Statement for United States House of Representatives
Committee on the Judiciary
Subcommittee on Crime and Federal Government Surveillance
"A Continued Pattern of Government Surveillance of U.S. Citizens"
April 8, 2025

Thank you, Chairman Biggs, Ranking Member McBath, and distinguished Members of this Subcommittee. I'm delighted to be back testifying before the Subcommittee, and hope my testimony is helpful as, once again, you grapple with the reauthorization of Section 702 of the Foreign Intelligence Surveillance Act, or FISA.

As you know, the Judiciary Committee has a long, distinguished, and complicated history with this law. Since 9/11, this Committee has initiated legislation to give the executive branch the tools to enforce antiterrorism laws against the foreign terrorists that attacked us, while attempting to preserve Congress's ability to conduct vigorous oversight of the enforcement of the law. I served on the Judiciary Committee following the 9/11 attacks when Chairman Jim Sensenbrenner and Ranking Member John Conyers helped shepherd the PATRIOT Act through Congress. The goal was modernizing surveillance for critical intelligence priorities, while ensuring the Executive Branch was operating within the bounds of the law and respecting American's cherished civil liberties. I discussed that history and other legislative efforts in the testimony I delivered to the Committee almost two years ago, which is attached as an addendum to this written statement

As a private citizen, I now have concerns about how these laws are being implemented, and that the government agencies implementing them have strayed away from what Congress originally intended. The errors and overreach of the intelligence community in using FISA authorities are well-documented in a series of publicly available Inspector General reports and FISA court opinions and have also come to light as a result of Congress's oversight work.

One must also contend with a rapidly changing environment, particularly as technology advances. Today, Internet-enabled platforms connect almost everyone to an extraordinarily complex digital world, which captures users' personal data, records "likes," preferences, and "dislikes," and creates a personality profile for every digital user. Some firms compile and sell this data to third parties.

Users, of course, often consent to such dissemination of their data when signing up to use these services. However, they often do so via lengthy, byzantine "terms of service" agreements, which they don't read in any meaningful way and would take several lawyers to decipher.

And there are passive ways that data is collected as well - from facial recognition cameras to license plate readers - that enable law enforcement to identify and investigate crime in real time. The rise of artificial intelligence only promises to make all of this more complicated and penetrating.

So, in a very real way, what our society has is a MODERN, ALBEIT CONSENSUAL, SURVEILLANCE STATE. Modern technology, including artificial intelligence, is amazing and has the potential to improve our lives in immeasurable ways. But it also has the potential for significant abuse. It is Congress's obligation to examine these authorities, the Executive's use of the authorities, and to ensure the authorities aren't being used in unforeseen, unintended ways that harm our civil liberties and violate the constitution.

What is needed, Members of this Subcommittee, is a renewed, bipartisan oversight effort by this body, to rein in abuse and protect Americans' expectations of privacy. It is in that spirit that I come before you today.

How do we do this? Well, one way is through targeted legislative reforms some of which were accomplished over the last several decades, and most recently in last Congress's FISA reauthorization. Bipartisan reforms like those in the recently enacted H.R. 7888, the Reforming Intelligence and Securing America Act (RISAA), are good and welcome. For example, requiring audits of all U.S. person queries and targeting procedures will help ensure Americans aren't targeted by a law that is explicitly aimed at "non-U.S. persons reasonably perceived to be located outside of the United States." Reforming Foreign Intelligence Surveillance Court (FISC) procedures as in Section 5 of RISAA, and requiring that exculpatory information be included in FISA applications, are positive. And these were not the only needed provisions that were enacted into law. Fortunately, there were many more.

Additionally, in an age where massive amounts of user data have been commercialized by data brokers, you should ask yourselves: If the government can obtain information from a company, or a third party data broker, which would ordinarily require a determination of probable cause from a detached magistrate, as the Fourth Amendment requires, does obtaining information by paying for it, without that time-honored legal process, undermine a crucial constitutional safeguard and civil liberty? I would submit that it does.

Last Congress, this Committee approved and the House passed H.R. 4639, the Fourth Amendment is Not for Sale Act. I would encourage you to do so again.

But legislative reforms are only half the battle. What is also absolutely required here is vigorous, targeted oversight by the legislative branch. And just as law enforcement is increasingly able to identify and interdict crime in real time, Congress's FISA oversight must also be in real time.

What does that mean? It means that the disclosure of the information I described above must be timely. Congress must insist it is timely. For too long, our Congressional Committees have received information, in response to reporting requirements, that is months, or even years, old in addition to being poorly organized and in many instances incomplete. I worked in two cabinet departments and know firsthand what it means to receive a "Congressional Oversight" letter.

The last time I appeared before this committee; I talked about how this "after-the-fact" approach was problematic. It remains so today. The numerous legislative reform provisions, in H.R. 7888 including the reporting and transparency measures are a valuable first step in solving this problem, but this will only work if through its oversight responsibilities Congress receives access to information in a timely manner. Make sure all these reforms are implemented promptly and within the next year prior to reauthorization. Congress must be allowed real-time access to this information to the greatest extent possible to ensure proper analysis and implementation by the agency is occurring.

Congress has the ability to receive, secure, and hold classified information. Every Member of Congress, under the U.S. Constitution and federal law (50 U.S.C. 3163), has access to classified material. However, the number of Congressional staff who hold TS/SCI clearances is very low, especially compared to the number of Executive branch employees who hold clearances. Do you know how many Judiciary Committee staffers hold a clearance today? I suspect it's fewer than you think. Congress should consider amending its rules to increase the number of qualified staff with clearances for classified material and briefings.

I would also direct Members' attention to section 18(b) of H.R. 7888, which requires the Director of National Intelligence to commission a study on technological enhancements that would enable the FBI to monitor compliance of the Bureau's 702 information systems in near-real time. Could

we use Artificial Intelligence to monitor, in near-real time, the FBI's compliance with FISA? If we could, why wouldn't Congress be entitled to that information on an ongoing or even rolling basis?

And of course, Congress must continue to include sunset provisions in FISA reauthorization. Without sunset provisions, we may never have learned about much of this abuse. Without sunset provisions, Congress will simply continue to cede its Constitutional, Article I, legislative and oversight authority to unelected entities within the Executive branch. FISA is up for reauthorization in another year. If it is reauthorized, I would suggest it be no longer than a two- or three-year period to ensure Congress can evaluate and update both the implementation and progress associated with its extension.

In conclusion: The short leash must be on the intelligence community, not on Congress.

Mr. Chairman, Ranking Member McBath, I am not someone who is hostile to strong national security laws or federal law enforcement. Congress should not repeal section 702. It is an important tool that provides vital intelligence on a range of foreign threats and has successfully foiled terrorist attacks. Congress should not neuter FISA—which was, of course, put in place in the 1970s to constrain the government's use of surveillance authorities against American citizens.

However, Congress, as the constitutional entity closest to the people, must reassert its vital and constitutional oversight role, to protect the people.

Thank you for the opportunity to testify.

Statement for United States House of Representatives
Committee on the Judiciary
Fixing FISA, Part II
Philip G. Kiko
July 14, 2023

Good morning. Thank you for the opportunity to appear and testify before the Committee.

Introduction

It is an honor for me to return to the Committee where I worked with former Chairman Jim Sensenbrenner as the Staff Director and General Counsel. My years working with the Judiciary Committee were one of the highlights of my professional career, and I will always be grateful to the Committee and all of its Members for the opportunity to serve you and the public.

The Critical Balance Between Protection of our National Security and Our Civil Liberties

At the outset, I want to underscore the importance of this hearing and the Committee's oversight and examination of the re-authorization of Section 702 of the Foreign Intelligence Surveillance Act (FISA).[1] Historically, the Committee has played a central role in protecting our country and its citizens from foreign enemies – hostile governments, terrorists, and transnational criminal organizations. At every step, the Committee has carried out this responsibility with proper regard for protection of our constitutional rights and liberties.

I am proud of the work that former Chairman Sensenbrenner, and former Chairs Goodlatte, Smith, Conyers, and Nadler (currently Ranking Member), and other Members of the Committee, on both sides of the aisle, devoted to this weighty issue. Today's hearing is yet another example of the

[1] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783, 50 U.S.C. § 1801 (1978).

Committee's tradition of reviewing important issues with proper regard for the need to ensure the safety of all Americans while protecting against abuses that may threaten our cherished civil liberties. It speaks to the tension in areas of national security between Congress' constitutional authority to pass laws to define the government's role in this area of the law versus the inherent Executive authority in the sphere of national security.

We faced similar challenges in the aftermath of the horrible and tragic attack against our country on September 11, 2001, in which we lost hundreds of innocent Americans.

The Committee – and our country – then faced an important crossroads and today we face a similar one, where we must adhere to our Constitution and our fundamental civil liberties while taking appropriate steps to protect our nation's security.

The USA PATRIOT Act in the Aftermath of the 9-11 Attack

I want to take a moment to outline for the Committee the events leading to enactment of the original USA PATRIOT Act ("Patriot Act")[2], the difficult issues we faced, and the necessary protections that the Committee and Congress as a whole agreed to when we enacted the Patriot Act. In my view, this context will provide some important lessons learned that may be helpful for the Committee to weigh as it considers re-authorization of Section 702 of FISA.

In the days after 9-11, former Chairman Sensenbrenner, Ranking Member Conyers, Committee Members, and staff all knew that changes to our foreign intelligence and law enforcement systems had to be made to ensure that such an attack could never occur again. It was apparent that the 9-11 attack exposed serious deficiencies in our intelligence system for collecting and analyzing data to prevent our citizens from future terrorist attacks. We were united in our mission, and the need

[2] USA PATRIOT Act, Pub. L. 107-56, 115 Stat. 272 (2001).

for Congress to act quickly and effectively to ensure that our country was safe. At the same time, however, I want to emphasize that we carried out this mission with dedication, bipartisan commitment, and a strict adherence to ensuring that our shared and cherished civil liberties were protected. It was a simple equation in our view – we will protect the country, but we will not do so at the expense of our freedoms, and we will continue to be governed by constitutional principles.

Over the following weeks, former Chairman Sensenbrenner, Ranking Member Conyers, Committee Members, and staff worked tirelessly to get this done. The Bush Administration responded quickly, and the Justice Department and the intelligence community proposed important reforms to the FISA and other intelligence and law enforcement authorities. It should be noted the Financial Services Committee played an important role in updating money laundering provisions which became Title 3 of the Patriot Act, which has become an important tool in cutting off terrorist financing schemes. The Committee moved quickly, conducted hearings to examine the important issues, and engaged in a thoughtful and vigorous debate.

Chairman Sensenbrenner and Ranking Member Conyers directed the Committee's effort. We arrived at a critical point in the process –we all knew that these new and extraordinary changes to FISA and related authorities depended on the professionalism of the Federal Bureau of Investigation and the intelligence community to follow safeguards to protect against possible abuse that may threaten everyone's civil liberties – the right to privacy, protection against unreasonable intrusions from surveillance, and improper targeting of individuals for searches and seizures.

The Administration placed significant pressure on the Committee and Congress to quickly enact reforms that they characterized as critical to protect our country from future attacks. In fact, there were reports the Administration wanted a bill passed within a week. The public mood was one of resolve, revenge, fear, anger, and demand for protection of our country's security. We all agreed

that the expanded authorities set forth in the Patriot Act required everyone to "trust" the Department of Justice, the FBI, and the intelligence community to operate within the requirements of the law and the United States Constitution. Implicit within this was that the Executive Branch would develop an effective verification process to ensure that our civil liberties were protected.

It was at this juncture when the Committee raised the issue of including – and indeed, insisted on - sunset provisions that would require Congress to re-examine several of the key provisions in the Patriot Act in four (4) years. The Committee and the House rallied behind the sunset provisions because we all agreed that, if unchecked, the Patriot Act, as originally crafted, could easily undermine and threaten a number of our cherished civil liberties.

As it turned out over the following 20 years, the sunset provisions have become a critical mechanism for Congress to re-examine Patriot Act provisions, and to reassess law enforcement and the intelligence community's performance, and the continued need for various authorities. In other words, we knew that the global threat and anti-terrorism requirements would evolve over time, and the sunset provisions were an important tool to ensure that the proper balance was struck between our national security needs and protecting our civil liberties.

And while the Members of the House Judiciary Committee agreed on the need for the sunset provisions, I wish I could tell you that everyone in the Administration and in the Senate agreed with us and that the provisions were simply added to the Patriot Act. But that is not how it happened.

Instead, House Leadership, Chairman Sensenbrenner and Ranking Member Conyers were subjected to extraordinary pressure and a torrent of calls – political, media generated, and public

opinion – to back down, to eliminate the sunset provisions and act quickly to protect our country from a future attack.

I can recall meetings with Leadership, our Senate counterparts, in addition to representatives from the White House, Justice, the intel community and others where Chairman Sensenbrenner stuck to the Committee's position – we would enact the Patriot Act with extraordinary new authorizations for use by the Justice Department, the FBI and the intelligence community, but the House and the Judiciary Committee would insist on including the sunset provisions to ensure that our national security was protected without any threat or diminution to our civil liberties.

Eventually, as everyone knows, our position prevailed. The House Judiciary Committee reported out the Patriot Act unanimously with the sunset provisions. The Patriot Act passed the House by a vote of 357-66 and the Senate by a vote of 98-1.

The rest, as they say, is history. But we all stood together in a unified voice committed to one fundamental principle – protection of our national security had to be accomplished with proper regard for our constitutional protections. And, as it turns out, we were ***absolutely*** right to insist on sunset provisions as a means to ensure appropriate oversight, refinement of authorities, transparency, and continued assessment of DOJ, the FBI, and the intelligence community.

History's Vindication: Protecting Our Country While Preserving Civil Liberties

Before addressing the current issue of re-authorization of Section 702, it is important to understand the origins of FISA, and the purpose that it serves as an important check on intelligence and law enforcement activities.

Following widespread wiretapping and surveillance abuses during the 1960s and 1970s,[3] Congress enacted FISA as an important new mechanism to establish procedures and requirements for domestic electronic intercepts of foreign intelligence.[4]

FISA provides a statutory framework for government agencies to secure authorization to gather foreign intelligence by means of: (1) electronic surveillance; (2) physical searches; (3) pen registers and trap and trace devices; and (4) production of certain business records. In addition, FISA created two new Article III courts: the Foreign Intelligence Surveillance Court (FISC) and the appellate Foreign Intelligence Surveillance Court of Review (FISCR).[5]

The most significant reform to FISA, as I outlined above, was the enactment of the Patriot Act in 2001, which was passed to "provide enhanced investigative tools" to "assist in the prevention of future terrorist activities and the preliminary acts and crimes which further such activities." The Patriot Act included four-year sunset provisions applicable to 16 of its new authorities.[6]

---

[3] S. Res. 21, 94th Cong (1975) (; 124 Cong. Rec. 34, 845 (1978); S. Rep. No. 94-755 (1976) (the Church Committee reports); Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 Harvard J.L. & Public Policy 757 (2014) (discussing the history leading to heightened protections afforded to domestic collection of U.S. citizens' information).

[4] FISA's definition of "foreign intelligence information" was modified by the Patriot Act to mean information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. 50 U.S.C. §3003(2). Congress initially restricted FISA to regulate use of electronic surveillance, but subsequently amended FISA to regulate other practices such as physical searches, the use of trap-and-trace and pen registers, and production of certain types of business records. *See* Laura K. Donahue, *The Evolution and Jurisprudence of The Foreign Intelligence Surveillance Court and Foreign Intelligence Surveillance Court of Review,* 12 Harv. Nat'l Sec. J. (2021). available at https://harvardnsj.org/2021/06/28/the-evolution-and-jurisprudence-of-the-foreign-intelligence-surveillance-court-and-foreign-intelligence-surveillance-court-of-review/.

[5] 50 U.S.C.A. § 1803(a)–(b).

[6] In 2020, three FISA provisions expired under applicable sunsets: Section 206 "roving wiretaps"; Section 215 "business records"; and the "lone wolf" provision. *See* Edward C. Liu, CRS, *Foreign Intelligence Surveillance Act: An Overview*, at 1 (2021)., available at https://sgp.fas.org/crs/intel/IF11451.pdf.

In 2008, Congress enacted the FISA Amendments Act and codified Title VII (including Section 702), which created procedures to collect foreign intelligence when communications travel through the United States' communications infrastructure.[7] Under Section 702, the government may compel electronic communications service providers for a period of up to one year to assist in targeting non-U.S. persons reasonably believed to be located outside the United States. The Attorney General and the Director of National Intelligence (DNI) must jointly certify that they authorize any such targeting, and the FISC must approve any program under Section 702 before its implementation.

In 2013, the foreign intelligence world was rocked by Edward Snowden's disclosure of documents that revealed that the National Security Agency (NSA) was engaged in the bulk collection of telephone metadata under Section 215 of FISA. The Snowden leaks revealed that the NSA was over-collecting upstream Section 702 data, monitoring U.S. citizens' email and text communications in and out of the country, and conducting a variety of warrantless searches to build profiles of individuals. Snowden's revelations led to a public backlash and explosion in litigation before the FISC amid controversies relating to NSA abuses involving unauthorized collection of metadata, including calls and electronic communications occurring entirely within the United States.[8]

[7] The FAA included important statutory and procedural protections regarding surveillance of U.S. persons located outside the United States. Congress reauthorized Title VII in early 2018 and included a five-year sunset, expiring in 2023. *See Id*. at 1-2.

[8] Press reports cited the fact that the NSA was using "back-door" techniques to access data from U.S. Internet companies. For example, over a 30-day period, approximately 97 billion internet data records and 124 telephone data records had been collected. Inside the U.S., approximately 3 billion data elements were collected over a 30-day period in 2013 concerning U.S. citizen activity. *See* Donahue, *supra* at 21-22.

In response to this controversy, former Chairman Sensenbrenner, Ranking Member Conyers and Senate Judiciary Chairman Leahy proposed and eventually secured passage of the USA Freedom Act,[9] which prohibited bulk collection under Section 215, FISA pen register/trap and trace authorities, and National Security Letters. The Act also required the appointment of at least five *amici* to appear before the FISC to address novel questions of law, and required a number of reports related to the operation of FISA authorities.

The Need to Reform Section 702

As I noted above, the Committee now stands at another important crossroads – the issues we face involve a delicate balance between two critical needs – we have to protect our country from foreign enemies and Section 702 is a critical tool for accomplishing that purpose. On the other side, however, Congress must enact real and meaningful reform to protect Americans' civil liberties.

Since the leak of the Snowden documents and the public disclosure of abuses that resulted in the passage of the USA Freedom Act reforms, the country continues to witness escalating and serious concerns surrounding law enforcement and intelligence community misconduct and failures to comply with checks needed to protect our civil liberties.

Needless to say, the Department of Justice, law enforcement and the intelligence community's record of compliance failures has been amply documented, cited and disclosed by various credible

[9] *USA Freedom Act*, Pub. L. No. 114-23, 129 Stat. 268 (2015).

parties, including: (1) the FISC itself;[10] (2) the Department of Justice's Inspector General;[11] and (3) this Committee's own oversight and investigative record.[12] The record of DOJ, the FBI and intelligence community is disturbing and cannot be ignored.

In its April 21, 2022, *Memorandum Opinion and Order*, the FISC cited numerous instances of noncompliance, misrepresentations, and unlawful access (over 278,000 times) to data collected pursuant to Section 702 over a multi-year period. The FISC's citation of violations and abuse of querying of Section 702-collected data is described in detail at pages 28 to 34 of its *Memorandum Opinion and Order*.

Similarly, the DOJ Inspector General has demonstrated the difficulties faced by the Department of Justice and the FBI in maintaining a proper balance between protecting national security and

[10] *See Document re: Section 702 2021 Certification, FISA Ct., April 21, 2022, (Memorandum Opinion and Order)* available at: https://www.intelligence.gov/assets/documents/702%20Documents/declassified/21/2021_FISC_Certification_Opinion.pdf; *see also*, Donahue, *supra* at 54-71.

[11] *See* U.S. Dep't of Justice, Off. of Inspector Gen.*, Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation* (2019), available at https://www.justice.gov/storage/120919-examination.pdf; U.S. Dep't of Justice, Off. of Inspector Gen.*, Audit of the Federal Bureau of Investigation's Execution of its Wood Procedures for Applications Filed with the Foreign Intelligence Surveillance Court Relating to U.S. Persons* (2021) , available at *https://oig.justice.gov/sites/default/files/reports/21-129.pdf* (Non-compliance identified in all 29 FISA applications reviewed by the OIG. DOJ later discovered 209 errors in those applications, 4 of which DOJ deemed material. 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); and U.S. Dep't of Justice, Off. of Inspector Gen.*, Audit of the Roles and Responsibilities of the Federal Bureau of Investigation's Office of the General Counsel in National Security Matters* (2022), available at https://oig.justice.gov/sites/default/files/reports/22-116.pdf (DOJ's National Security Division (NSD) and FBI's Office of General Counsel (OGC) had differing interpretations of the query standard under the FBI's Section 702 Querying Procedures, which resulted in numerous compliance incidents and disputes between the FBI's OGC and DOJ's NSD attorneys).

[12] *Fixing FISA: How a Law Designed to Protect Americans Has Been Weaponized Against Them*: Hearing Before the Subcomm. on Crime and Government Surveillance, 116 Cong. (2019), available at https://www.govinfo.gov/content/pkg/CHRG-116hhrg44884/html/CHRG-116hhrg44884.htm.

safeguarding civil liberties.[13] In particular, DOJ's Inspector General testified before this Committee and highlighted three important issues in light of the Committee's consideration of re-authorization of Section 702: (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.[14]

In this context, the FISA world of foreign intelligence has changed significantly since 2001 and the aftermath of 9-11. Over the last 20 years, Congress at one point or another has faced the difficult question of whether to re-authorize powerful foreign intelligence authorizations against the backdrop of a disturbing record of non-compliance. We have seen this before.

Without belaboring this point or rehashing the evidence over the last 20 years, suffice it to say, the Committee needs to implement meaningful reforms to prevent potential problems before they occur. All too often, the Committee and the public have learned about compliance failures after the fact, and then relied on law enforcement and the intelligence community to institute remedial solutions. This "after-the-fact" approach is not sustainable, and a new proactive approach is needed. Specifically, I would urge the Committee to examine proactive solutions that mandate procedural and substantive reforms to the internal processes and procedures used by law enforcement and the intelligence community, which would be subject to oversight in real time and

---

[13] *See Id*. (Statement of Michael E. Horowitz, Appendix *Prior OIG Reports on FISA and National Security Authorities*), available at https://oig.justice.gov/sites/default/files/2023-04/4-27-2023.pdf

[14] *See Id*. (Statement of Michael E. Horowitz).

not on a yearly or more basis after the damage has been done. We can no longer rely on DOJ's, the FBI's, and intelligence community's promises of reform to existing procedures and processes.

A new solution must be found, and the Committee must find a way forward to continue Section 702 collection while implementing real and significant reforms to protect our constitutional rights. Just like our original mission in 2001 in the aftermath of the attack against our country, the basic principles remain the same: we must protect our country from future terrorist attacks, and we must do so without harming our civil liberties.

There is no doubt that Section 702 has been a valuable tool and we should be careful about allowing it to expire. FISA was created in 1978 as a restraint against government and as a protection to Americans, however it is clear it needs to be updated. I would urge the Committee to undertake serious reforms, beyond those we have ever considered or enacted before, to ensure that the FBI and the intelligence community will not be permitted to threaten our fundamental civil liberties.

The Committee has before it a difficult task that requires a delicate balancing act. There are some who advocate that Congress should let Section 702 authority expire; and there are others who argue that if 702 is allowed to expire, the Executive branch will fall back on its inherent authority in the national security arena and executive orders and would probably be happy to do so without the pesky interference of Congressional oversight. If Section 702 is re-authorized, implementation of proactive monitoring programs, real and significant changes to law enforcement and intelligence community processes, and an increase of overall transparency of this powerful tool could serve as important checks. There must be consequences for abusing FISA as a deterrent to bad behavior.

We need to put teeth in FISA, so people think twice about doing inappropriate things. The trust can be rebuilt, but only if there is more accountability by the intelligence and law enforcement community. Congress and the FISC can exercise appropriate oversight and protection of our cherished liberties while ensuring the protection of our safety from foreign enemies. In the past, beginning with the creation of FISA, Congress has had to be reactive; now there is an opportunity to be proactive.

Apart from Section 702, it needs to be noted there has been a constant chipping away at the protections of the 4th Amendment. Data brokers regularly sell large quantities of personal data about United States citizens to law enforcement agencies and do so without notifying any United States citizen that such practice is occurring. Further, warrantless access is given to all kinds of information without any knowledge of the person who submitted it. Why is this data not protected? I am sure the individuals affected did not expect their data to be sold and accessed without their knowledge. The constant chipping away of 4th Amendment protections needs to be addressed.

When Chairman Sensenbrenner and I visited the horrific scene of the Twin Towers days after the 9-11 attack, we both knew at that time that our country's future would depend on our work with everyone in Congress, the Executive Branch, law enforcement, and the intelligence community to make sure the words "Never Again" would become a reality. I am convinced that today we can reaffirm this solemn promise to the American people by reforming FISA and by taking a broader look at how data is gathered on Americans without their knowledge by law enforcement agencies. Protections need to be, and should be, reviewed by Congress and addressed.