FIXING FISA: HOW A LAW DESIGNED TO PROTECT AMERICANS HAS BEEN WEAPONIZED AGAINST THEM

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME AND FEDERAL GOVERNMENT SURVEILLANCE

OF THE

COMMITTEE ON THE JUDICIARY

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

THURSDAY, APRIL 27, 2023

Serial No. 118–18

Printed for the use of the Committee on the Judiciary

Available via: *http://judiciary.house.gov*

U.S. GOVERNMENT PUBLISHING OFFICE

52–124 WASHINGTON : 2023

COMMITTEE ON THE JUDICIARY

JIM JORDAN, Ohio, *Chair*

DARRELL ISSA, California
KEN BUCK, Colorado
MATT GAETZ, Florida
MIKE JOHNSON, Louisiana
ANDY BIGGS, Arizona
TOM MCCLINTOCK, California
TOM TIFFANY, Wisconsin
THOMAS MASSIE, Kentucky
CHIP ROY, Texas
DAN BISHOP, North Carolina
VICTORIA SPARTZ, Indiana
SCOTT FITZGERALD, Wisconsin
CLIFF BENTZ, Oregon
BEN CLINE, Virginia
LANCE GOODEN, Texas
JEFF VAN DREW, New Jersey
TROY NEHLS, Texas
BARRY MOORE, Alabama
KEVIN KILEY, California
HARRIET HAGEMAN, Wyoming
NATHANIEL MORAN, Texas
LAUREL LEE, Florida
WESLEY HUNT, Texas
RUSSELL FRY, South Carolina

JERROLD NADLER, New York, *Ranking Member*
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
ADAM SCHIFF, California
DAVID N. CICILLINE, Rhode Island
ERIC SWALWELL, California
TED LIEU, California
PRAMILA JAYAPAL, Washington
J. LUIS CORREA, California
MARY GAY SCANLON, Pennsylvania
JOE NEGUSE, Colorado
LUCY MCBATH, Georgia
MADELEINE DEAN, Pennsylvania
VERONICA ESCOBAR, Texas
DEBORAH ROSS, North Carolina
CORI BUSH, Missouri
GLENN IVEY, Maryland

SUBCOMMITTEE ON CRIME AND FEDERAL GOVERNMENT SURVEILLANCE

ANDY BIGGS, Arizona, *Chair*

MATT GAETZ, Florida,
TOM TIFFANY, Wisconsin
TROY NEHLS, Texas
BARRY MOORE, Alabama
KEVIN KILEY, California
LAUREL LEE, Florida
RUSSELL FRY, South Carolina

SHEILA JACKSON LEE, Texas, *Ranking Member*
LUCY MCBATH, Georgia
MADELEINE DEAN, Pennsylvania
CORI BUSH, Missouri
STEVE COHEN, Tennessee
DAVID N. CICILLINE, Rhode Island

CHRISTOPHER HIXON, *Majority Staff Director*
AMY RUTKIN, *Minority Staff Director & Chief of Staff*

C O N T E N T S

THURSDAY, APRIL 27, 2023

FIXING FISA: HOW A LAW DESIGNED TO PROTECT AMERICANS HAS BEEN WEAPONIZED AGAINST THEM

Thursday, April 27, 2023

HOUSE OF REPRESENTATIVES

SUBCOMMITTEE ON CRIME AND FEDERAL GOVERNMENT SURVEILLANCE

COMMITTEE ON THE JUDICIARY

Washington, DC

The Subcommittee met, pursuant to notice, at 9:05 a.m., in Room 2237, Rayburn House Office Building, Hon. Andy Biggs [Chair of the Subcommittee] presiding.

Members present: Representatives Biggs, Jordan, Gaetz, Tiffany, Nehls, Moore, Kiley, Lee, Fry, Jackson Lee, Nadler, Dean, and Cicilline.

Also present: Representatives Bishop and Cline.

Mr. BIGGS. The Subcommittee will come to order. Without objection, the Chair is authorized to declare a recess at any time. We welcome everyone to today's Hearing on the Foreign Intelligence Surveillance Act and appreciate our witnesses being here. I do apologize because, like you, Ms. Jackson Lee, I was down at the Judiciary Committee room, on the floor, just wondering where everybody was. That is the way it goes. So, I will now recognize myself for an opening statement.

I welcome my colleagues to this important hearing and I want to welcome our witnesses. Thank you for being here.

FISA, the Foreign Intelligence Surveillance Act, has shown to be a powerful tool for United States intelligence, but the United States intelligence community has shown they cannot be fully trusted to retain this vast power. In fact, I cannot think of an example of when a powerful intelligence tool was not abused in the United States in this way. When we give power to the Federal government, the Federal government has abused that power seemingly every time.

In my experience, we have a saying that when a man gets power, thinks that they have power, they almost always tend to abuse it. I think that is the case here.

President Obama's IRS had to apologize after targeting conservatives. President Biden's DOJ targets Catholics and characterizes worshippers as adhering to a radical traditional Catholic ideology.

Just last week, the Judiciary Committee learned that the Biden campaign, without any governmental power, peddled a conspiracy theory that the Hunter Biden laptop was Russian disinformation to effect the outcome of an election. They did this without FISA.

A former CIA official testified to this Weaponization Committee that then Biden campaign senior advisor, now Secretary of State Antony Blinken, played a role in the inception of the public statement signed by the current and past intelligence officials that claim that the Hunter Biden laptop was part of a Russian disinformation campaign.

A Twitter user was just sentenced for up to 10 years for election interference for tweeting a meme, a joke, that fewer than 5,000 people saw or believed. How many people believe this election effort in the *Politico* article,

> Hunter Biden story is Russian disinfo, dozens of former intel office officials say. More than 50 former intelligence officials signed a letter casting doubt on the provenance of a *New York Post* story on the former Vice President's son.

We want to be able to trust our intelligence community, the officials who gather intelligence. Well, I view this now with a great deal of skepticism. If they would lie to the free flow of information to subvert an election and earn a top job with the new administration without FISA, I fear that these same people would still think they can break the rules if they retain powerful tools like FISA. I believe they would do it, too, just as they have done before.

In 2019, Department of Justice Inspector General Michael Horowitz, who is one of our witnesses today, exposed the extent to which President Obama's FBI violated its authorities under FISA using FISA as a pretext to illegally spy on Trump campaign associates in an attempt to affect another election. They weren't as successful in 2016 as they were in 2020. I remember having private conversations with Inspector Horowitz, besides his public testimony, and always enlightening, and I appreciate his candor. I look forward to it today.

At that time, in his investigation, Inspector General Horowitz analyzed a sampling of 29 applications to the FISA Court to authorize surveillance. In 25 of them, there was unsupported, uncorroborated, or inconsistent information in the Woods files which are procedures for ensuring the factual accuracy of information contained in FISA applications. The FBI was unable to even locate the Wood files for the other four applications.

Further review by the Inspector General revealed that the FBI failed to recognize the significant risk posed by systemic noncompliance with the Woods procedures. In those 29 applications which were reviewed, the Inspector General found over 400 instances of noncompliance with the Woods procedures. The FISA Court, the FISC, approved all 29 of those applications.

In 2020, FBI Director Wray testified before the Committee telling then Ranking Member Jordan that,

> Jordan would not lose any sleep over the vast majority of FISA applications and we wouldn't want to grind FISA to a halt with more scrupulous review.

Well, I can't speak for Chair Jordan, but I actually do lose sleep over FISA applications. I lose sleep over the 3.4 million warrantless searches of Americans' communications using FISA Section 702;

3.4 million warrantless searches in 2021 alone, which is nearly triple the approximately 1.3 million queries in 2020.

While reports indicate the FBI conducted fewer queries in 2022, it still made roughly 559 searches per day. That represents, in my opinion, intelligence officials breaking the rules 559 times per day. I lose sleep over the fact that Section 702 information acquired without a warrant can later be used by the FBI in criminal prosecutions unrelated to foreign intelligence or national security. I lose sleep knowing that the FBI has misused privileged, warrantless spying power to conduct rogue surveillance on innocent Americans. To me, this is not a partisan issue. I don't believe either side can condone that.

I lose sleep knowing that these reports are only a piece of the government's abuses of the FISA program and only the ones that I know about.

At the end of this year, Section 702 of FISA is set to expire. Reports in recent years have exposed the government's and specifically, the FBI's abuse of this program. A law designed to provide tools to collect foreign intelligence and prevent foreign terrorist attacks has been worked into a domestic intelligence tool to intercept and catalogue Americans' phone calls, text messages, emails, and other electronic communications. Unfortunately, for the intelligence community, we have a Fourth Amendment in the United States and I say that sarcastically. It is not unfortunate that we have a Fourth Amendment. It is one of the great blessings that sets the United States apart from every other nation.

As Congress considers whether to reauthorize this program, this Committee will be at the forefront, this Subcommittee will be at the forefront. This Subcommittee has the opportunity to shed a light on the broad issue of warrantless, mass surveillance and hopefully end it once and for all. We must consider whether this program can be reformed or if it is beyond repair.

FISA Section 702 explicitly states that it may only be used to target non-U.S. persons located abroad for the purpose of obtaining foreign intelligence information, but it is clear that the government has used communications acquired through this program to conduct back-door searches of Americans' communications.

For years now, I have called for serious reform or even full repeal of FISA, but the Federal intelligence community, even Members of Congress, have attempted to scare us to make us believe that these unchecked powers are the only method available to protect our Nation from harm. Well, every American should be concerned to know Federal agents are spying on them, even if you have nothing to hide.

We need to prohibit warrantless surveillance of Americans and hold accountable any Federal official who violates the civil liberties of Americans. I wonder how much longer we must watch the FBI brazenly spy on Americans before we start stripping it of its unchecked authority. Make no mistake, actors within the FBI and other similar Federal agencies will continue to conduct unlawful and unconstitutional surveillance of Americans.

While there are political examples of abuse of intelligence agencies to affect elections, this is not a political issue. It is not a partisan issue. I hope that this issue has the potential to be a rare bi-

partisan effort in this Congress to protect the rights of Americans. I know I have talked to some of my colleagues across the aisle who have similar views as I do and I look forward to working with them to either fix or end these abuses.

I thank again our witnesses for being here and look forward to hearing your testimony today and with that, I will yield back and recognize the distinguished Ranking Member, the gentlelady from Texas, Ms. Jackson Lee.

Ms. JACKSON LEE. Good morning, Mr. Chair, and thank you very much. Thank you to the Members who are present here today and thank you to the witnesses who are likewise present here today.

I realize that today we are speaking of fixing FISA. I hope it is in reference to many aspects of what we have seen particularly in the September 2021 report. We have found that there are fixes that can go across administrations, across investigations, and our responsibility is to be the oversight board, if you will, for the American people.

Having been here since 9/11, and recognizing the terror we felt and the immediacy of concern, but this Committee, working with our Chair and other Members of the Committee, made sure that we likewise protected the American people in the legislation that we passed at that time. In fact, we had to redo it, in essence, to ensure the protection of the American people. So, I know that we are talking about and should be talking about a law that is designed to enhance America's national security.

Let's be very clear. I take issue with my good friend's assessment of the weaponization of this particular tool. We must, in fact, find a way as we did previously in a bipartisan manner to deal with the tool that we use for individuals that are non-U.S. persons and who happen to be abroad.

Let me be clear, as well, that if we are specifically looking at the contact between the 2016 Trump campaign and surveillance of Carter Page, a former campaign advisor, we know that this was under Title 1 of FISA, not under 702. So, we need to recognize the broad base of the needs of national security. I am about to mention as I begin my remarks the airman, the National Guard Airman that has brought at least personal terror to me. It is not a 702 case, but we will need the tools of investigation to ensure, as we are now learning, that there may be overseas connections to investigate the horror of a young airman of being able to access the highest level of national secrets in this country. We are not looking at that today. I think that is an appropriate review. If it deals with tools that the FBI may ultimately have to use. I, for one, certainly hope that justice is rendered and that the gentleman faces sufficient punishment to know that this is not something that you fool with.

Today, we should be looking at not fooling with America's security and doing it in the right way and ensuring that the tools are stood up and that they are stood up right.

So, I thank you for convening today's hearing on the Foreign Intelligence Surveillance Act. As the important and sometimes controversial Section 702 of FISA is set to sunset this year, hearings before this Subcommittee will be critical to sorting out the record of privacy compliance by the intelligence community during this last reauthorization period.

I expect that today's witnesses will offer us insight on the performance of the intelligence visions under Section 702 and be distinctive, distinctive in what we are talking about here today. We are not on a fishing expedition today. Maybe it will be necessary forthright, but under Section 702 and compliance efforts implemented in recent years to ensure that U.S. persons are not needlessly swept into our international surveillance web. The Foreign Intelligence Surveillance Act was passed in 1978 to curb abuses in the collection and use intelligence information, foreign and domestic. Under the original provision of FISA, collection of foreign intelligence required the government to show not only that there is probably cause to believe the target of intelligence surveillance is an agent of a foreign power, but also that foreign intelligence gathering is a primary purpose of the collection.

As I indicated when we had to take a look at this under the USA Patriot Act 2001 and the aftermath of 9/11 and beyond, the government need only show such probable cause and that foreign intelligence gathering is merely a significant purpose of the collection. That was framed around the fears of 9/11.

In the wake of 9/11, the intelligence gathering needs of the Nation and advances in technology require the government to devote substantial resources to obtaining court approval based on a showing of probable cause to conduct surveillance against terrorists located overseas.

Witnesses before this Committee testified that these standards frustrated intelligence gathering and stated that the intelligence community was collecting only approximately two thirds of the foreign intelligence information. That was collected prior to legal interpretations that required the government to obtain individualized FISA Court-ordered or overseas surveillance.

In response to this situation and the evolution of technology, Congress enacted the FISA Amendments Act of 2008. The FAA authorized the government to collect massive amounts of information through the targeted surveillance of foreign persons reasonably believed to be outside of the United States without a warrant. With such massive amounts of information being collected invariably, information involving U.S. persons in the U.S. whose information is not constitutionally subjected to targeting might be collected.

However, the statute includes protection for U.S. persons who may be on the other end of these communications. The FAA requires intelligence agencies to design targeting procedures which limit the scope of collection before the government acts and minimalization [sic] of procedures which limit the use of information about U.S. persons after the government incidentally collects the information, rightly so for the American people's protection.

The Foreign Intelligence Surveillance Court reviews these procedures for legal sufficiency. The FISA Court is indispensable and must play a meaningful role in ensuring compliance with the law and Congress must have regular access to information about the extent to U.S. communications being collected and the authority to require of U.S. persons are being scooped up through the surveillance of a target. That is crucial to fit into our constitutional infrastructure.

The intelligence community reports that it adheres to both the letter and the spirit of the law. So, remember, with nearly all this oversight conducted in secret, the public has no choice, but to take the government at its word and that is why we are here today in an open, nonclassified briefing and hearing. With the war in Ukraine and other political instability around the globe, we clearly live in unstable times requiring our intelligence community to maximize its resources to keep America safe from threats both foreign and domestic.

America and its allies face continuous national security threats from foreign nations and terrorist organizations, foreign agents from rival nations continue to spy on the United States and Al-Qaeda and other terrorist networks continue to plot attacks against America. America's security cannot be guaranteed at the border alone and I am reminded of my early remarks about the young airman.

Congress must ensure that our national security agencies are able to gather foreign intelligence information from foreign terrorists and nation states, so that we can stop threats before they reach our shores. It is clear that FISA and Section 702 have proven successful in achieving this goal, but as we consider reauthorization, we must also ensure that the constitutional right of U.S. persons are not compromised in the process. The objective is any authorized program of foreign intelligence surveillance must be to ensure that American citizens and persons in America are secure and that their persons, papers, effects while making terrorists everywhere else in the world insecure.

Finally, the best way to achieve these dual goals is to follow the rule of law and the exclusive law to follow with respect to authorization authorizing foreign surveillance gathering on U.S. soil is FISA which can, and should be modernized to accommodate new technologies. Therefore, as we consider reauthorization of Section 702, we must examine the existing privacy safeguards and consider further modification to ensure Americans' constitutional rights are protected as we have done in previous years.

In 2015, Congress enjoyed a great deal of success working together to pass the USA Freedom Act that created a new program for the targeted collection of telephone metadata, while providing greater privacy in civil liberties protections for Americans, expanding existing Congressional oversight for businesses, and creating greater transparency of the Nation's security programs operated under FISA. At that time, we demonstrated that we can build consensus around our common values, both in this Committee and on the House floor. Among those values are a dedication to privacy, transparency, and protection from unreasonable searches.

Mr. Chair, we have a similar opportunity before us again as we discuss ways in which we can craft and reach an authority that serves the Government's needs and respect our commitment to protecting the cherished privacy of Americans. So, therefore, let us work together on behalf of the American people.

I look forward to the testimony of the witnesses, Mr. Chair, and I yield back. Thank you for the time.

Mr. BIGGS. Thank you. The gentlelady yields back. The Chair now recognizes the Chair of the Full Committee, Mr. Jordan, for an opening statement.

Mr. JORDAN. Mr. Chair, I look forward to hearing from our witnesses. Thanks for putting this hearing together. I yield back.

Mr. BIGGS. The gentleman yields back, and I now recognized the Ranking Member of the entire Committee, Mr. Nadler.

Mr. NADLER. Thank you, Mr. Chair. Today, this Committee finally gets back to the serious work of keeping Americans safe, safe from those who seek to do us harm and safe from those who might trample on our civil liberties in a quest to keep our country secure no matter the cost. Section 702 of the Foreign Intelligence Surveillance Act is scheduled to sunset on December 31st of this year. I, myself, have never voted to reauthorize Section 702, but I recognize that these authorities are also important to national security especially in today's threat environment.

I am looking forward to hearing from the expert witnesses in today's hearing and the hearings to come. I intend to approach the question of reauthorization this year with a cautious, but open mind, toward reform.

Since FISA Section 702 was last reauthorized in January 2018, the surveillance landscape has considerably evolved. Five years later, on the other end of the pandemic, our on-line communications represent an even broader reflection of our daily lives. Under an authority as powerful as Section 702, even if the intelligence agencies are not targeting us directly, the government is sweeping up records of our banking, our meetings, our education, and our simplest human interactions.

Foreign State actors have also adjusted to the new way of life. Ransomware, cyber-threats, and cyber-espionage are all now common threats to the United States. Today, a foreign state actor can disable a hospital's computer systems, shut down a power grid, and steal classified national security information, all without entering the United States.

Section 702 is one important tool our intelligence community uses to fight these and other threats. The problem with this authority has always been in its application. The statutory protections on the books are simply insufficient for protecting our civil rights and our privacy. For example, although Section 702 authorizes only the targeting of non-U.S. persons who are outside the United States, we know that massive amounts of U.S. persons' data are swept up under this programmatic surveillance.

Despite our best efforts, our intelligence agencies have kept us largely in the dark as to how many Americans' communications are incidentally collected every year. We know from what reporting is available that the government has a lot of this data and that much of it could not have been obtained without a warrant had they tried to collect it directly.

The warrantless collection of this much data alone should give anyone pause. Those American communications are not just collected and set aside. They are made available to agencies like the FBI, who can search the 702 data base for our communications for purposes having nothing to do with national security. These so-called back-door searches are neither hypothetical, nor rare. Last

year, the FBI used U.S. personal identifiers to query the 702 data base nearly 3.4 million times.

Now, the FISA Court has found that querying information that has already been legally acquired is not considered another search under the Fourth Amendment. Incidental collection is not accidental collection. The government knows at the outset that it will obtain our communications. The FBI should not also be able to rifle through them as if they arrived by chance.

Simply put, Congress should no longer entertain the legal fiction that back-door searches are either constitutional or respectful of our privacy. Nor, should we find comfort in the FBI's track record accessing this information appropriately. The FISA Court has repeatedly found violations at the FBI where employees searched U.S. personal identifiers for neither foreign intelligence nor evidence of a crime.

True, in many of those cases the court found that the unauthorized searches were not malicious or intentional, but rather the product of a lack of training and difficult to use technology. I suppose we should be gratified that the rate of these incidents appears to have dropped dramatically in the past year. We have been tinkering with better training and better technology for almost two decades. Moving from of a few million violations a year to merely a few hundred thousand does not inspire confidence.

No massive surveillance operation should be given free rein to evade our constitutional protections. Section 702, as it currently exists, does just that.

The question we face this year is whether changes to the 702 program can effectively protect our civil liberties. That is not a question that can be answered in just one hearing, but there is reason to be optimistic that Section 702 can be changed for the better. When Congress last reauthorized this provision in January 2018, it implemented some minor statutory changes to improve civil liberties protection. The effects of these changes is just beginning to be seen in DOJ querying practices and its publication of U.S. persons query numbers among others.

These small improvements are not new to congressional legislation. After the Court of Justice of the European Union struck down the U.S.-EU privacy shield in 2020, an agreement that governed the flow of data across the Atlantic, the Biden Administration took steps to improve, redress, and oversight of its surveillance operations as part of negotiations for a different data privacy agreement. These, too, were steps in the right direction.

As we consider the merits of this program, I could caution my colleagues against using the Federal government as a bogeyman to prove some political point. Many of us agree that Section 702 needs to be updated to better protect Americans' communications, but we should also acknowledge that the problems presented by 702 are not cabined to this administration or to the last administration. Section 702 has been a threat to our privacy and civil liberties for years and to pretend otherwise does a disservice to the important bipartisan work ahead of us.

Thank you, Mr. Chair. I look forward to hearing from our witnesses and I yield back the balance of my time.

Mr. BIGGS. I thank Mr. Nadler and I am optimistic after hearing your positions, because I think we share a lot of the same positions on this.

We will now introduce today's witnesses.

The Honorable Michael Horowitz. Mr. Horowitz is the Inspector General of the Department of Justice. He oversees a staff of more than 500 special agents, auditors, inspectors, attorneys, and support staff tasked with deterring, detecting waste, fraud, abuse, and misconduct in DOJ programs and personnel. He previously served as Chair of the Council of the Inspectors General on Integrity and Efficiency from 2015–2020.

Welcome, Inspector General Horowitz.

The Honorable Sharon Bradford Franklin. Ms. Franklin is the Chair of the Privacy and Civil Liberties Oversight Board. Prior to her appointment, she served as Co-Director of the Security and Surveillance Project at the Center for Democracy and Technology. From 2013–2017, she served as the Executive Director of the Privacy and Civil Liberties Oversight Board.

Thank you for being here, Ms. Franklin.

The Honorable Beth Williams. Ms. Williams is a Board Member of the Privacy and Civil and Liberties Oversight Board. Prior to her appointment, she served as an Assistant Attorney General for the Office of Legal Policy at the Department of Justice and was a litigator in private practice.

Welcome, Ms. Williams. Thank you for being here.

We welcome you today and thank our witnesses. We will begin by swearing you in. Would you please each rise and raise your right hand?

Do you swear or affirm under penalty of perjury that the testimony you are about to give is true and correct to the best of your knowledge, information, and belief, so help you God?

Let the record reflect the witnesses have answered in the affirmative. You may be seated.

Please know that your written testimony will be entered into the record in its entirety. Accordingly, we ask that you summarize your testimony in five minutes. As I let you know at the beginning, I will let all our Members know as well, just so you will remember, we have the Joint Session of Congress for the President of the Republic of Korea will be here at 11:00 and we have to be in our seats by 10:35-ish I think is the word.

With that, Mr. Horowitz, you may begin.

STATEMENT OF THE HONORABLE MICHAEL HOROWITZ

Mr. HOROWITZ. Thank you, Chair Biggs, Ranking Member Jackson Lee, and Members of the Committee. I appreciate you inviting me to testify today.

In every year since 2006, the OIG's Annual Report on the Top Management and Performance Challenges Facing the Department of Justice has highlighted the difficulty faced by DOJ and the FBI in maintaining the proper balance between protecting national security and safeguarding civil liberties.

My office regularly conducts national security and surveillance oversight work, including OIG reviews of the FBI's use of its specific FISA authorities, the FBI's use of other national security au-

thorities, and the FBI's and other DOJ law enforcement components' use of confidential human sources and administrative subpoenas. I've attached to my written testimony links to the 20 post-9/11 reports that my office has done in these areas.

The overarching conclusion from this series of reports is that compliance has certainly been far from perfect, and that transparency, effective internal controls, and rigorous internal and external oversight are needed and critical to ensuring that the significant authorities held by the department investigators and prosecutors to surveil Americans are used in accordance with applicable laws, court orders, and the Constitution.

Indeed, the importance of rigorous, ongoing, and effective oversight in this area was highlighted by disturbing findings in three of our recent reports.

First, our review of four FISA applications and other aspects of the FBI's Crossfire Hurricane investigation.

Our audit of the FBI's execution of its Woods Procedures in connection with FISA applications for U.S. persons.

Our audit on the roles and responsibilities of the FBI's Office of General Counsel on national security matters.

These reports highlight three centrally important principles that this Subcommittee and the Committee should be considering as you look at the future of 702.

First, there needs to be effective supervisory review, and that needs to occur in real time to prevent compliance errors from occurring in the first place. In our experience, effective and strong supervisory review helps detect and prevent errors before they occur. In connection with both our Crossfire Hurricane review and our Woods review, we identified significant inadequacies in the supervisory review, as we reported on, that could have had a meaningful impact on how those programs were conducted.

Second, effective, routine, and regular internal oversight is needed to identify and address any program weaknesses. With any program, but, particularly, with the National Security Program, DOJ, and FBI must have their own effective internal auditing and compliance functions and controls to ensure that they're complying with laws, rules, and regulations, and, of course, the Constitution.

During our Woods Procedures audit, we actually found that they did have such procedures and were doing such audits. The problem was they weren't looking at the results, so that they could make effective reforms and make changes.

We've seen recently that the FBI and the department has created a compliance training—Compliance Trends Analysis Group and an Office of Internal Accounting. Those are important steps. We will be reviewing those as we look at our recommendations and consider whether and how those actions have affected compliance.

Third, the significant issues that we've identified demonstrate the need for strong, rigorous, outside oversight. That's the kind of work we've done. We're going to hear from the Privacy and Civil Liberties Oversight Board, the work that they've done, and others, to ensure that recommendations—to ensure there's compliance and to ensure that recommendations are followed and implemented.

One of the things that requires is timely access to information and records. This Committee and the Congress took an important

step in that regard, in 2016, with passage of the IG Empowerment Act. That work is also resource-intensive. Our recent work on the Crossfire Hurricane and Woods audits required well more than a dozen of our staff to work on those matters for an extended period of time.

We've appreciated the strong support that Congress has given us through the Appropriations Committees, and we look forward to continuing that work with the support of the Congress. We look forward to speaking further of that with the Subcommittee, about how the work we do and our future—what we've done, and our future work can continue to ensure that the department operates with integrity, with efficiency, with accountability, and in compliance with all laws, and, of course, the Constitution.

Thank you. I look forward to answering your questions and appreciate being here today.

[The prepared statement of the Hon. Horowitz follows:]

Office of the Inspector General
United States Department of Justice

Statement of Michael E. Horowitz
Inspector General, U.S. Department of Justice

before the

U.S. House of Representatives Committee on Appropriations
Subcommittee on Crime and Federal Government Surveillance

concerning

"Fixing FISA: How a Law Designed to Protect Americans Has Been Weaponized Against Them"

April 27, 2023

Chairman Biggs, Ranking Member Jackson Lee, and Members of the Subcommittee:

Thank you for inviting me to testify today regarding the Foreign Intelligence Surveillance Act (FISA), and the Department of Justice (DOJ) Office of the Inspector General's (OIG) prior oversight work on FISA. Many of the findings and recommendations from our prior oversight of the Department's use of FISA and other investigative authorities will help to inform congressional deliberations on FISA's Section 702, which expires at the end of this year.

In every year since 2006, the OIG's annual report on "Top Management and Performance Challenges Facing the Department of Justice" has highlighted the difficulty faced by the Department and the Federal Bureau of Investigations (FBI) in maintaining a balance between protecting national security and safeguarding civil liberties. The OIG's prior national security and surveillance oversight work has included OIG reviews of the FBI's use of specific FISA authorities, the FBI's use of other national security-related surveillance authorities, and the FBI's or other Department law enforcement components' use of confidential human sources (CHSs) and administrative subpoenas. We have also conducted reviews that specifically examined the impact of the FBI's use of investigative authorities on U.S. persons engaged in activities that are protected by the First Amendment. For reference and additional information as the Subcommittee and Congress examine Section 702, I have included an appendix with links to twenty, post-September 11, 2001 reports from the OIG on these topics.

The overarching conclusion from this series of reports is that transparency, and effective internal and external independent oversight, are necessary to ensure that the tremendous authority held by the Department's investigators and prosecutors to surveil Americans is used in accordance with applicable laws, court orders, and the Constitution. Without transparency and oversight -- from the OIG, the U.S. Privacy and Civil Liberties Oversight Board (PCLOB), Congress, the Foreign Intelligence Surveillance Court (FISC), non-government stakeholders, and importantly, effective internal audits and assessments by the FBI and National Security Division (NSD) -- mistakes, errors, and abuses risk being repeated, eroding public trust in the proper use of these authorities to the detriment of national security.

In today's testimony, I will focus on the need for ongoing, rigorous, and effective oversight of the Justice Department's national security authorities by discussing the findings and recommendations from our three most recent FISA-related reports: 1. Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation (Crossfire Hurricane Review); 2. Audit of the Federal Bureau of Investigation's Execution of Its Woods Procedures for Applications Filed with the Foreign Intelligence Surveillance Court Relating to U.S. Persons (Woods File Audit), and 3. Audit of the Roles and Responsibilities of the Federal Bureau of Investigation's Office of the General Counsel in National Security Matters (FBI OGC Audit). For each of these reports, I will provide a summary of the report and the steps taken by the FBI and Department to implement our recommendations to strengthen compliance with the Constitution and the laws, rules, and regulations that govern the Department's use of these authorities.

The OIG's Review of Four FISA Applications and other Aspects of the FBI's Crossfire Hurricane Investigation

In December 2019, the DOJ OIG released our review of certain actions by the FBI and the Department during an FBI investigation, known as "Crossfire Hurricane," into whether individuals associated with the Donald J. Trump for President Campaign were coordinating, wittingly or unwittingly, with the Russian government's

efforts to interfere in the 2016 U.S. presidential election. Among other issues, our review assessed four applications filed with the FISC in 2016 and 2017 to conduct FISA surveillance targeting Carter Page, who had been a Trump campaign official prior to the FISA surveillance. The applications to surveil Carter Page were sought pursuant to Title I of FISA, which requires the Department to file an application with the FISC to authorize the electronic surveillance of a telephone number, email account, or other "facility." In its application, the government must show probable cause to believe that the proposed target is a foreign power or an agent of a foreign power.

Our review of the Department's applications to authorize FISA surveillance of Carter Page found that FBI personnel fell far short of the requirement in FBI policy that they ensure that all factual statements in a FISA application are "scrupulously accurate." We identified multiple instances in which factual assertions relied upon by the FISC in the FISA applications were inaccurate, incomplete, or unsupported by appropriate documentation, based upon information the FBI had in its possession at the time the applications were filed. We found that the problems we identified were primarily caused by the FBI's Crossfire Hurricane team failing to share all relevant information with the NSD and, consequently, the information was not considered by the Department decision makers who ultimately decided to support the applications. We identified 17 significant inaccuracies and omissions in the four applications -- 7 in the first FISA application and a total of 17 by the time of the final renewal application in 2017.

In our conclusion to that report, we explained the significance of these errors, noting:

> The authority under FISA to conduct electronic surveillance and physical searches targeting individuals significantly assists the government's efforts to combat terrorism, clandestine intelligence activity, and other threats to the national security. At the same time, the use of this authority unavoidably raises civil liberties concerns. FISA orders can be used to surveil U.S. persons, like Carter Page, and in some cases the surveillance will foreseeably collect information about the individual's constitutionally protected activities, such as Page's legitimate activities on behalf of a presidential campaign. Moreover, proceedings before the Foreign Intelligence Surveillance Court (FISC)—which is responsible for ruling on applications for FISA orders—are ex parte, meaning that unlike most court proceedings, the government is present but the government's counterparty is not. In addition, unlike the use of other intrusive investigative techniques (such as wiretaps under Title III and traditional criminal search warrants) that are granted in ex parte hearings but can potentially be subject to later court challenge, FISA orders have not been subject to scrutiny through subsequent adversarial proceedings.
>
> In light of these concerns, Congress through the FISA statute, and the Department and FBI through policies and procedures, have established important safeguards to protect the FISA application process from irregularities and abuse. Among the most important are the requirements in FBI policy that every FISA application must contain a "full and accurate" presentation of the facts, and that agents must ensure that all factual statements in FISA applications are "scrupulously accurate." These are the standards for all FISA applications, regardless of the investigation's sensitivity, and it is incumbent upon the FBI to meet them in every application.

The FBI fell far short of these standards in the applications targeting Carter Page, even though the FBI recognized that these applications would be subject to greater scrutiny than most FISA applications.

In addition, we identified numerous instances of non-compliance with the FBI's factual accuracy review procedures (the "Woods Procedures") in connection with the four Carter Page FISA applications. The FBI's Woods Procedures require agents to document in a Woods File the support for all factual assertions contained in FISA applications for surveillance. The FBI adopted its Woods Procedures in 2001, following earlier concerns raised by the FISC about inaccuracies in FISA applications. However, in connection with the Carter Page applications, we found basic, fundamental, and serious errors during the FBI's completion of its Woods Procedures and that some agents did not appear to know certain basic requirements of the Woods Procedures. In light of the significant compliance issues we identified, the OIG initiated an audit to more broadly examine the FBI's compliance with its Woods Procedures. I detail below the results of that audit.

In addition to initiating the Woods Procedures audit, the OIG made nine recommendations to the Department and the FBI to assist them in avoiding similar failures in future investigations. The first of these recommendations, which remains open in part, included four subparts, and is intended to strengthen the accuracy of FISA applications submitted by the Department to the FISC. It requires the Department and the FBI to ensure that adequate procedures are in place for NSD to obtain all relevant and accurate information needed to prepare accurate FISA applications and renewal applications, including any exculpatory information in the FBI's possession.

The Department and FBI concurred with this recommendation, have completed 3 of the 4 subparts, and are continuing with their efforts to fulfill the final requirement. In early 2022, the Department submitted to the OIG a FISA Accuracy and Completeness Memorandum, revised procedures and forms, and provided evidence that employees had completed revised training on these procedures. We believe these steps demonstrate progress the FBI and the Department have made towards addressing the issues we identified in our Crossfire Hurricane review. However, given the importance of the issue and our concerns about the lack of compliance with prior reforms (such as the Woods procedures), we have informed the Department and FBI that evidence from future internal compliance reviews will be necessary to accumulate sufficient data for the Department and the FBI to assess, and the OIG to verify, the effectiveness of the new policies and procedures in ensuring that the NSD receives from the FBI all relevant and accurate information to prepare accurate FISA applications.

Audit of the Federal Bureau of Investigation's Execution of Its Woods Procedures for Applications Filed with the Foreign Intelligence Surveillance Court Relating to U.S. Persons

Because of the extensive failures we identified in the Crossfire Hurricane Review and the unacceptable level of errors and omissions in the Carter Page applications, we determined that additional OIG oversight work was required to assess the FBI's compliance with Department and FBI FISA-related policies that seek to protect the civil liberties of U.S. persons. Accordingly, we initiated the Woods File Audit to further examine the FBI's compliance with the Woods Procedures in Title I FISA applications that target U.S. persons. We completed our Woods File Audit in September 2021.

In March 2020, prior to the completion of our audit, and based on the information we had gathered during our initial assessment of a sample of FISA applications, we issued a Management Advisory Memorandum (MAM) to FBI Director Wray to report that we had identified Woods Procedures non-compliance in all 29 FISA applications we reviewed. These applications had all been approved by the FISC between fiscal years 2015 and 2019. The Department thereafter notified the FISC of 209 errors in those applications, 4 of which

DOJ deemed material. Our further audit work identified over 200 additional instances of Woods Procedures noncompliance—where Woods Files did not contain adequate supporting documentation for statements in the 29 applications—although the FBI and NSD subsequently confirmed the existence of available support elsewhere. We also identified at least 183 FISA applications for which the required Woods File was missing or incomplete.

In addition to the Woods File compliance and accuracy errors, we identified significant weaknesses in the FBI's supervisory review of Woods Files, which we determined contributed to the compliance and accuracy errors in the Woods Files and applications. Specifically, we observed that the Woods Files generally did not contain evidence of the thoroughness or completeness of this supervisory review, which is an important quality control check in the process. Rather, the files we reviewed indicated only that a supervisor had signed a verification form, indicating that they had reviewed the documentation in the Woods File.

We also raised concerns, both in our March 2020 MAM and the final September 2021 Woods Procedures Audit Report, about the lack of follow through by the Department and FBI in response to issues identified from the FBI and NSD's internal oversight findings and reviews. The FBI and NSD conduct periodic reviews designed to ensure that FISA applications contain accurate information. However, as we noted in our March 2020 MAM, FBI personnel told us that the FBI and NSD accuracy review reports had not been used in a comprehensive, strategic fashion by FBI Headquarters to assess the performance of individuals involved in and accountable for FISA applications, to identify trends in results of the reviews, or to contribute to an evaluation of the efficacy of quality assurance mechanisms intended to ensure that FISA applications were "scrupulously accurate." That is, the accuracy reviews were not being used by the FBI as a tool to help assess the FBI's compliance with its Woods Procedures.

Based on these and related findings in our MAM and full audit report, the OIG made an additional twelve recommendations to strengthen the Woods Procedures and reduce the risk of erroneous information being included in FISA applications, which can lead to faulty probable cause determinations and the infringement of U.S. persons' civil liberties.

During our audit, the FBI began to implement over 40 corrective actions to address the OIG's recommendations. These corrective actions included: (1) updating the FBI's forms and checklists used during the preparation of FISA applications and Woods Files to ensure that all relevant information to the FISA request has been provided and verified by responsible parties; (2) formalizing the role of FBI attorneys in the legal review process for FISA applications; (3) developing and implementing new training for FBI personnel; (4) pursuing technological improvements to aid in consistency and accountability; and (5) identifying new audit, review, and compliance mechanisms to ensure that the changes to the FISA application process are effective.

In addition, in August 2020, then Attorney General Barr announced supplemental reforms to enhance compliance, oversight, and accountability of FBI foreign intelligence activities, as well as to augment the internal compliance functions of the FBI. Specifically, then Attorney General Barr directed the FBI to create an Office of Internal Auditing to conduct routine audits of the FBI's compliance with FISA and FISC orders and to assess measures taken by the FBI to ensure accuracy and completeness of FISA applications.

In response to the March 2020 MAM and Woods File Audit recommendations, the Department and FBI have taken a number of additional actions. One of the most significant of these actions is the FBI's creation of the Compliance Trends Analysis Group (CTAG). The CTAG is responsible for reviewing compliance reports regarding the FBI's use of national security legal authorities, including FISA applications submitted to the FISC, and analyzing internal and external compliance reports to identify trends, including cross-cutting issues.

Based on the establishment of the CTAG, which will help improve the efficacy of the internal FBI and NSD review processes, and related reforms established to improve accountability and accuracy in the Woods Procedures, the OIG has closed all but one of the 12 recommendations from our March 2020 MAM and Woods File Audit. The remaining open recommendation requires the FBI to develop and implement a policy that describes the expectations for supervisory review of Woods Files. Although the FBI has updated its supervisory review policy, it has not updated it in a way that effectively demonstrates that a supervisor's review of a Woods File and supporting documentation consist of more than simply signing the FISA Verification Form. The FBI is continuing to work on a method to demonstrate further evidence of the steps that a supervisor has taken to review and ensure accuracy, beyond signing a form.

Audit of the Roles and Responsibilities of the Federal Bureau of Investigation's Office of the General Counsel in National Security Matters

Following the issuance of our Crossfire Hurricane Review, then Attorney General Barr requested that the OIG conduct an audit to review the roles and responsibilities of the FBI's Office of the General Counsel (OGC) in overseeing compliance with applicable laws, policies, and procedures relating to the FBI's national security activities. We completed this audit in September 2022.

FBI's OGC and the Department's NSD both have roles in ensuring that the authorities exercised by the FBI and DOJ respect the rule of law and maintain public trust and confidence in the FBI's use of intrusive investigative authorities, including those authorized by FISA. Our audit identified several instances of ineffective coordination between FBI OGC and NSD and uncertainty in the delineation of their roles that negatively impact important workflows between them. For example, we found instances of FBI OGC attorneys advising FBI investigators on topics traditionally reserved for prosecutors, disagreements between FBI OGC and NSD attorneys related to FISA processes, and varying interpretations by FBI OGC and NSD of key legal principles.

We also found that, for several years, NSD and FBI OGC had differing interpretations of the query standard under the FBI's Section 702 Querying Procedures. As the Subcommittee is aware, Section 702 of the FISA Amendments Act of 2008, 50 U.S.C. § 1881a, governs targeted surveillance of foreign persons reasonably believed to be located outside the United States with the compelled assistance of electronic communications service providers. An acquisition authorized under Section 702 may not intentionally target a United States person or any person known at the time of the acquisition to be located in the United States. To ensure the requirements of Section 702 are appropriately met, the Attorney General, in consultation with the Director of National Intelligence (DNI) adopted: (1) targeting procedures designed to ensure the FBI targets foreign persons outside the United States, (2) minimization procedures designed to ensure the FBI safeguards United States person information incidentally acquired, and (3) querying

procedures containing a query standard that sets the requirements for the FBI to query, or search, its unminimized, or raw, Section 702-acquired information.

In 2015, DOJ told the FISC that the FBI's standard for querying was "reasonably likely to return foreign intelligence information or evidence of a crime." However, the language in the FBI's querying rules at that time was "to the extent reasonably feasible, authorized users...must design such queries to find and extract foreign intelligence information or evidence of a crime." Consequently, we were told by FBI OGC that FBI and NSD operated under different query standards. One senior FBI OGC official stated that this led to numerous compliance incidents and resulted in the FBI almost losing its Section 702 authorities.

We also were told that FBI OGC had significant concerns that this NSD interpretation of the FBI's query standard, which FBI OGC says has a heightened threshold, creates limitations and operational risks that may prevent the FBI from identifying threats through methods that were available prior to implementation of the new interpretation of the query standard in 2015. In contrast, NSD told us that the query standard has been the same since 2008 (when Section 702 was created by Congress). A senior NSD official told us that the FBI had a fundamental misunderstanding of the standard and that compliance incidents were not identified sooner because NSD can only review a limited sample of the FBI's queries and NSD improved upon its ability to identify non-compliant queries over time.

The FBI clarified the query standard in its 2018 Section 702 Querying Procedures. The FBI's amended Section 702 Querying Procedures defined the query standard as: "Each query of FBI systems containing unminimized contents or noncontents (including metadata) acquired pursuant to section 702 of the Act must be reasonably likely to retrieve foreign intelligence information, as defined by FISA, or evidence of a crime, unless otherwise specifically excepted in these procedures." To help ensure implementation of the amended query procedures occurred, the FBI, in consultation with NSD, developed mandatory training on the query standard and required that all personnel with access to raw FISA-acquired information complete the training by December 2019.

However, despite these efforts, we learned that there were still disputes between NSD and FBI OGC on query-related compliance incidents. A senior FBI OGC official stated that FBI OGC has recently redoubled its efforts to ensure compliance with the query standard after concerns were raised about FBI query incidents in a November 2020 FISC opinion, a semiannual assessment conducted jointly by NSD and the Office of the Director of National Intelligence (ODNI) released in November 2020, and an Attorney General (AG) Memorandum issued on April 22, 2021. This senior FBI OGC official said the FBI is currently focused on addressing its query-related compliance incidents through a variety of methods, including database changes, an audit, and training.

On November 1, 2021, the Department issued new guidance titled "FBI FISA Query Guidance," which is designed to assist FBI personnel in understanding the querying standard and in conducting queries of raw FISA collection that comply with applicable requirements. Further, the guidance provides illustrative examples of both compliant and noncompliant queries. In response to the new guidance, the FBI developed and deployed an updated training course on the query standard, which FBI personnel with access to raw FISA-acquired information were required to complete by January 2022. We verified that all FBI personnel with access to raw FISA-acquired information either completed the required training or had their access to this information revoked by the end of January 2022.

To address the type of disconnect between FBI OGC and NSD that we observed during the audit, we made a total of 5 recommendations – 3 to the FBI and 2 to the Office of the Deputy Attorney General (ODAG). The FBI and ODAG concurred with each of the recommendations, and their resolution is still largely in progress (one of the five recommendations, related to the use of FISA-derived information in criminal trials, has been recently closed).

Additional Observations

As these recent reports demonstrate, transparency and effective internal and external oversight are essential to ensuring that these important authorities are used in accordance with applicable laws, court orders, and the Constitution. In the context of oversight of Section 702 authorities, I want to highlight three important issues for consideration: 1) the need for effective supervisory review that occurs in real time and can prevent compliance errors from occurring; 2) the need for effective, routine, and regular internal oversight to identify and correct any errors or program weaknesses close in time to their occurrence; and 3) the role of the OIG and other independent oversight entities in conducting periodic, big picture external reviews.

1. *Ensuring there is an appropriate level of review and approval at the Department and FBI prior to FBI personnel querying unminimized Section 702 information*

In connection with both our Crossfire Hurricane Review and Woods File Audit, we identified inadequate supervisory review as a significant concern and emphasized the importance of ensuring meaningful and effective supervisory review before a FISA application is submitted to the FISC. In our experience, effective and strong supervisory review can help detect and prevent compliance errors before they occur. With regard to Section 702 queries, in June 2021, the FBI instituted a policy requiring FBI attorney approval prior to FBI personnel conducting a "batch job" that would result in 100 or more queries of unminimized Section 702 information. According to the Department, the FBI attorney pre-approval requirement is designed to ensure that there is additional review in situations where one incorrect decision could potentially have a greater privacy impact due to the large number of query terms. While we have not tested the FBI's new approval procedures, in general this type of higher level or legal sufficiency review prior to any query, if implemented effectively, promotes accountability, can provide opportunities to better explain query standards before an error is made, and may be appropriate in light of the non-supervisory positions, such as "technical information specialist," identified by the FISC as being responsible for some of the reported query errors.

2. *Ensuring there is effective internal oversight by FBI OGC and NSD through regular audits and/or other accountability measures*

As with any program, but particularly with a sensitive national security program, the Department and the FBI are invariably the first line of defense in ensuring its own personnel are complying with laws, rules, and policies governing the use of such authorities. Internal auditors and oversight personnel at the FBI and NSD have direct access to information, as well as the capacity and mandate, to conduct routine audits and compliance reviews that can and should identify and correct compliance errors close in time to their occurrence. As we noted in our March 2020 MAM, we were concerned to find that the compliance problems and trends identified by the FBI and the Department through their own internal oversight efforts were not

timely addressed. That is why we are continuing to monitor the implementation of the corrective actions taken in response to our Crossfire Hurricane Review, including seeking evidence of the efficacy of the post-reform internal reviews conducted by the FBI and NSD. As I noted throughout this testimony, the FBI and Department have taken a number of steps to improve internal oversight, including the establishment of the CTAG and the FBI's Office of Internal Accounting. We also have noted language in the December 2021 Compliance Assessment by the Attorney General and Director of National Intelligence, which states:

> The resolution of particular compliance incidents can provide lessons learned for all agencies. Robust communication among the agencies is required for each to effectively implement its authorities, gather foreign intelligence information, and comply with all legal requirements. For those reasons, NSD and ODNI generally lead calls and meetings on relevant compliance topics, including calls or meetings with representatives from all agencies implementing Section 702 authorities, so as to address interagency issues affecting compliance with the statute and applicable procedures.

As the OIG continues to assess the FBI and NSD's efforts to promote compliance with our outstanding recommendations and Section 702, we will test this and related reforms instituted by the Department and FBI, to better understand how these identified issues and concerns are communicated to the individual FBI user of FISA information. We will also continue to emphasize the importance of internal oversight, as we work with the FBI and Department to close the remaining open recommendations from our FISA-related reviews.

3. *Ensuring independent oversight entities, such as the OIG and the PCLOB, have timely access to information, as well as sufficient resources, to conduct effective oversight and to report on the Department and FBI's compliance with laws, rules, and regulations*

Independent oversight, conducted by entities like the OIG and PCLOB, plays an essential role in identifying any compliance issues or concerns, and allows recommendations to be made to address them that, in turn, guide the ongoing, routine oversight conducted by the FBI and NSD. In order to perform this oversight in a meaningful way, we need timely and complete access to all information. In 2016, Congress greatly assisted the OIG in that regard by passing the IG Empowerment Act. Currently, for my office, resources and personnel are the biggest challenges we face in conducting more than periodic oversight of the FBI and Department's use of national security authorities, including FISA's Title I and Section 702. The OIG has approximately 506 FTEs and an annual budget of $139 million (plus $10 million for Crime Victims Fund oversight) to oversee a DOJ workforce of about 125,000 employees and a discretionary budget of about $37.3 billion, which includes the FBI, the Federal Bureau of Prisons, and the Department's three other law enforcement components (the DEA, ATF, USMS), as well as billions of dollars spent through DOJ contracts and grants. Moreover, the national security reviews referenced in this testimony were resource intensive; for example, the Crossfire Hurricane Review and the Woods File Audit required the efforts of more than a dozen OIG personnel for an extended period of time. Nonetheless, we will continue to conduct, consistent with our available resources, periodic oversight of FISA implementation (including, if requested, a review of any reforms passed by this Congress related to Section 702), and we greatly appreciate the strong support that we have received from Congress that has allowed us to perform this critical oversight work.

Conclusion

Thank you for your continued support for our mission, which allows the OIG to conduct objective, fact-based, and thorough oversight of the Department and provide transparency for the public and Congress. I look forward to continuing to work closely with the Subcommittee to help ensure that DOJ operates with integrity, efficiency, and accountability. That concludes my prepared remarks, and I would be pleased to answer any questions that the Subcommittee may have.

Appendix – Prior OIG Reports on FISA and National Security Authorities

Reviews of the FBI's use of specific FISA authorities

1. A Review of the FBI's Handling of Intelligence Information Related to the September 11 Attacks (November 2004), https://oig.justice.gov/sites/default/files/legacy/special/s0606/final.pdf;

2. A Review of the Federal Bureau of Investigation's Activities Under Section 702 of the Foreign Intelligence Surveillance Act Amendments Act of 2008 (September 2012), https://oig.justice.gov/reports/2016/o1601a.pdf;

3. A Review of the Federal Bureau of Investigation's Use of Section 215 Order for Business Records (March 2007), https://oig.justice.gov/sites/default/files/legacy/special/s0703a/final.pdf;

4. A Review of the FBI's Use of Section 215 Orders for Business Records in 2006 (March 2008), https://oig.justice.gov/reports/2016/215-2008.pdf;

5. FBI's Use of Section 215 Orders: Assessment of Progress in Implementing Recommendations and Examination of Use in 2007 through 2009 (May 2015), https://www.oversight.gov/sites/default/files/oig-reports/o1505.pdf;

6. A Review of the FBI's Use of Section 215 Orders for Business Records in 2012 through 2014 (September 2016), https://www.oversight.gov/sites/default/files/oig-reports/o1604.pdf;

7. A Review of the FBI's Use of Trap and Trace Devices Under the Foreign Intelligence Surveillance Act in 2007 through 2009 (June 2015), https://www.oversight.gov/sites/default/files/oig-reports/o1506.pdf.

FBI use of other national security-related surveillance authorities

8. A Review of the Federal Bureau of Investigation's Use of National Security Letters (March 2007), https://oig.justice.gov/reports/2016/NSL-2007.pdf;
9. A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006 (March 2008), https://oig.justice.gov/reports/2014/s1410a.pdf;
10. A Review of the Federal Bureau of Investigation's Use of National Security Letters: Assessment of Progress in Implementing Recommendations and Examination of Use in 2007 through 2009 (August 2014), https://oig.justice.gov/reports/2014/s1408.pdf;
11. A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records (January 2010), https://www.oversight.gov/sites/default/files/oig-reports/s1001r.pdf;
12. A Review of the Department of Justice's Involvement with the President's Surveillance Program (July 2009), https://oig.justice.gov/reports/2016/PSP-01-08-16-vol-3.pdf.

FBI's and other Department law enforcement components' use of confidential human sources (CHSs) and administrative subpoenas

13. Audit of the Bureau of Alcohol, Tobacco, Firearms and Explosives' Management and Oversight of Confidential Informants (March 2017), https://oig.justice.gov/reports/2017/a1717.pdf;

14. Audit of the Drug Enforcement Administration's Confidential Source Policies and Oversight of Higher-Risk Confidential Sources, Audit Division 15-28 (July 2015), https://oig.justice.gov/reports/2015/a1528.pdf;

15. Audit of the Drug Enforcement Administration's Management and Oversight of its Confidential Source Program

(September 2016), https://www.oversight.gov/sites/default/files/oig-reports/a1633.pdf;

16. Public Summary of the Addendum to the Audit of the Drug Enforcement Administration's Management and Oversight of its Confidential Source Program (March 2017), https://oig.justice.gov/reports/2017/a1633a.pdf;

17. A Review of the Drug Enforcement Administration's Use of Administrative Subpoenas to Collect or Exploit Bulk Data (March 2019), https://www.oversight.gov/sites/default/files/oig-reports/o1901.pdf;

18. The Federal Bureau of Investigation's Management of Confidential case Funds and Telecommunication Costs (January 2008), https://oig.justice.gov/reports/FBI/a0803/final.pdf.

Reviews on the impact of the FBI's use of investigative authorities on U.S. persons engaged in activities that are protected by the First Amendment

19. A Review of the FBI's Investigative Activities Concerning Potential Protesters at the 2004 Democratic and Republican National Political Conventions (April 2006), https://oig.justice.gov/sites/default/files/legacy/special/s0604/final.pdf;

20. A Review of the FBI's Investigations of Certain Domestic Advocacy Groups (September 2010), https://www.oversight.gov/sites/default/files/oig-reports/s1009r.pdf.

Mr. BIGGS. Thank you, Inspector General.

Now, Ms. Franklin, you may begin.

STATEMENT OF THE HONORABLE SHARON BRADFORD FRANKLIN

Ms. BRADFORD FRANKLIN. Chair Biggs, Ranking Member Jackson Lee, and Members of the Committee, thank you for the opportunity to testify before you today.

I'm testifying in my individual official capacity. So, the views I express today are my own and not necessarily the views of any fellow board members.

The Privacy and Civil Liberties Oversight Board is an independent agency, and our role is to review Federal counterterrorism programs to ensure that they have appropriate safeguards for privacy and civil liberties.

The PCLOB is currently examining Section 702 of FISA, which, as you know, is set to expire at the end of this year, unless reauthorized. Our review does not examine traditional FISA orders, such as those at issue in the Crossfire Hurricane investigation.

Section 702 authorizes the government to target non-Americans located outside the United States and to collect the content and metadata of their communications. Although the board has not yet completed our Section 702 report, we can already say that we agree three things are true.

Section 702 is valuable in protecting our national security, and Section 702 creates risks to privacy and civil liberties, and these risks can, and should be, addressed without undermining the core value of the program. We are confident that the privacy risks posed by Section 702 can be addressed while preserving the program's value in protecting our national security.

Since our report is not yet complete, I cannot say what recommendations we'll make collectively as a board. Instead, I will briefly describe my own views regarding three particular privacy risks that I urge Congress to address.

First, Section 702 implicates the privacy rights of Americans due to the volume of incidental collection. Section 702 targets can only be non-U.S. persons reasonably believed to be located outside of the United States. The FISA Court annually reviews and approves the general categories of foreign intelligence to be collected, as well as targeting procedures, minimization procedures, and querying procedures. No judge ever reviews analysts' targeting decisions, nor do the procedures require that targets be suspected of wrongdoing.

The legal rationale for these lower standards is that 702 targets are non-U.S. persons. So, they do not have recognized Fourth Amendment rights. Nonetheless, if a U.S. person communicates with a foreign target, their communications can be collected through what the government calls incidental collection.

The term "incidental" makes it sound like a small amount, but we don't actually know the scope of this collection. The government has argued that it would not be feasible to calculate a meaningful number, but I believe that an estimate that involves some margin of error can still be helpful to Congress, as you assess what safeguards are needed for Section 702.

A second key aspect of Section 702 involves what the government calls U.S. person queries. Analysts use queries to search through already collected communications. As I've just described, Section 702 does not require judicial review before targeting or at the front end of Section 702 surveillance. There also is no requirement that government agents establish probable cause or obtain the permission of a judge before they conduct a search through 702 data seeking information about a specific American. That is why privacy advocates refer to these U.S. person queries as "backdoor searches."

There's been a lot of public attention to FBI's violations of the existing query rules. Importantly, the FBI has recently implemented several reforms designed to improve compliance, but I do not believe that these changes are sufficient to address the privacy threats.

U.S. persons' communications are entitled to protection under the Fourth Amendment. So, when there's no judicial review at the front end, the government should not be able to search through collected communications for a specific American's communications without any individualized judicial review. As Congress debates reauthorization of Section 702, I urge you to incorporate a requirement for FISA Court review of U.S. person query terms to ensure protection of U.S. persons' Fourth Amendment rights.

The final privacy risk I want to mention is the risk that the government will seek to restart "abouts" collection, which involves communications that are neither to or from a target, but, instead, include a reference to a target. In 2017, the NSA announced that it had suspended "abouts" collection. Then, the January 2018 reauthorization of Section 702 prohibited "abouts" collection, but also provided that the government could restart this collection after obtaining FISA Court approval and giving notice to Congress.

However, the unique privacy risks posed by "abouts" collection would reemerge if restarted. I'd, therefore, urge Congress to remove the provision authorizing the government to restart this type of collection.

Ultimately, I urge Congress to use the opportunity of the Section 702 sunset to adopt meaningful reforms, and I'm encouraged that this Committee is beginning this process now. I am confident that Congress can address the privacy risks posed by Section 702, while preserving the key value the program offers to protect our national security.

Thank you, and I look forward to your questions.

[The prepared statement of the Hon. Bradford Franklin follows:]

Statement of Sharon Bradford Franklin
Chair, Privacy and Civil Liberties Oversight Board
Before the Subcommittee on Crime and Federal Government Surveillance
Of the House Judiciary Committee
Hearing titled "Fixing FISA: How a Law Designed to Protect Americans Has Been Weaponized Against Them"
April 27, 2023

Chairman Jordan, Chairman Biggs, Ranking Member Jackson Lee, and Members of the Subcommittee,

Thank you for the opportunity to testify before you today. I want to start by noting that I am testifying in my individual official capacity, so the views I express are my own, and not necessarily the views of the Privacy and Civil Liberties Oversight Board as a whole or of any of my fellow Board members.

For those of you who may not be familiar with our agency, the PCLOB is an independent agency within the executive branch, and our role is to review federal counterterrorism programs to ensure that they include appropriate safeguards for privacy and civil liberties. Congress created the PCLOB based on a recommendation of the 9/11 Commission. The Commission urged that as Congress took steps to expand the government's powers to address terrorist threats, Congress should also create a board to serve as a voice within the government for privacy and civil liberties.

The PCLOB is headed by a five-member bipartisan Board, and I am the Chair. Because the PCLOB is an independent agency, we are not required to take positions consistent with those of the administration.

When the PCLOB conducts oversight, our role is not only to assess whether a program complies with existing law and rules, but it is also to make policy recommendations to ensure that there are adequate safeguards for privacy and civil liberties. Our recommendations may urge the executive branch agencies conducting a program to take action, and other recommendations may urge Congress to enact legislative reforms.

The PCLOB is currently examining Section 702 of the Foreign Intelligence Surveillance Act (FISA), which is scheduled to expire at the end of December, unless Congress acts to reauthorize the program. Section 702 authorizes the government to target non-Americans located outside the United States, and to

collect both the content and metadata of their communications. The surveillance must be conducted for a foreign intelligence purpose that is approved by the Foreign Intelligence Surveillance Court (FISA Court), as part of an annual certification process. This program is operated principally by the NSA, but also by the FBI, the CIA and the National Counterterrorism Center.

The PCLOB first reviewed and released a report on Section 702 back in 2014, and we are working to develop and publish a new report this year, to inform the public and congressional debate over reauthorization. Our review focuses on Section 702, which is the sole provision of FISA that is scheduled to sunset at the end of this year. It does not examine traditional FISA orders, such as the type at issue in the Crossfire Hurricane investigation.

Although the Board has not yet completed our Section 702 report, we can already say that we agree that three things are true: Section 702 is valuable in protecting our national security; Section 702 creates risks to privacy and civil liberties; and these risks can and should be addressed without undermining the core value of the program. We are confident that the privacy risks posed by Section 702 can be addressed while preserving the program's value in protecting Americans' national security.

Since our report is not yet complete, I cannot say what recommendations we will collectively make as a Board. Instead, I would like to briefly describe three particular privacy risks that I urge Congress to address as you consider reauthorization of Section 702: the volume of "incidental" collection, the rules governing U.S. person queries, and the current statutory authority for restarting "abouts" collection.

Volume of Incidental Collection

First, Section 702 implicates the privacy rights of Americans due to the volume of incidental collection. Under Section 702, surveillance targets can only be non-U.S. persons – so only people who are not U.S. citizens or legal permanent residents – and at the time of collection, targets must be reasonably believed to be located outside the United States. Each year, the FISA Court reviews and approves submissions from the Attorney General and Director of National Intelligence that set out the categories of foreign intelligence to be collected, and the FISA Court annually reviews and approves a series of procedures that govern how the Section 702 program is run: targeting procedures, minimization procedures, and querying procedures.

In this way, the FISA Court does review the standards that government analysts need to apply when they select targets under Section 702. These standards focus on whether a target is likely to possess or communicate foreign intelligence information, but do not require any finding of probable cause or even a determination that a target poses a threat or is associated with wrongdoing. In addition, no judge ever reviews analysts' targeting decisions.

By contrast, when the government seeks to conduct surveillance of a target who is a U.S. person, the government must establish probable cause and obtain the approval of a judge before conducting the surveillance. The legal rationale for this distinction is that under Section 702, the targets are non-U.S. persons – so, they are people who do not have recognized Fourth Amendment rights. Nonetheless, if a U.S. person communicates with a foreign target, their communications can be collected through what the government calls "incidental collection."

Understandably, the government wants to know who is on the other end of communications with its 702 targets – including people inside the United States. They want to figure out whether those people in the United States are working with the non-American targets to plot acts of terrorism or otherwise pose threats to the United States. Thus, incidental collection is a feature of Section 702 and not a bug. This should be distinguished from reverse targeting, which the statute explicitly prohibits, and which would involve targeting someone outside of the United States as a pretext, when the real intent is to acquire the communications of someone inside the United States.

The term "incidental" makes it sound like it's a small amount or insignificant. But we don't actually know the scope of this collection, and this is one of the key policy issues that I believe Congress should address in connection with reauthorization of Section 702. When the PCLOB issued its earlier Report on Section 702 in 2014, the Board recommended that the NSA should calculate and publish several metrics designed to provide insight into the extent of incidental collection, and since that time, Members of the House Judiciary Committee have also urged the intelligence agencies to provide an estimate of the scope of incidental collection.

But the government has not attempted to estimate the number of U.S. persons whose communications have been collected under Section 702, and has instead argued that it would not be feasible to calculate a meaningful number. Within

the past year, some academics have published a paper outlining a method based on secure multi-party computation to provide an estimate of the extent of incidental collection, and this seems to be a promising approach worth exploring further. Essentially, the dispute is over what kind of metrics would be meaningful to Congress and the public.

The extent of incidental collection matters, because the greater the number of Americans who are directly affected, the greater the need for Congress to ensure the safeguards throughout the 702 program are sufficient. So, when the alternative is that we have no estimates at all on the scope of incidental collection, I believe an estimate that involves some margin of error can still be meaningful and helpful to Congress as you assess what safeguards are needed under Section 702.

U.S. Person Queries

A second key aspect of Section 702 surveillance involves what the government calls U.S. person queries, and many privacy advocates refer to as "backdoor searches." A U.S. person query is a method for intelligence analysts and FBI agents to search through the communications the government has collected under Section 702, seeking information about a particular U.S. person. As I've just described, under Section 702, there is no requirement for judicial review before targeting – or at the "front end" of 702 surveillance. And the rules for conducting U.S. person queries also do not require government agents to establish probable cause or to seek the permission of a judge before they conduct such a search through Section 702 data. This is why privacy advocates refer to these U.S. person queries as "backdoor searches."

This Committee has, in the past, considered and approved amendments to Section 702 that would address this very issue. Although those particular amendments have not made it into law, when Congress last reauthorized Section 702 in January 2018, it did adopt an amendment that applies in a very narrow set of circumstances, to require the FBI to seek a warrant from the FISA Court before accessing the results of a U.S. person query. However, not only is that statutory requirement very narrow, but the FBI has never sought such a court order, even in several documented cases where the requirement actually applied.

In most instances, the existing rules permit intelligence analysts to search through 702 data for information about specific U.S. persons if they assess that

the query is reasonably likely to return foreign intelligence information, and, in the case of the FBI, they may also conduct U.S. person queries if they assess the query is reasonably likely to return evidence of a crime.

There has been a lot of public attention recently to violations of the existing rules for U.S. person queries by the FBI. These have included publicized accounts about queries searching for information about Members of Congress, and queries seeking information about individuals who had requested to participate in FBI's "Citizens Academy" program for business, religious, civic and community leaders.

Importantly, within the past year and a half, the FBI has implemented several reforms designed to improve compliance with the existing rules. These have included changing the default settings in its query system so that agents must affirmatively opt in to have their queries run through 702 data, and establishing special approvals for sensitive queries such as those involving elected officials, members of the media, members of academia, and religious figures.

These reforms are welcome, and the FBI has announced that the changes have already led to a drop in the number of U.S. person queries it conducts of over 90%, and that compliance with the existing rules is improving. But I do not believe these changes are sufficient to address the privacy threats posed by these warrantless searches seeking information about specific Americans.

U.S. persons' communications are entitled to protection under the Fourth Amendment. So, when there is no judicial review at the front end, the government should not be able to search through collected 702 data for a specific American's communications without any individualized judicial review. As Congress debates reauthorization of Section 702, I urge you to incorporate a requirement for FISA Court review of U.S. person query terms, to ensure protection of Americans' Fourth Amendment rights.

"Abouts" Collection

The third privacy risk I want to mention is the risk that the government may seek to restart what has been called "abouts" collection. "Abouts" collection involves the collection of communications that are neither "to" nor "from" a target, but instead include a reference to a target's selector, such as an email that contains a target's email address in the body of the message. NSA

previously conducted "abouts" collection through the upstream portion of Section 702, which involves collection of communications from the internet backbone.

As the PCLOB noted in its 2014 report on Section 702, "abouts" collection created unique threats to privacy, by increasing the risk that NSA would collect purely domestic communications and the risk that the government would "acquire communications exclusively between people about whom the government had no prior suspicion, or even knowledge of their existence, based entirely on what is contained within the contents of their communications."

In the spring of 2017, the NSA announced that it had suspended "abouts" collection, noting that this would reduce the risk of collection of communications of U.S. persons or others who are not in direct contact with a target.

When Congress reauthorized Section 702 in January 2018, the legislation prohibited "abouts" collection, but also provided that the government could restart such collection after obtaining approval from the FISA Court and giving notice to Congress.

Since the NSA suspended "abouts" collection in 2017, it has changed the ways in which it conducts upstream surveillance under Section 702, and the changes have significantly reduced the privacy risks from upstream collection. However, the privacy threats previously identified by the PCLOB would re-emerge if the government were to restart "abouts" collection. I therefore urge Congress to remove the provision authorizing the government to restart this type of collection.

Expanding and Strengthening the Role of the FISA Court Amicus

Finally, I urge that in connection with the reauthorization of Section 702, Congress should take the opportunity to expand and strengthen the role of the FISA Court amici. Congress created this "friend of the court" role through the USA FREEDOM Act in 2015, which requires the FISA Court to appoint a panel of at least five individuals with expertise in privacy, civil liberties, intelligence collection, or communications technology, and to select members of this panel to participate in cases involving "a novel or significant interpretation of the

law." The amicus role has been valuable, and FISA Court judges have relied upon the amici's positions.

Back in 2014, when the PCLOB issued its report examining the Section 215 bulk phone records program, the Board unanimously recommended that Congress create what the Board called a "special advocate" role, which was similar to the amicus role that Congress later created. However, the amici role as enacted in 2015 is weaker than the special advocate position described by the PCLOB in three critical ways. First, the PCLOB recommended that the special advocates participate in more than just matters involving "novel and significant" issues. Second, the PCLOB urged that the special advocates should have full access to information related to the matters in which they participate. Third, the Board recommended that the special advocates should be able to petition for an appeal from the FISA Court to the FISA Court of Review (FISCR), and from the FISCR to the Supreme Court. None of these requirements are contained in the current statute.

As Congress crafts legislation in anticipation of the Section 702 sunset date, I urge you to include provisions that would expand and strengthen the role of the amici in at least these three ways: expand the types of matters in which amici participate, require that amici be provided with full access to information related to the matters in which they participate, and enable the amici to petition for appeal of decisions by the FISA Court and by the FISA Court of Review.

Ultimately, I urge Congress to use the opportunity of the Section 702 sunset date to adopt meaningful reforms, and I am encouraged that the Committee is beginning the process now. I am confident that Congress can address the privacy risks posed by Section 702 while preserving the key value the program offers to protect our national security.

Thank you and I look forward to your questions.

Mr. BIGGS. Thank you, Ms. Franklin.

Now, Ms. Williams, you are recognized for five minutes.

STATEMENT OF THE HONORABLE BETH A. WILLIAMS

Ms. WILLIAMS. Good morning.

Thank you, Chair Biggs, Ranking Member Jackson Lee, and Members of the Committee, for inviting me to testify before you today regarding Section 702. On behalf of the Privacy and Civil Liberties Oversight Board, I'm grateful to be here today.

Before I begin, there are a few caveats to my testimony.

First, as the Chair said, "I am also only one Member of the Board. So, I'm speaking in my individual capacity as a board Member and not for the board as a whole."

Second, I want to note that we are currently working on an extensive report on the Section 702 program. We anticipate that this report will explain the program in as complete and unclassified a manner as possible, and that it will provide further recommendations going forward.

On that last point, with the exception of the three points of agreement Chair Franklin stated at the outset, the report and the Members' discussions and deliberations are very much still in process. So, out of respect for my fellow Members, as well as the fact that we are still receiving new information, much of which is classified, I'll be somewhat limited in what I can opine on at this time.

Third, I note that our forthcoming report is focused on the program operated pursuant to Section 702, and not on FISA as a whole and not on Title I authorities. So, I would defer to my copanelist and Inspector General Horowitz on questions beyond Section 702.

I am, however, deeply concerned, as I know are many of the Members of this Subcommittee and others in Congress, regarding FBI misuses of its authority. There must be no repeat of the egregious violations of law and policy committed during the investigation of alleged Russian interference in the 2016 election campaign of former President Trump.

Furthermore, although those violations occurred under a separate section of FISA that governs investigations of U.S. citizens, the intelligence community has not been faultless in its application of the Section 702 program, either. Indeed, it is evident that many queries of information about U.S. persons were run against 702-collected information, specifically, by the FBI in conflict with governing policies and procedures. This is unacceptable and must be acknowledged and addressed.

The FBI has taken some steps to remediate this problem. I anticipate that the board's forthcoming report will detail some of the significant compliance incidents and will make further recommendations to the FBI and to the intelligence community as a whole.

Having said that, I would like to spend a few minutes this morning clarifying some points about the program. To begin with, Section 702 does not permit targeting of U.S. persons. Also important, Section 702 is not a bulk collection program. Instead, the program targets specific non-U.S. persons abroad about whom an individualized determination has been made that they are reasonably likely

to possess, receive, or communication foreign intelligence information.

That intelligence information has led to the discovery of previously unknown terrorist plots directed against the United States and our allies, enabling the disruption of those plots. It has assisted and protected our troops abroad, and it has been used to identify and to prevent multiple foreign attacks on our critical infrastructure. There can be no question that the program is extraordinarily valuable to the safety and well-being of Americans.

In contrast to some of the query and compliance issues that I mentioned, we also have not seen significant compliance problems with regard to the collection of information. Indeed, in the most recently released joint assessment of the program, the NSA targeting compliance incident rate was .08 percent. During the same reporting period, the FBI targeting compliance rate was .007 percent.

This means that the intelligence community is largely avoiding improper collection under existing law and policies. That is, they are not improperly targeting U.S. persons or persons reasonably believed to be located in the United States.

As you are deliberating on how to improve Section 702 going forward, I'd like to offer two topics for your consideration.

First, what the FBI considers sensitive queries are crucially important. When you get at the heart of what most worries concerned citizens, it is that the intelligence community will be weaponized against politically disfavored opponents. That is unacceptable in a democracy and must be guarded against.

Recently, and belatedly, the FBI put in place procedures that require heightened review for certain queries, such as those involving elected officials, members of the media, and religious figures. In the most sensitive cases, review is required by the Deputy Director of the FBI personally. Congress should look closely at these enhanced preapproval policies and consider whether this requirement might be codified, strengthened, or reviewed by the FISC.

Finally, Congress might consider how Section 702-derived information could be used in the context of vetting, both for immigration purposes and for individuals applying for high-level security clearance. Currently, for most agencies, a query of unminimized Section 702 data is permitted only where the search is reasonably likely to retrieve foreign intelligence information. This means that the U.S. Government may already have in its possession information that a visa applicant or a person applying for the high-level clearance poses a threat to our national security or is in communication with someone who does. No one from our government might ever see this information because our agents and analysts cannot run a query for it in the unminimized 702 collection.

If Congress wants to ensure that persons coming in to work in our country or persons entrusted with our most important national security information are thoroughly vetted against information already in the government's possession it might consider looking further.

Mr. BIGGS. Ms. Williams your five minutes has expired.

Ms. WILLIAMS. Thank you. I look forward to your questions.

[The prepared statement of the Hon. Williams follows:]

Statement of Beth A. Williams
Member, Privacy and Civil Liberties Oversight Board
Before the Subcommittee on Crime and Federal Government Surveillance
Of the House Judiciary Committee
Hearing titled "Fixing FISA: How a Law Designed to Protect Americans Has Been Weaponized Against Them"
April 27, 2023

Thank you, Chairman Jordan, Chairman Biggs, and Ranking Members Nadler and Jackson Lee for inviting me to testify before you today regarding Section 702 of the Foreign Intelligence Surveillance Act ("FISA"). On behalf of the Privacy and Civil Liberties Oversight Board ("PCLOB"), I am grateful to be here today, and I commend this Committee and your Staff for its attention to this very important law, months before a potential reauthorization deadline.

Before I begin, there are a few caveats to my testimony today. First, I am only one Member of a bipartisan, five-Member Board, so I am speaking in my individual capacity as a Board Member, and not for the Board as a whole. Second, I want to note that we are currently working on an extensive report, updating the Board's 2014 Report on the Section 702 program. We anticipate that this report will explain the program in as complete and unclassified a manner as possible; that it will provide analysis both of its privacy and civil liberties implications and of the value of the program to our national security; and that it will provide further recommendations going forward. On that last point, the report – and the Members' discussions and deliberations – are very much still in process, so out of respect for my fellow Members and our discussions, (as well as the fact that we are still receiving new information, much of which is classified), I will be somewhat limited in what I can opine on at this time.[1] Third, I note that our forthcoming report is

[1] Although the Board has not yet completed our Section 702 report, we can already say that we agree that three things are true: Section 702 is valuable in protecting our national security; Section 702 creates risks to privacy and civil liberties; and these risks can and should be addressed without undermining the core value of the program. We are

focused on the program operated pursuant to Section 702, which is due for reauthorization in December, not on FISA as a whole, and not on the Title I authorities. So I would defer to my co-panelist, Inspector General Horowitz, on questions beyond Section 702.

I am, however, deeply concerned, as I know are many of the members of this Subcommittee and others in Congress, regarding FBI misuses of its authority. There must be no repeat of the egregious violations of law and policy committed during the investigation of alleged Russian interference in the 2016 election campaign of former President Trump.

Furthermore, although those violations occurred under a separate section of FISA that governs investigations of U.S. citizens, the Intelligence Community has not been faultless in its application of the Section 702 program either. Indeed, it is evident that many queries of information about U.S persons were run against 702-collected information, specifically by the FBI, in conflict with governing policies and procedure. This is unacceptable, and must be acknowledged and addressed. The FBI has taken some steps to remediate this problem going forward. I anticipate that the Board's forthcoming report will detail some of the significant compliance incidents, and will make further recommendations to the FBI and to the Intelligence Community as a whole.

Having said that, I would like to spend a few minutes this morning clarifying a few points about the program. To begin with, Section 702 permits the U.S. Government to target non-U.S. persons outside the United States, and the targeting must be conducted to acquire foreign intelligence information. If you are physically located in the United States, or if you are a U.S. person abroad, you may not be targeted.

---

confident that the privacy risks posed by Section 702 can be addressed while preserving the program's value in protecting Americans' national security.

Also important, Section 702 is ***not*** a bulk collection program. Instead, the program consists entirely of targeting specific non-U.S. persons abroad about whom an individualized determination has been made that they are reasonably likely to possess, receive, or communicate foreign intelligence information. That intelligence information has led to the discovery of previously unknown terrorist plots directed against the United States and our allies, enabling the disruption of those plots. It has assisted and protected our troops abroad. And it has been used to identify, and to allow the United States to mitigate or prevent multiple foreign attacks on our critical infrastructure. There can be no question that the program is extraordinarily valuable to the safety and well-being of Americans.

In contrast to some of the querying compliance issues that I expect we will discuss further, we also have not seen significant compliance problems with regard to the ***collection*** of information. Indeed, in the most recently released Joint Assessment of the program, the NSA targeting compliance incident rate was 0.08 percent, not including notification delay errors. During the same reporting period, the FBI targeting compliance incident rate was 0.007 percent. These low rates have been fairly constant. This means that the Intelligence Community is largely avoiding improper collection under existing law and policies—that is, they are not improperly targeting U.S. persons or persons reasonably believed to be located in the United States.

As you are deliberating on how to improve Section 702 going forward, I would like to offer two topics for your consideration:

First, what the FBI considers "sensitive queries" are crucially important. When you get at the heart of what most worries concerned citizens, it is that the Intelligence Community will be weaponized against politically disfavored opponents. That is unacceptable in a democracy, and must be guarded against. Recently, and belatedly, the FBI put in place procedures that require

heightened review for certain queries, such as those involving elected officials, members of the media, and religious figures—in the most sensitive cases, review by the Deputy Director of the FBI personally. Congress should look closely at these enhanced pre-approval policies, and consider whether this requirement might be codified, strengthened, or reviewed by the Foreign Intelligence Surveillance Court (FISC).

Second, Congress might consider how Section 702-derived information could be used in the context of vetting – both for immigration purposes, and for individuals applying for high-level security clearance. Currently, for most agencies, a query of unminimized 702 data is permitted only where the search is "reasonably likely to retrieve foreign intelligence information."[2] This means that the U.S. Government may already have in its possession information that a visa applicant or person applying for a high-level clearance poses a threat to our national security or is in communication with someone who does. But no one from our government might ever see this information, because our agents and analysts cannot run a query for it in the unminimized 702 collection unless they first have specific information tying that applicant to foreign intelligence information or evidence of a crime. If Congress wants to ensure that persons coming to live and work in our country, or persons entrusted with our most important national security information, are thoroughly vetted against information already in the Government's possession, it might consider looking further into this issue.

In closing, as the Chair stated, the Board was created by Congress based on a recommendation of the 9/11 Commission. In recommending creation of the Board, the Commission explained, "The choice between security and liberty is a false choice, as nothing is more likely to endanger America's liberties than the success of a terrorist attack at home. Our history has shown us that insecurity threatens liberty. Yet, if our liberties are curtailed, we lose the values that we are struggling to defend."

Thank you, and I look forward to your questions.

---

[2]https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_Cert_NSA%20Querying%20Procedures_10.19.2020.pdf

Mr. BIGGS. Well, thank you so much, and we look forward to—well, I've read your statement. I'll review it again.

Ms. WILLIAMS. Thank you.

Mr. BIGGS. Thank you. With that, we're going to proceed now under the five-minutes rule for questions.

The Chair recognizes the gentleman from Florida, Mr. Gaetz.

Mr. GAETZ. Good to see you again, Mr. Inspector General. We appreciate you and all the great members of your team. I want you to know we do read your reports. Just yesterday, I was questioning the ATF Director about why they weren't following some of the recommendations you put forward, and noted that work is appreciated.

I also take note of our distinguished Ranking Member's call for this FISA reform to be bipartisan and to be nonpartisan, which at times are two different things. I think it is thoughtful and mature, and I will do all I can to resist the temptation to frequently point out that the very political weaponization that Ms. Williams testified about is often directed against Republicans.

Based on the Ranking Member's solemn, and I think thoughtful, advice, we'll try to avoid seizing on that point as frequently as we might otherwise.

I want to get into the 3.4 million backdoor searches that the Ranking Member pointed out in his opening statement.

Mr. Inspector General, how should the public think about those?

Mr. HOROWITZ. Well, I think what we've seen in the various public reports—and I'm limited in what I can say about what's public, which I think is one of the issues, by the way, that's worth talking about, is transparency here—it's, obviously, very concerning that there's that volume of searches, and particularly, concerning the error rate that was reported on in the last two years in the public reporting. Now—

Mr. GAETZ. That error rate was what?

Mr. HOROWITZ. I believe it was around 30 percent. I think—fellow members? I think it's around 30 percent.

Mr. GAETZ. Well, 30. Yes, I'm a lawyer, not a mathematician, but 3.4 million, about 30 percent, you're talking about seven figures of error in terms of these searches. I'm wondering, how many people can perform these backdoor queries?

Mr. HOROWITZ. I'm going to defer to board members, because you have the review ongoing.

Ms. BRADFORD FRANKLIN. I'm afraid I don't have those figures at my fingertips in terms of the number of people that can conduct those types of searches. I share the concern expressed in the question that we need to have greater safeguards, and I urge Congress to incorporate a requirement for FISA Court review of these kinds of searches to protect Americans' Fourth Amendment rights.

Mr. GAETZ. There are 3.4—you had 3.4 million backdoor searches, more than a million of them in error. If I represent to you that we believe there may be north of 10,000 people in the Federal government that can perform those queries, would anyone here have a basis to disagree with that assessment?

Mr. HOROWITZ. No.

Mr. GAETZ. So, FISA is unique in our jurisprudence because it's not an adversarial process. Most of us think about justice, where

there's a lawyer on one side, a lawyer on the other, and then, a judge or a jury makes the decision. Here in FISA, you've got just one team and the referee, and you don't have a defense attorney or an advocate there to point out these things.

Given that FISA isn't adversarial, how does that increase the importance of the Department of Justice taking the recommendations of the Inspector General, as you've laid out over the years?

Mr. HOROWITZ. Congressman, I think it's critical. You're exactly right. That is one of the concerns we saw in the Title I work we did on the Carter Page FISAs, which is, to some extent, the FISC is relying—well, it is relying entirely on what the government tells it. So, in some respects, it's unfair to look to the FISC to try and do the kind of work that, as you noted, a defense lawyer would do.

I was a Federal prosecutor. I was a defense lawyer as well. There's a search for the truth—

Mr. GAETZ. Again, I'm a little annoyed they don't hold the Federal prosecutors in contempt who come before them and don't present complete evidence if that happened.

Mr. HOROWITZ. I'll just say, on the Carter Page FISAs, one of the problems that we found, and one of the serious problems we found, was the FBI was sitting on information and it wasn't telling the prosecutors that information.

Mr. GAETZ. See, if I was in a civil litigation environment in North Florida, and I was withholding evidence that the other side had a right to, I would expect a judge to sanction me. I know you don't oversee the court, but perhaps a message that they would absorb.

Speaking of messages to absorb, we have this nonadversarial process. We have these 3.4 million backdoor queries, more than a million of them in error. It just doesn't seem like DOJ is listening and they are as quick on the uptake as they should be.

In 2019, you write a 470-page report detailing the problems. In 2020, you publish a management advisory that lays out the problems. In 2021, you lay out additional reforms. It seems as though every time you write a report, and then, the DOJ comes in and tells us that they now have fixed everything and have seen the light. Then, you write another report showing that there hasn't been sufficient compliance. I know there's a report coming after this hearing, but I think that just continues the cycle until we constrain these authorities.

Mr. BIGGS. The gentleman's time has expired.

The Chair recognizes the gentlelady from Texas, the Ranking Member, Ms. Jackson Lee.

Ms. JACKSON LEE. Thank you very much.

Good morning.

Ms. Franklin, when Congress reauthorized FISA in January 2018, we added a provision requiring the Attorney General to develop procedures for querying information in the 702 data base, to be reviewed by the FISA Court as part of its annual certification. Can you explain why having clearly defined querying procedures can help protect Americans' Fourth Amendment rights?

Ms. BRADFORD FRANKLIN. Thank you for that question.

Yes, I agree that requiring specified querying procedures is important. Previously, the rules that applied to querying were con-

tained in minimization procedures. They have now been fleshed out and documented further, and we just had a release recently, this week, by the FBI, of a public version of their querying procedures. Having clarity can help prevent the kinds of compliance violations that we have seen.

However, I would urge that those are not sufficient. I believe that, in addition to having specified rules which are approved by the FISA Court, Congress should incorporate a requirement that individual queries be submitted to the FISA Court for review to ensure full protection.

Ms. JACKSON LEE. So, in any reform, you would add the individual queries as well for clarification and transparency?

Ms. BRADFORD FRANKLIN. Yes, and—

Ms. JACKSON LEE. Within the intelligence community?

Ms. BRADFORD FRANKLIN. Well, I think FISA Court review can—the individualized judicial review is important because in this program we do not have individualized judicial review at the front end. So, when we are looking—when analysts are looking for the information about specific Americans who have recognized Fourth Amendment rights, to have the judicial review at that point.

Ms. JACKSON LEE. Thank you.

Inspector General Horowitz, in the 2018 reauthorization of Section 702, Congress made some small changes to the law to attempt to protect U.S. persons whose communications may be swept up in 702 collections. One of the changes was to impose a limited warrant requirement for U.S. persons who are the subject of an open criminal investigation. How has the warrant requirement been used in practice? What impact?

Mr. HOROWITZ. Let me get back to you on that. I want to make sure that I'm fully informed on that. I have not looked at that recently, and I want to be careful on how much I can say in a public forum at this point.

Frankly, one of the challenges in talking about the use of these tools is how much remains classified and how only in the last recent months have we seen information coming forward. So, I need to get back to you, if I can, on that, Congresswoman.

Ms. JACKSON LEE. I want to take a leap, but you notice that I mentioned the young airman. As I recall, what is in the public domain is that there may have been some foreign contacts that may come to our attention.

How would—we're all appalled at that. I'll just take a brief moment on that before I ask Ms. Franklin a very quick question. We're all appalled at that.

So, I want to just frame what we need to do to secure 702. Just give us, if that was the case, and if there was a need to engage, how the 702 would be utilized.

Mr. HOROWITZ. So, I think the important one—I'm not going to talk about any specific case.

Ms. JACKSON LEE. Yes.

Mr. HOROWITZ. As a general matter, what you mentioned is the need to get a warrant in certain circumstances. That requires a court. You don't self-issue a warrant. That creates the oversight process that, I think, the Chair is referencing more broadly, as a

means by which there would be further court review in other areas as well.

I won't speak for the Chair, but—

Ms. JACKSON LEE. I have a question for her. She can follow-up on that, if she desires. Let me, let me do the question.

I think I just want to get to the point. It wouldn't be willy nilly, if I may use that terminology. The FBI needs to well document—

Ms. BRADFORD FRANKLIN. It depends what they're trying to do, I think is the right answer on that one. I don't know if—

Ms. JACKSON LEE. Well, she can—let me pose this question. Then, you might want to expand. Is it clear whether the small changes in the 2018 legislation reauthorizing Section 702 have improved the administration of Section 702?

Ms. BRADFORD FRANKLIN. Thank you. I believe there have been some benefits, as I had just discussed, regarding the requirement for querying procedures that has helped, but I do not believe that those changes were sufficient, and I urge Congress to incorporate more robust and meaningful safeguards, just as the three that I mentioned during my opening remarks, including requiring account of the extent of incidental collection; requiring FISA Court review of U.S. person query terms, and preventing the restarting of "abouts" collection.

Ms. JACKSON LEE. I thank the witnesses.

Mr. BIGGS. I thank the gentlelady.

With that, I recognize the gentleman from Wisconsin, Mr. Tiffany.

Mr. TIFFANY. Thank you, Mr. Chair.

Mr. Inspector General, and all of you, good to see you here today.

You referenced Carter Page, and the third authorization to spy on him, and there was a lie that was told to the FISC by former FBI Attorney Kevin Clinesmith. He ended up getting a sentence of 12 months' probation, 400 hours of community service.

Now, over the last week, it has been exposed, as a result of the work of the leadership of this Committee, that the Secretary of State colluded with the intelligence community to lie to the American people about Hunter Biden's laptop.

How effective will the reforms of Section 702 be if we can't trust our intelligence agencies? Justice, the FBI, NSA, can we trust them to reform?

Mr. HOROWITZ. From my standpoint, I think it's all about verifying and controls and oversight. You have to build in the appropriate controls for these programs. I think we've seen over the years, despite, as the Ranking Member just indicated, changes that have helped improve the process, they clearly haven't been sufficient.

Mr. TIFFANY. Do you have a couple of mechanisms that you suggest that should be added?

Mr. HOROWITZ. Well, I think one of the things that clearly has been talked about is what the Chair just mentioned about more—greater oversight by the FISC, by the Foreign Intelligence Surveillance Court, of various authorities under 702.

I think there needs to be greater transparency. I think this notion that we did a review recently of the FBI's Office of the General Counsel and how it interacted with NSD and in the course of that

we found they had two differing views of what the querying standard was for 702 queries. That's highly problematic. We would not have known that, the public wouldn't have known that unless we did our report. Having greater clarity, clear rules, public transparent rules rather than having this come up on the eve of every reauthorization where there all the sudden seems to be more and more transparency.

Mr. TIFFANY. Thank you.

Ms. Franklin, Ms. Williams, you can both—either of you can take a shot at this. Should we be taking a hands-off approach as the Judiciary Committee to this issue?

Ms. BRADFORD FRANKLIN. No, Congressman, you should not be taking a hands-off approach. I am encouraged that this Committee is starting its consideration of Section 702 now with the upcoming sunset at the end of this year. I'd like to agree with the comments made by the Inspector General. It's important to pair reforms with rigorous oversight, by Congress, by the Inspector General, the PCLOB, and others.

Mr. TIFFANY. So, why don't I just follow-up with my next question then, Ms. Williams. So, we hear the sky is falling from some if 702 goes away. Isn't there a backup to that?

Ms. WILLIAMS. Congressman, I wish there were. It's not like the intelligence community doesn't have other authorities, but I don't think this specific authority allows and puts actually some privacy safeguards, but I agree not enough on the collection of information.

I would just say also I think you really put your finger on it with your last question because you said should we trust? Obviously, there's a long way to go to regain trust. From my perspective as an oversight body I feel like it's not my job to trust. It's our job to look at what's actually going on, to put strong guardrails in place and to recommend them to all of you.

Mr. TIFFANY. Are you familiar with Executive Order 12333?

Ms. WILLIAMS. I am.

Mr. TIFFANY. Yes. Would that provide more or less protection than 702?

Ms. WILLIAMS. Well, it provides a different set of protections. It involves foreign collection overseas. It wouldn't apply with regard to communications that are traversing U.S. soil.

Mr. TIFFANY. Mr. Horowitz, do you care to comment on that?

Mr. HOROWITZ. Well, one is a Presidential Executive Order; the other is a statute. They are in two different spaces, but from my standpoint having a clear congressional decision and statute is preferable than having internal guidance that—an Executive Order is public, but what we've seen mostly in 702 is internal guidance and querying standards that, for example, were not public, the most recent ones, until the last few days.

Mr. TIFFANY. Thank you. I think there is a broader question here. Is the FBI's fixation on politics undermining crime fighting in America? I think about the Parkland shooting. Horrible incident down in Southern Florida. The FBI was warned about that. Are they misallocating resources at this point? Are they so focused on politics that they are not fighting crime in America which this Committee has shown very capably that we have a crime epidemic in America?

I yield back.

Mr. BIGGS. The gentleman's time is expired.

The Chair recognizes the gentleman from New York, Mr. Nadler.

Mr. NADLER. Thank you, Mr. Chair.

Ms. Franklin, the Chief concern that everybody here seems to have is the incidental collection of information about American citizens when we are targeting a foreign citizen abroad. Why is it not feasible to require that all that information immediately be destroyed, that the name of the American be removed and that all references to whatever he or she said also be removed?

Ms. BRADFORD FRANKLIN. Thank you for that question. Incidental collection is a recognized feature of Section 702 collection. Of course it is targeted at non-Americans located overseas, but part of what has been authorized; and an important role the intelligence agencies would tell you, for that collection is when those people are talking to people inside the United States to be able to identify them and know if they are working with our valid 702 targets to plot or otherwise pose a threat to the United States.

Now, of course, once we have identified those Americans in the 702 collection, it then becomes incumbent on the intelligence agencies and with assistance from Congress to have those robust safeguards like FISA Court review. At the outset the fact that somebody is talking to a foreign overseas target—to be able to identify those potential threats inside the United States is a feature of this program that is known and recognized and not necessarily the problem. It's only when they start to focus in on the American that we need to ensure we have those safeguards.

Mr. NADLER. What do you mean when they start to focus in on the American?

Ms. BRADFORD FRANKLIN. At the point they're conducting U.S. person queries, when they are looking to find what is going on with a particular American and they want to search through the data. At that juncture that is where we are implicating the Americans' Fourth Amendment rights.

Mr. NADLER. So, why do we not prohibit that unless they get a search warrant?

Ms. BRADFORD FRANKLIN. Exactly. That is—I urge that.

Mr. NADLER. That is not in the current law?

Ms. BRADFORD FRANKLIN. Correct.

Mr. NADLER. OK. In April 2016, I signed a bipartisan letter to ODNI Director James Clapper requesting a public estimate of the number of communications or transactions involving U.S. persons subject to Section 702 surveillance on an annual basis. Seven years later that number has still not been provided.

Inspector General Horowitz, has DOJ or FBI reported this number to you and are you prepared to share this today?

Mr. HOROWITZ. They have not reported it to me.

Mr. NADLER. Can you get that information?

Mr. HOROWITZ. I will follow-up with them, but my understanding is the position has been that it would be impossible to come up with an accurate number, which I find concerning.

Mr. NADLER. Yes.

Ms. Franklin, do we have any idea of the quantity of American data collected through Section 702 surveillance each year?

Ms. BRADFORD FRANKLIN. We do not, and I urge Congress to require that they provide such an estimate. Even if it can't be as mathematically precise as some of the other numbers they produce, I believe it still can be meaningful to Congress as you assess whether safeguards are adequate under Section 702.

Mr. NADLER. Thank you.

Ms. Williams, in the PCLOB's 2014 report which we referenced in the letter PCLOB recommended that the NSA annually count certain communications including telephone communications in which one caller is located in the United States, Internet communications that originate or terminate in the United States, and communications concerning U.S. persons. Has the NSA provided you with these numbers?

Ms. WILLIAMS. Congressman, the NSA has not provided us with these numbers because it is their position that it is infeasible or would cause other privacy concerns, but that is something that we are actively looking at. We are looking at—there's one paper, in particular, that I'm thinking about with regard to Princeton University they put out, and we're looking at different methods of ways that perhaps they could do it in a privacy protective way. I expect that we'll encourage them to consider those methods.

Mr. NADLER. Thank you.

Ms. Franklin, after Section 702 data is collected by the NSA certain sections are made available to intelligence agencies. The 702 data base often includes the communications of Americans swept up in 702 surveillance. Do we know who at the FBI has access to that information and what safeguards if any exist to limit the number of people with access to the 702 data base?

Ms. BRADFORD FRANKLIN. The FBI does have in place requirements that agents undergo training on an annual basis to maintain their access to 702 data. So, there are some safeguards in place in that regard, and I think that is important.

Mr. NADLER. Thank you very much. I yield back.

Mr. BIGGS. Thank you.

The Chair recognizes the gentleman from Texas, Mr. Nehls.

Mr. NEHLS. Thank you, Mr. Chair.

Thank you, Inspector General Horowitz. I served in law enforcement for 30 years, as a sheriff for eight of a large county. We served hundreds of warrants, if not thousands throughout my years in law enforcement, and I can tell you to obtain a warrant we had to find a judge, we had to establish probable cause. if you didn't meet that threshold, the judge wouldn't give you the warrant. Reasonable suspicion didn't meet the standard; it was probable cause. This I agree with because I think it was there—the whole purpose was to protect people in their Fourth Amendment right.

Can you explain the process the FBI uses to obtain a FISA warrant specifically? What is required to show probable cause?

Mr. HOROWITZ. So, on the Title I side of FISA, when they're going to seek a warrant like they did in the Carter Page circumstance, they need to show that there is sufficient evidence, probable cause to believe that the individual they're seeking the warrant against may be an agent or could be an agent of a foreign power.

Mr. NEHLS. Yes. I want to talk about the illegal surveillance of Trump campaign associate Carter Page, and I want to thank you for you and your investigative report, which found that the FBI had abused its FISA authority on several occasions to conduct illegal surveillance on Page, Mr. Page. This was and continues to be critical for our oversight. Here is the article, *Washington Examiner*, "DOJ Inspector General Finds 17 Significant Errors or Omissions in Carter Page FISA Applications."

You know when I go through this timeline and when you look at Mr. Page—for those of you that may not be familiar with some of these characters, you have got Carter Page, you have got Kevin Clinesmith, Peter Strzok, Lisa Page, Christopher Steele, the dossier, and Stuart Evans.

This Carter Page was a great American. In 1993, he graduates from the Naval Academy, he serves in the Navy five years, worked as an intel officer before rising to the rank of lieutenant. In 2000, he goes to work for Merrill Lynch in London. In 2004, Merrill Lynch promotes him to Deputy Branch Manager in Moscow. He leaves Merrill, becomes an International Energy Consultant based in New York and travels primarily from London to Moscow. The CIA begins debriefing Page about his contacts with Russians in 2008. So, he has a relationship now. He is being interviewed. The CIA is interviewing him. CIA is sharing information with the FBI.

In 2013, Russian agents posed as bankers approach Page in New York, that energy symposium and try to cultivate him as a source for economic information. The FBI, in April 2013, records it. They record it. Russians are complaining because Page didn't want to agree, didn't want to cooperate with them. In June that same year the FBI interviews Mr. Page again and reveals that he has spoken with the CIA. So, they are all talking. This is good. The Federal agencies are talking to each other.

Page agrees to cooperate as a key witness against this Russian agent and the agent gets found guilty; sentenced him to 30 months in prison.

Then this is where it goes wrong. This is where it happens. Then all of a sudden Page then starts working for Trump and that is where these individuals: Christopher Steele, the former British intel agent—he brings the Steele dossier together. Hilary Clinton hires Fusion GPS to dig up the dirt on Trump. This is the problem we have. We can see that it was all out there to go after Trump, to dig up dirt on Trump.

The FBI knew Page was a credible man, but they ignored all this. They get warrant after warrant after warrant and we take it all the way up through 2017 and then eventually they find out Mr. Page didn't do anything wrong. They sentence Mr. Clinesmith. I didn't think they gave him enough time. They sentence him to 12 months' probation and 400 hours of community service.

When you look at what happened to Mr. Page because he joined the Trump team, Mr. Page's previous years of serving his country, doing a great job, cooperating with the FBI and the CIA, they turn this guy now into some type of a villain, some type of a Russian agent, all in the name of what? To go after Trump and the Trump campaign, to make Trump look like he was in collusion with the Russians.

I don't have time to go through the whole story, but what safeguards have been in place, what safeguards have been in place to ensure this doesn't happen in the 2024 election especially given that Donald Trump is the leader of the Republican Party? What are we going to do?

Mr. HOROWITZ. So, we made a series of recommendations in both our review of the Crossfire Hurricane matter and the Woods review that we did. We have a series of recommendations. Most of those have been addressed, but not all of them. We continue to follow-up to make sure what has been done is being implemented effectively and works.

Mr. NEHLS. Thank you. I certainly hopes so. God bless our country. I yield back.

Mr. BIGGS. Yes, thank you.

I recognize the gentleman from Rhode Island, Mr. Cicilline.

Mr. CICILLINE. Thank you, Mr. Chair.

I want to thank the witnesses for being here today to testify and to answer our questions about this very important issue.

With Section 702 set to sunset at the end of this year it is vital that we have these discussions before we take our next steps. Over the last few decades the national security landscape and warfare have changed dramatically. War is not just fought on the grounds with troops and artillery anymore. In fact it is more and more rare that we see this traditional warfare alone.

Now, it is cyber warfare fought by enemies that don't ever have to physically enter the United States or even see an American soldier or citizen to cause grave harm. Entire societies can be shut down by a cyber security threat. Computers are now a battlefield of choice for terrorists. This makes strong reliable intelligence perhaps more important than ever before. Moreover, with mass atrocities still happening across the world, with war criminals committing grave human rights violations intelligence gathering is vital to a strong response.

For example, last week Deputy Attorney General Monaco testified before the Senate Judiciary Committee that Russia's forces committing shocking atrocities as part of its brutal and unprovoked invasion of Ukraine, and that some of this intelligence was being gathered that today—that is being gathered was gathered in connection with some of the authorities that we are discussing today.

With that said, it is more important than ever that we ensure that our civil rights are protected as our national security agencies gather this intelligence. Our civil liberties are not currency. They are not a price we pay for national security. They are sacred and fundamental to our society and we must ensure they are protected to the fullest extent.

I think we all recognize that information that gets swept up by these searches, particularly, in the 702 data base and the way they are accessed can present some real challenges. So, I would like to pick up where Ranking Member Nadler left off talking about just how much U.S. person data is swept up in 702 surveillance.

Inspector General Horowitz, is there any indication that the intelligence agencies have even tried to track the quantity of U.S. person communications that come in through 702, even a general estimate, for last year for example?

Mr. HOROWITZ. I don't have information about the other intelligence agencies. We only oversee the FBI. I'm not aware of data from the FBI on what the numbers look like today.

Mr. CICILLINE. Ms. Franklin, should U.S. data be collected going forward; that is, U.S. person data? If so, what additional procedures should be in place to make that happen, or before that can happen?

Ms. BRADFORD FRANKLIN. Thank you. I'd also like to address the—

Mr. CICILLINE. Yes.

Ms. BRADFORD FRANKLIN. —piece of the question about what they have done. So, the intelligence agencies have briefed I believe Members of this Committee as well and us on several techniques that they have considered to calculate the quantity of U.S. person information. They have asserted that is infeasible to calculate a meaningful number, however I believe that the difference is in what is meaningful. They are thinking of mathematical certainty and where the alternative is, that we have no estimate whatsoever. An estimate that involves some margin of error can still be meaningful, which is why I urge Congress to require them to produce such an estimate.

With regard to the incidental collection, as I was stating in my earlier response, at the outset knowing who valid foreign targets are talking to, including if they are talking to people inside the United States, is an important feature of the program. However, it is at the juncture where the intelligence agencies want focus in on a U.S. person and search through the collected data, looking for their particular communications that I believe it is important to protect those Americans Fourth Amendment interests and their communications. Congress should incorporate a requirement for FISA Court review of those U.S. person queries.

Mr. CICILLINE. Finally, is there any reason that with respect to the second category; that is, information that relates to a U.S. person query that currently doesn't require judicial review or a finding of probable cause, or even a review by a court? Is there any reason for that query when it involves a U.S. person that you simply—we couldn't simply impose statutorily a probable cause requirement or judicial review requirement like every other citizen in the United States and every other search context?

Ms. BRADFORD FRANKLIN. I believe Congress certainly has the power to impose that requirement. I'm urging Congress to do so—speaking personally for myself as board member, to do so in this reauthorization.

Mr. CICILLINE. Do you agree, Mr. Horowitz?

Mr. HOROWITZ. Congress certainly has the authority to do that and I think that's one of the key issues for this Committee and the Congress to consider.

Mr. CICILLINE. Do you think that is a responsible action for Congress to take?

Mr. HOROWITZ. I would say that I think what you'll hear from the department and the FBI is the question of the volume of cases, and probably from the FISC as well, which is you will need to consider the volume of the work that would increase for the FISC and how you address that.

Mr. CICILLINE. We are happy to pay for—provide additional resources—

Mr. BIGGS. The gentleman's time is expired.

Mr. HOROWITZ. That is the question.

Mr. CICILLINE. Thank you. I yield back, Mr. Chair.

Mr. BIGGS. Thank you, Mr. Cicilline.

I recognize the Chair, Mr. Jordan.

Chair JORDAN. Ms. Franklin, you testified you have no idea how many Americans are picked up in the incidental collection and the FBI won't tell you or won't even give you an estimate what that number may be. Is that right?

Ms. BRADFORD FRANKLIN. That's correct.

Chair JORDAN. You have no idea the amount of data collected on American citizens and the FBI won't tell you or give you an estimate on that either?

Ms. BRADFORD FRANKLIN. The intelligence agencies have asserted that it is infeasible for them to calculate a meaningful number and they have not done so.

Chair JORDAN. Then 10,000 people, approximately 10,000 people at the Justice Department have the ability to query this incidental collection data base without any probable cause. We know as the Ranking Member of the Full Committee, Mr. Nadler, said earlier, "there were 3.4 million queries of this data base and 30 percent of those were in error." Is that all right?

Ms. BRADFORD FRANKLIN. I don't have at my fingertips all those number, but I do recall specifically the 3.4 million number of queries conducted in the prior calendar year.

Chair JORDAN. The solution is simple, right? Require probable cause if you are going to query this data base on American citizens?

Ms. BRADFORD FRANKLIN. As I have stated, I urge Congress to require that the FISA Court review those U.S. person query terms before they—

Chair JORDAN. Ms. Williams, do you agree?

Ms. WILLIAMS. Well, Congressman, that's something that we're looking at right now. I think you put your finger on it, which is that you want to increase privacy and civil liberties as much as possible for U.S. persons. The pros of that is that it would make it harder to run a U.S. person search. The con of that is it would make it harder to run a U.S. person search. So, there's a balance there.

Chair JORDAN. Americans are being picked up in this incidental collection. We don't know the number. My guess it is pretty darn big. They won't tell us. Without probable cause that data base is being searched 3.4 million times with all kinds of error rates, as Mr. Gaetz in his round of questioning determined earlier.

How about if we just get the FBI out of the business altogether?

Ms. WILLIAMS. I think the question is should—

Chair JORDAN. What if the FBI can't query this data base? In other words, you can't query—don't even mess with the—FBI can't query this data base on American citizens.

Ms. WILLIAMS. Look, the FBI has a long way to go to regain public trust. The question is, I think if the FBI is not doing these searches to figure out who in the United States is talking to terror-

ists abroad, who is going to do it? So, the concerns are real and the—

Chair JORDAN. Well, who is going to do it? We got other agencies that do it already.

Ms. WILLIAMS. Well, we have agencies. Do you want to—there's a risk of turning the CIA or NSA, who look outward, inward on Americans. We don't want to—

Chair JORDAN. We are not allowed to do that.

Ms. WILLIAMS. Right. Exactly.

Chair JORDAN. The CIA is not allowed to do that.

Ms. WILLIAMS. Exactly.

Chair JORDAN. We are not going to change that.

Ms. WILLIAMS. Exactly.

Chair JORDAN. No way.

Ms. WILLIAMS. Right.

Chair JORDAN. I mean this Committee—you guys are on the Privacy and Civil Liberties Board. That is what the main function of this Committee, the Judiciary Committee, is to protect the Constitution, protect the Bill—that is our fundamental responsibility. Section 702 is up for—this the most important thing we are probably going to do this Congress, get this right, not let it continue with the data that you all understand. That is our focus, should be our focus this—and the fact that I think we can get bipartisan—we can get agreement here on protecting those liberties I think is just so—

When is the report going to be ready? Many of you have referenced that. I think all three of you referenced it in your opening statements. When is that coming?

Ms. BRADFORD FRANKLIN. Not able to give you an exact date. We are working hard. There's a lot of complex information at issue.

Chair JORDAN. Well, let me ask this question: Is it going to be ready before December 31?

Ms. BRADFORD FRANKLIN. Yes.

Chair JORDAN. OK. That is important. We are working on this now. I want to thank the Chair for calling this hearing. This is something we had a—all Republicans met yesterday. We had a one-hour meeting on this issue alone. We are trying to figure out exactly what is best to protect Americans' privacy rights, their fundamental freedoms. The sooner we get that report; I think that is helpful information, the better. Any idea again.

Ms. BRADFORD FRANKLIN. We're aiming for the summer.

Chair JORDAN. Sooner the better.

With that, Mr. Chair, I yield back. Again, I thank the Chair for putting this hearing together.

Mr. BIGGS. I thank you, Mr. Chair.

With that, we are going to go into recess until the sound of the gavel so that people can go to the Joint Session of Congress. With that, we are in recess.

[Recess.]

Mr. BIGGS. The Subcommittee is called to order. We expect other Members to be coming back and joining us momentarily.

At this point, I thank the witnesses. Let the record reflect the witnesses are all back. You are still under oath. We are still in the five-minutes rule for questioning.

With that, the Chair recognizes the gentlelady from Florida, Ms. Lee.

Ms. LEE. Thank you, Mr. Chair.

FISA is intended to be an important tool in gathering foreign intelligence information designed to give law enforcement a way to promote national security and keep our homeland safe from foreign threats. It is a great responsibility to have a surveillance technique that exists outside of the standard public parameters of our courts and search warrant procedures and incumbent on all of us to ensure that when that process is used, it is used judiciously and always within the parameters of the law.

We know that certain actors in our own government have instead used FISA and Section 702 to conduct warrantless surveillance of Americans, going against the ostensible purpose of collecting information on non-U.S. persons and gathering foreign intelligence information.

I have the utmost respect for our law enforcement officers and our intelligence agencies when they are using the tools afforded to them by law to keep Americans and our country safe. We must carefully consider the use and the continuation of these powers in the face of evidence of overreach and abuse.

Ms. Williams, I would like to start with a question for you, going back to something that you mentioned in your opening that actually relates to how we can be making constructive use of some of the information that we have that we may not be already doing. That is, you specifically mentioned background checks, security clearances, and immigration related matters. Would you please elaborate on how you think we could be using information constructively within the law?

Ms. WILLIAMS. Well, thank you very much, Congresswoman.

I think this is a really important question, because one of the things that I think a lot of the American people don't realize is that this information may be about a clear and present danger of persons to our national security is already within our knowledge. The government may have already collected that information. They can't run, our agents and analysts can't run searches in the data base of this information unless they have a reasonable belief that they will find foreign intelligence information with regards to that query.

So, one idea for Congress to consider is for visa applicants or for people who are applying for high-level clearances to require them, when they apply for these things, to consent to these searches, so that you don't have to have a particularized reason to run that search. You can ensure that these are people who are not talking to foreign terrorist targets overseas, not in communication with those people, not in concert with those people before they enter our shores and come to work in our country.

Ms. LEE. Now, I also want to just follow-up generally. When it is being used properly, with whom is 702-acquired information shared?

Ms. WILLIAMS. So, 702-acquired information is shared basically on a need-to-know basis. So, if an agency, if an agent runs a query for a purpose, that information can be communicated to other intelligence agencies who may have a need to know that for their own

either domestic law enforcement purposes or for their own investigations.

Ms. LEE. In the conduct of your review and analysis of that information and its actual use in practice, do you have ongoing and continued concerns about whether that standard that you just articulated for us is being followed?

Ms. WILLIAMS. So, we are taking a look at it. Part of that is the minimization procedures, right, especially for U.S. persons. So, when there is a finished intelligence product, any U.S. person identifier would have to be masked.

I think one of the questions, one area Congress may want to look at and that we are looking at is are the masking guidelines appropriate or should they be tighter. So, if somebody wants to unmask an identity, should there be more transparency about when that happens? Should there be more guardrails about when that happens?

Ms. LEE. So, in particular, are there specific reforms or recommendations that you would make to us to help distinguish, to help confine appropriate use of the tool and also limit inappropriate, expansive overreach?

Ms. WILLIAMS. Absolutely. I think that is exactly what we are hoping to do as a board to provide these recommendations. Two of the areas that I mentioned in my statement, so the special investigative matters for congresspeople, for elected officials, journalists, religious figures, that I think is one ripe area, and the other vetting, but also unmasking I think are the areas that we would, some of the areas that we are focusing on as a board.

Ms. LEE. Thank you, Mr. Chair.

Ms. WILLIAMS. Thank you.

Ms. LEE. I yield back.

Mr. BIGGS. Thank you. The gentlelady yields back.

I yield time to myself, recognize myself for five minutes of questions.

So, I am going to begin with you, Mr. Horowitz. You mentioned earlier today that the FBI and DOJ lawyers had a different understanding of the querying standard. That is what I understood your testimony to be. That is a fairly significant revelation.

The FBI, which conducts the queries, didn't show the same understanding of the query standards as DOJ, who is supposed to give the FISC accurate information about how the FBI is using Section 702. What was the misunderstanding or what is the—or is it persistent? What is that misunderstanding?

Mr. HOROWITZ. It was differing interpretations of what evidence was, what the purpose was in going forward with the searches. They were both looking at the same language and having a different understanding of what the language was with regard to the querying standards. So, it wasn't they were making their own standards up. There was a standard there. They had differing views of what that was.

As we reported on it, it has since been addressed by the department in the querying standards that were released last week where it became, that were released publicly last week that were done well before that, that made it clear that, in fact, the NSD lawyers

were more correct in the approach they were taking than what the approach was of the FBI—

Mr. BIGGS. Are you telling me that it has been, you think it has been resolved then?

Mr. HOROWITZ. The dispute has been resolved with these new standards. What I can't tell you is how, yet, is how it is being implemented, because it is recent. That is one of the issues that we are planning to follow-up on, because, as you know, whenever we do these and release recommendations, we then follow-up to make sure that what we have been told has addressed it has, in fact, addressed it.

Mr. BIGGS. OK. So, well, we hope that it is solved going forward anyway.

Mr. HOROWITZ. Well, we hope that they are aligned in understanding it and that their understanding is reasonable and appropriate. That is the thing we are going to, that is what we will be asking questions about.

Mr. BIGGS. OK. I am going to ask—well, I will ask all of you this question, because part of the problem that I have always had with this is the FISC itself. There is a just a few judges. It is behind closed doors. There doesn't seem to be over review, no transparent review of whether the judges themselves are following the law appropriately.

What would you do to make or understand how to make the FISC work more appropriately to protecting Fourth Amendment rights and protections of U.S. citizens? I will start with you, Ms. Williams.

Ms. WILLIAMS. Sure. I think that is an excellent question, because you are right, there is not a lot of transparency around the FISC.

One of the things that has been done is the introduction of an amicus. That is someone who comes in. There is a few people to represent the interests of the other side so that there actually is an adversary process. One of the considerations, I will speak only with regard to 702, because that is what we are focusing on, is whether there should be an amicus appointed for the annual 702 certifications. Right now there is not. That is one of the potential recommendations that we are thinking about.

Mr. BIGGS. Thank you. Ms. Franklin.

Ms. BRADFORD FRANKLIN. So, I would like to build on that and just clarify. There is no requirement for the amicus to come in. Typically there is. That is not necessarily required for the FISA Court to appoint one.

I have done prior work on the issue of the amicus. Back in 2014, the Privacy and Civil Liberties Oversight Board, as part of its report on the Section 215 program, actually recommended something that the board then called special advocates. This preceded the codification by Congress of the requirement for the amici. It was stronger in recommendation than what ultimately became enacted in law.

So, I would continue to urge that, consistent with the original recommendations by the PCLOB, that the role of the amicus be expanded and strengthened to expand the number of cases, the types of cases in which they are required to be appointed, including Sec-

tion 702 and a recertification and sensitive investigative matters, also that they have access to all information relevant to the proceeding that they are participating in, and finally that they have the ability to petition for appeal to the FISA Court of Review or from there on to the Supreme Court.

Mr. BIGGS. Thank you. Mr. Horowitz, my time has expired. I recognize the gentleman from South Carolina, Mr. Fry.

Mr. FRY. Mr. Chair, I yield my five minutes to you for further questioning.

Mr. BIGGS. Thank you.

Mr. Horowitz, would you please continue with your answer?

Mr. HOROWITZ. I will. So, building on what my two fellow panelists mentioned, that is something that concerned us, the lack of an adversarial process in connection with Carter Page FISAs and that the problem being that agents when they swear out affidavits are likely never to have to face cross examination or any testimony that would be challenged by an adversarial party in that process, because it is not like a criminal case.

In a criminal case, having worked, again, as a prosecutor, you understand that at some point you are going to produce that to the defense, and if the case goes to trial or if there is a pretrial hearing, the agent may be under oath in a witness stand. That focuses the mind in making sure that you have got every detail and fact correct. So, I think that is very important.

I also would suggest considering how to make it more, as you referenced, transparent. How do we find out, how does the public find out sooner about decisions, about key findings? I think one of the challenges has been, much as it has been for our reports and my guess for the PCLOB's reports, is getting through the clearance process, the security review process, and how long it takes.

For example, our FISA report, we finished it in essence around Labor Day of 2019. It was released publicly on December 9, 2019. During almost all that time, it was in the classification review process, and exactly what was going to be able to be made public and what could not be made public.

Mr. BIGGS. OK. So, I hope that maybe you will include some of those recommendations for the FISC itself in your report going forward as well.

Ms. Williams, in your earlier testimony, and I wrote it and I had it right here before the recess, so I am going by memory, but I thought I jotted down something about the general collection process. I think you said it is not meant to be a bulk collection of data or information. It seems to be a bulk collection of data or information.

The question is U.S. citizens getting caught up in that somehow. I would like you to elaborate on how it has become, it is bulk. It is broad. Then how do we somehow get back? You guys, this is what the whole hearing has been about and you have talking about this. How do we get it so where U.S. citizens on U.S. soil are protected, because the intention of this is non-U.S. citizens not on U.S. soil?

Yes, you got to mic up.

Ms. WILLIAMS. Yes. So, that is exactly right. So, the reason I made the statement that it is not a bulk collection is because that

was what the PCLOB unanimously said in our 2014 report, "that this is not a bulk collection program." What that means is that before any collection can be done on any foreign person overseas usually the NSA has to do very detailed targeting to make sure that it is not a U.S. person, there is a foreignness determination, and to make sure that there is an expected collection of foreign intelligence information. So, every single person is targeted.

That is the compliance rate that I talked about that was low. There is a very—they are doing pretty well on that. Your question, which is then the people of, U.S. people who get caught up on that, the incidental collection are U.S. persons who may be communicating with those targets overseas.

Mr. BIGGS. So, I was fascinated by the statement you kind of threw offhand and you kind of did earlier when you testified to this. I would like everybody, we only have 48 seconds left, so to be fast. When you said the compliance rate was low on the bulk collection, I want to hear about that.

Ms. WILLIAMS. Yes, and I am sorry. I may have misspoken. So, the compliance error rate was low, which means that they are generally collecting in the way they should be collecting.

Mr. BIGGS. OK.

Ms. WILLIAMS. The query error rate is high, which is once the information is collected, are they searching the collected information appropriately? That is where there are more errors.

Mr. BIGGS. This is what we were talking about earlier. I think the actual query error rate was 3.2 percent. Is that what the actual query error rate is, 3.2 percent? Or would you please check, Mr. Horowitz, and verify on that? That would be—

Mr. HOROWITZ. Yes, it has dropped significantly.

Mr. BIGGS. OK.

Mr. HOROWITZ. I think that is where we are currently.

Mr. BIGGS. OK. Great.

Mr. HOROWITZ. Or the most recent data I should add.

Mr. BIGGS. Thank you so much.

I yield back to Mr. Fry.

Mr. FRY. I see my time has expired. I yield back, Mr. Chair.

Mr. BIGGS. The gentleman's time has expired.

Actually, no one else being present, I again thank the witnesses. We look forward to hearing from you, look forward to seeing your reports. I would urge the earlier the better, because we are really going to try to do something. We don't want to wait until the last minute. We want to make sure we have a good product that will result from some of your testimony. We will have additional hearings. Please, I think we have asked for some data. If you could please respond to that, that would be awfully kind.

With that, thanks again. We are adjourned.

[Whereupon, at 12:46 p.m., the Subcommittee was adjourned.]

The record for this hearing by the Members of the Subcommittee on Crime and Federal Government Surveillance is available at: *https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=115812*.

○