamin Wittes: All right. So the last time we had a reauthorization discussion, we had partisan polarization. You know, it was the end of the Obama admin or the sorry, the beginning of the Trump administration. Things were pretty raw. But, and of course, the president opposed reauthorization the morning that it happened. But at the end of the day, you could get it done. Today, while you are here arguing for reauthorization, there is a select subcommittee devoted to the supposed weaponization of law enforcement and intelligence against conservatives. I don't really understand, I'm not a vote counter, but I don't really understand where the votes come from.

It seems to me this is a 70-vote matter in the Senate, and I can't see where the votes come from in the House. And so I am understanding that you're, you're a national security law and operations guy, not a congressional strategist. I'm going to ask you to be a congressional strategist. What's the, what is the coalition that sees this matter the way you do and that is open to the argument that you're making, which, which is, hey, there's, there's something above our partisan politics. And this is a, this is an authority that with all the warts and compliance issues that we've had, is really important and responsibly run. I don't know that I see 218 votes for that idea.

Matthew Olsen: So you're right, I'm not a congressional strategist, but I will say this, and this is drawing on my own experience as a both as a career government official and as a political appointee. But I go back to Section 702 when it was first authorized, first enacted in 2008. It was not

an easy argument to make then. I remember we were coming to Congress in the aftermath of the terrorist surveillance program, which authorized warrantless surveillance of Americans. And then you fast forward to the next, to the reauthorizations, the two reauthorizations over the past ten years, both occurring after the Snowden disclosures.

So what I come back to is that it's just our job. It is our responsibility in the executive branch to be partners with Congress and to be as transparent as we possibly can to provide to Congress, we can provide classified briefings, but we can also declassify information and we can make the case both to members of Congress publicly and to the American people directly on the value of the statute of 702.

And look, I fundamentally trust, I fundamentally trust, as I did having been a career DOJ official for almost 20 years, that at the end of the day, the Congress working with us will not allow politics to get in the way and will understand that national security is more important than partisan politics and national security transcends partisanship, and it has in the past in my experience. And I am confident that when we make the case, it will be successful and will prevail again.

Benjamin Wittes: So what is the form, I mean, this morning you that the attorney general and the DNI sent up a letter, Jake Sullivan issued his statement, and you're here, but what is the form in which you're going to make this case? You know, is it primarily congressional hearings? Is it forums like this? What's the, what's the, what's the, the, the, the audience to which you're going to make it? And, and how do you see that translating into legislative action?

Matthew Olsen: So I think it's an all-out effort. And so it's sort of all of the above. It is certainly making the case directly to members of Congress, and that includes the intelligence committees and the Judiciary committees in particular, providing classified briefings to give the fine details of how 702 is used, but also giving them the public argument so that they can take those arguments home to their constituents. That's first and foremost. But it's also forums like this. You know, it is speaking to informed audiences, it's gathering people who are in, who were in government, who are now outside of government, people like Glen Gerstell in the front row or David Kris, who know how these things work, bringing those folks together and, and explaining, you know, how the government is thinking about this and allowing them to, to add their voice to this effort.

So and then I think when you have people like the attorney general and the director of national intelligence and the national security adviser, all, all joining their voices to this effort, and

ultimately the White House and the president, you know, that is, that's how we're going to get this done. But it's going to require that. And I acknowledge that there are challenges ahead, acknowledge that the mistakes we've made have cost us in terms of trust. But again, there's no doubt in my mind that the value here is so essential that we cannot, we cannot fail.

Benjamin Wittes: So we are going to go to audience questions. If you have a question, please flag me, I will direct the microphone to you. Please frame your question in the form of a question. Our interest level in anybody's speechifying is extremely limited. And if you are abusive to our guest, I will shut you down with a shocking lack of due process. And while we are, while the microphone is coming in, I have one, one additional question of my own, which is, you know, like the debt ceiling, there is the day of expiration, which is in this case, December 31st when the law expires. And then there's the day of impact, which is sometime later. Realistically, what happens on December 31st and how much grace period does Congress have? When does Congress need to act by for you to be comfortable?

Matthew Olsen: So to be comfortable, Congress needs to act far in advance of December 31st. The law expires on December 31st. The impact would be felt immediately. Even though there are some provisions that allow certain types of collection to continue. But it would be, it would be you know, it would be a significant impact if we let this lapse as of December 31st. And even in the run up to December 31st, having been in the intelligence community, when sunsets are about to occur, you know, the people in the intelligence community are, are adjusting and reacting, so as far in advance of December 31st as possible is what's going to make me most comfortable.

Benjamin Wittes: Sir, the floor is yours. Please introduce yourself. And when you're done, just pass the microphone to your right.

Audience Member: Thanks. Yes. Alex Mallin, ABC News. Matt, I just want to ask kind off of Ben's last question, once you get close to that December 31st deadline, at what point do you start engaging with the White House if this just becomes something that's not within the realm of political reality, to discuss whether there's a possibility of using emergency powers by the president to make sure that you still have some of this intelligence capability that comes with 702. And I'm sorry, an off-topic question, because we have you here today. The DOJ and DNI are set to brief the Gang of Eight today on classified documents that were found at Trump, Pence and Biden's residences. I wonder, are you going to be a part of that briefing? And can you just describe at all, whether given the

concerns expressed by the Gang of Eight about not getting enough information from DOJ and DNI up to this point, what exceptions are you willing to make to give them enough information?

Benjamin Wittes: I'm going to grandfather in that last second question, please. For future questioners, stay on the subject at hand.

Matthew Olsen: I think you can appreciate I'm not going to address those reports. But on your question, you know, I think we're going to be looking, I think it's just incumbent on us as the deadline or the sunset approaches to look at all available options, existing authorities, whether it's emergency authorities or not. But that the real point, I think, is there's really no operationally feasible way to compensate for the loss and it just doesn't work like it.

Well, if there's a, if, if the law sunset or if it's watered down or diluted in a way or made so it's not as effective because, for example, there's some new requirement to get probable cause for searching the data, that it's just not something that we have the operational capability to, to meet. So, yes, there will be some contingency planning that will take place, but there shouldn't be any sort of illusion that any plan that we could come up with will even come close to compensating for the loss.

Benjamin Wittes: Ma'am.

Audience Member: Thanks. Hi, I'm Suzanne Smalley with Reuters, I cover cybersecurity and also disinformation. And I wanted to ask about disinformation because I've heard from many people who are experts in it that there are major concerns about Russia in particular seizing on this as something to stir up disinformation and division on. And I'm wondering if you've seen that, if you have concerns about it, etc.

Matthew Olsen: Disinformation about the reauthorization effort.

Audience Member: That, or even about the, the law itself. And, and its meaning, I mean, just given especially, you know, the history with the Russian investigation.

Matthew Olsen: Right. Well, look, I mean, I, I, I would say.

Audience Member: [inaudible]

Matthew Olsen: Yeah. Yeah. So I appreciate the question. I do think it's the kind of issue, you know, that you could imagine that Russia, given its past practice of using mis- and disinformation to sow discord in the United States, finding rifts in the American public on this type of issue, you could imagine this would be an area that would be rife for that. I'm not going to comment further about sort of what I've seen or not seen, but I think it's again, I think for us in the government, the goal here is to

be as transparent as we possibly can be, to have the most credible voices that we have, which include the attorney general and the director of national intelligence, talk directly to the American people and to Congress to put out information that is reliable, that is credible, that can be tested. And that, I think, is our best effort, our best way to combat that problem.

Benjamin Wittes: Sir.

Audience Member: Thanks, Ben. And how are you doing, Mr. Olsen? Jerry Dunleavy of The Washington Examiner. Given that this is something that I think congressional Republicans are going to bring up quite a bit, can you share your personal feelings on the FBI's use of the Steele dossier to obtain FISA surveillance and the FBI's effort to include it in the intelligence community assessment? And also— this is FISA related— can you confirm that FISA surveillance was obtained against CFC energy official Patrick Ho? And given how much you've talked about the significant and particular threat posed by China, I just wondered, a year after your decision to end DOJ's China initiative, if you still, you know, stand by that decision, if you could explain it a little bit more. Thanks.

Matthew Olsen: Yeah. So know, obviously I'm not going to talk about any particular FISA, right. And what I can say is with respect to whether we're talking about China and the China initiative or the range of nation states that we currently face threats from, that the way we are using Section 702 as I said to you, Ben, at the beginning, you know, initially it was really focused on counterterrorism. It has now become a critical source of intelligence when we talk about the threats we face from China, Russia, Iran or North Korea. And we've provided some detail about the nature of those threats and the way Section 702 is used to combat them.

So while I can't obviously address any particular use of FISA, whether we're talking about Title one, you know, directly using traditional FISA authorities or Section 702 in particular, other than, for example, Zawahiri, I can tell you that those two authorities together and the way we're using them have proven to be indispensably effective in protecting the country.

Benjamin Wittes: So Matt mentioned Glen Gerstell, who is the former general counsel of NSA, and David Kris, who is one of his predecessors at NSD. And we have questions from both of them. So, Glenn, the floor is yours.

Audience Member: Okay. Thank you very much. And, and thanks to both of you for, for doing this. It's very important that we have a good, strong public discussion of this vital, vital statute. One of the points, and I wish you could comment on it, Matt, is that, that is made and Ben alluded to

this when he said what happens if we don't go ahead with a reauthorization, one of the points that sometimes gets lost is that not only would we lose the actual statutory authority to compel U.S. providers by giving them a court directive to say, hand over this information pursuant to the statute, but also other sections of Title seven are lapsing and, and a bunch of other provisions in in the various statutory amendments that provide additional, additional information, reporting, etc, also goes away.

So my understanding is that in one case, we would revert to a situation in which the Attorney general alone could make decisions that now, under the new law, under the law, require FISA court decisions under other sections. Could you just comment a little bit on, on why in many ways, not only are we losing intelligence, but we're also losing some legal safeguards that would fall away?

Matthew Olsen: Yeah, it's a really important point, Glenn. I mean, look, that, you know, the core of and the focus of our conversation is on the Section 72 and that, those provisions of Title seven of FISA. But the, there are other provisions, for example, the one you mentioned that require the court to approve targeting of a U.S. person who's overseas, not a non-U.S. person, but a U.S. person overseas, which previously was done under the attorney general's own authority, still based on probable cause, but it was an additional protection that was built into the 2008 amendments to FISA that would lapse along with the rest of, of that particular title of FISA.

Look, I mean, I think the big, the big point here is so much of what's happened in intelligence law since, in the last 50 years is a reflection of the Church Committee and its report, really landmark study of surveillance abuses. And the lesson there is that we need to have oversight and accountability and we need to embed in not just the executive branch, but other branches of government, Congress and the Intelligence committees, FISA and the FISA court, with authorities to conduct oversight and to ensure accountability.

This is the lesson that we carry forward today, as now security lawyers and, and operators. And it is playing out in this debate exactly where if we lose 702, we lose not just the authority to collect, but we lose the accountability mechanisms that were built into the statute, whether it's for U.S. persons overseas or actually for US persons in the United States who may be subject to incidental collection and all of the oversight that comes with how that information is handled, those are all embedded in the statute and they all are, the, they all reflect the lessons that we've learned from the past 50 years going back to Church.

Benjamin Wittes: So, David Chris writes in from Seattle, hi Matt, how will the administration meet the demands of the traditional civil liberties constituencies and the newer concerns on the other side of the political spectrum? And if the solution for both lies ultimately in significantly limiting FBI authorities and access to 702 data, will the administration ultimately make the hard choice to cut off a finger to save the hand?

Matthew Olsen: So I'm hoping to have to do no amputations during the course of this reauthorization, David, it's a good question. Look, we're going to work with Congress. I've talked about how we're going to be, you know, it's our responsibility. We're going to do everything we possibly can to partner with Congress and where there are improvements to the statute that we can make without undermining its fundamental efficacy, you know, I think we are going to be considering those.

But as we embark at this very early stage of seeking reauthorization, I think our first and sort of primary goal is to make the case for its reauthorization based on how effective it's been and to demonstrate how we've made changes to the oversight and accountability mechanisms to address the concerns that we've raised, that we've identified. You know, I think and David, I think David Chris and others who've been around involved in this business can fully appreciate that we don't want to do is, for example, impose a requirement for probable cause to search data that the FBI for the judge.

Benjamin Wittes: And just to be clear, why not? Why, why, you know, if, if our ACLU friends were here, they would say, dude, we have a solution to this problem. It's called a warrant requirement. Why is that not good enough?

Matthew Olsen: Because think about what we'd be saying. Think about, look security is a team effort, right? You have the CIA and the NSA looking overseas, you have the FBI with primary responsibility for protecting the United States, protecting the homeland. CIA or NSA may collect based on its overseas collection. What we absolutely want is the FBI to be able to search through that data, search through that data without a probable cause requirement. Again, this is lawfully obtained data. If we were to impose a probable cause requirement, we'd be basically going back to sort of a pre911, you know, sort of wall scenario where it is very difficult for the FBI, in many cases impossible for them to search through lawfully collected data to protect us in the United States. The lesson of 9/11 is that threats that emanate overseas can affect us here at home. Sometimes, tragically. We do

not want to imperil that sort of intelligence sharing or that intelligence sort of agility and speed that allows the FBI to quickly search to identify threats that are in the United States.

Benjamin Wittes: We are going to leave it there. Please join me in thanking Matt Olsen for joining us today.

Matthew Olsen: Thank you. And thank you, everybody. Thank you.