Senate Judiciary Committee Hearing
"Reauthorizing the USA FREEDOM Act of 215"
Questions for the Record
for Hon. Adam Klein
Chairman and Member
Privacy and Civil Liberties Oversight Board

Submitted November 13, 2019

QUESTIONS FROM SENATOR WHITEHOUSE

1. The Privacy and Civil Liberties Oversight Board conducted ongoing oversight of the NSA's collection of call detail records under Section 215 until the program was decommissioned.
    a. Do you believe this program can be administered in a constitutional manner?

Under *Smith v. Maryland* and subsequent cases applying it, collecting telephone dialing and routing information held by a third-party provider is not a Fourth Amendment "search" or "seizure." *Carpenter v. United States* modified the third-party doctrine with respect to the collection of cell-site location information in criminal investigations, but otherwise confirmed that *Smith* remains the law. Notably, the USA Freedom Act bars the government from using the CDR authority to collect cell-site location information or GPS information.

The Board's draft report on NSA's collection of call detail records under the USA Freedom Act applies these and other cases to the CDR program. The draft report is currently undergoing classification review by the Intelligence Community.

    b. Do you agree with the Board's 2014 assessment that this program has not "made any significant contribution to counterterrorism efforts"?

Having reviewed the operational use of the program as modified by the USA Freedom Act, I agree with NSA's publicly stated view that the value generated by the program was outweighed by the program's costs and the "compliance and data integrity concerns caused by … using these company-generated business records for intelligence purposes."

I would be pleased to provide additional detail about the administration and operation of the CDR program in a classified setting. We are prepared to provide a classified briefing or testimony at any time that would be convenient for Senators. The Board is also committed to working with the Intelligence Community to ensure that our report is made available to the public to the greatest extent possible, consistent with the protection of classified information.

2. The Office of the Director of National Intelligence recently declassified a 2018 decision by the FISA Court which found that the FBI was accessing Americans' communications collected under Section 702 in violation of the statute and the Fourth Amendment.[1] Among other things, FBI agents were conducting thousands of searches that were not reasonably likely to result in foreign intelligence information or evidence of a crime.[2]

   The Privacy and Civil Liberties Oversight Board is also reviewing the FBI's queries of U.S. persons data obtained under Section 702. Do you believe that the procedures the FBI implemented in response to the FISA Court's decision are sufficient to protect U.S. persons from unlawful searches without unduly impeding legitimate law enforcement?

Programs involving collection at scale of potentially sensitive data about Americans, even if that information is incidentally collected, must include safeguards to ensure that the data is used only for appropriate purposes and subject to applicable rules. Our review of the FBI's use of data from Section 702 will examine the issues identified by the FISC and FISCR, the remedies imposed, and other issues related to access controls, accountability, and auditability.

We would be pleased to brief Senators on our findings once that project approaches its conclusion. The Board will also ensure that any resulting report is made available to the public to the greatest extent possible, consistent with the protection of classified information.

[1] Decision and Order (FISA Court Oct. 18 2018), available at https://www.intel.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf.
[2] Id. at 68-71.

Hon. Adam I. Klein –
Reauthorizing the USA FREEDOM Act of 2015
Questions for the Record
Submitted November 13, 2019

QUESTIONS FROM SENATOR COONS

1. You mention in your written testimony that the Privacy and Civil Liberties Board created a panel of cleared amicus advocates to assist the Foreign Intelligence Surveillance Court (FISC). What are the criteria used to select advocates?

In its 2014 report on the collection of telephone call records under Section 215 of the USA PATRIOT Act, the Board recommended that Congress "enact legislation enabling the FISC to hear independent views … on novel and significant applications and in other matters in which a FISC judge determines that consideration of the issues would merit such additional views." The USA Freedom Act of 2015 adopted that recommendation by creating a panel of cleared amici to assist the FISC in certain matters.

Under the Act, amici must be selected based on their "expertise in privacy and civil liberties, intelligence collection, communications technology, or any other area that may lend legal or technical expertise" to the court, and their eligibility to obtain a security clearance. At present, the court has designated five legal experts and three technical experts as eligible to serve as amicus curiae.

2. In what percentage of cases before the FISC is an amicus appointed?

According to the annual report on the FISC by the Administrative Office of the U.S. Courts, the court appointed an amicus in nine instances in 2018. That year, the FISC received 1,318 applications. The nine appointments reflect an increase over prior years: There were no amicus appointments in 2017, one in 2016, and four in 2015.

3. The Privacy and Civil Liberties Oversight Board has made a number of suggestions regarding the role of amici curiae in the FISC, including expanding the types of cases they can participate in, improving access to materials, and being able to trigger appeals. Which alterations are most important to ensure robust protections at the FISC?

The institution of the amicus is an important reform that provides a valuable resource for FISC judges and enhances public confidence in the court. The Board made several recommendations concerning FISA court amici in its 2014 report. The Board believed each of these recommendations to be worthwhile but did not indicate which took precedence.

One proposal I have made in a previous, nongovernmental capacity is that Congress mandate the appointment of an amicus to advise the FISC as it reviews each annual certification under Section 702. Because the court's oversight of Section 702 is programmatic rather than individualized, each certification proceeding is systemically significant: The rules imposed will govern thousands of targeting, minimization, and querying decisions made within IC elements implementing Section 702. By contrast, most other matters on the Court's docket may more closely resemble the type of fact-intensive proceedings, comparable to an application for a search warrant, that are ordinarily conducted *ex parte* in the criminal context.

Adam I. Klein
Chairman and Member
Privacy and Civil Liberties Oversight Board
Questions for the Record
Submitted November 13, 2019

QUESTIONS FROM SENATOR BOOKER

1. The joint statement from the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA) for this hearing says the following about the Call Detail Records (CDR) program:

> [T]he NSA recently discontinued the CDR program for technical and operational reasons. But the CDR program retains the potential to be a source of valuable foreign intelligence information. The CDR program may be needed again in the future, should circumstances change. NSA's careful approach to the program, and the legal obligations imposed by the FREEDOM Act in the form of judicial oversight, legislative oversight, and transparency, support the reauthorization of the CDR program. . . . [T]he Administration's view is that the time has come for Congress to extend these authorities permanently.

   a. Are you aware of any examples of past instances in which DOJ, the FBI, or the NSA (or any other relevant agency) shut down a statutorily authorized program, but Congress nevertheless permanently reauthorized the underlying statutory authority to make it available for an unspecified future use?

The closest comparator of which I am aware is the FISA Amendments Reauthorization Act of 2017. In April 2017, NSA announced that it had stopped using Section 702 of FISA to collect communications "that are solely 'about' a foreign intelligence target," rather than to or from the target. In the Reauthorization Act, which became law in January 2018, Congress reauthorized Section 702 without banning this type of collection, known as "abouts" collection. However, the Act required the government to inform Congress 30 days in advance of resuming "abouts" collection, during which time Congress can "hold hearings and otherwise obtain information."

   b. Are you aware of any examples of existing provisions in the U.S. Code for which DOJ, the FBI, or the NSA (or any other relevant agency) have discontinued the authorized program, but could reactivate the program if the agency chose to do so?

See response to 1(a).

   c. In your testimony, you noted that the Board has reviewed the CDR program and has submitted a report for classification review. What is your understanding of the

"technical and operational reasons" that the CDR program was discontinued, with as much specificity as possible as you can currently provide in an open setting?

Discussion of the relevant operational details would likely implicate classified information. I would be pleased to provide additional detail about the administration and operation of the CDR program in a classified setting. We are prepared to provide a classified briefing or testimony at any time that would be convenient for Senators. The Board is also committed to working with the Intelligence Community to ensure that our report is made available to the public to the greatest extent possible, consistent with the protection of classified information.

d. The NSA's collection of call-detail records from telecommunications providers more than tripled from 2016 to 2017, rising from more than 151 million to more than 534 million.[1] When this increase was first reported last year, the Office of the Director of National Intelligence's chief civil liberties officer, Alex Joel, "cited a variety of factors that might have contributed to the increase, potentially including changes in the amount of historical data companies are choosing to keep, the number of phone accounts used by each target and changes to how the telecommunications industry creates records based on constantly shifting technology and practices."[2] A few weeks after this report was issued, the NSA began purging hundreds of millions of call- detail records that were subject to "technical irregularities."[3] Given what you can currently disclose in a public setting about the Board's review, was the tripling in the collection of call-detail records from 2016 to 2017 attributable in any part to the "technical irregularities" in these records? If so, did the dramatic increase in collection help to spur the discovery of the underlying data integrity and compliance problems?

Discussion of the relevant operational details would likely implicate classified information. I would be pleased to provide additional detail about the administration and operation of the CDR program in a classified setting. We are prepared to provide a classified briefing or testimony at any time that would be convenient for Senators. The Board is also committed to working with the Intelligence Community to ensure that our report is made available to the public to the greatest extent possible, consistent with the protection of classified information.

e. In an August 2019 letter, then-Director of National Intelligence Dan Coats said the following in support of reauthorizing the provision that underlay the discontinued CDR program: "as technology changes, our adversaries' tradecraft

[1] OFFICE OF CIVIL LIBERTIES, PRIVACY & TRANSPARENCY, OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, STATISTICAL TRANSPARENCY REPORT REGARDING USE OF NATIONAL SECURITY AUTHORITIES, CALENDAR YEAR 2017, at 34 fig.19 (Apr. 2018), https://www.dni.gov/files/documents/icotr/2018-ASTR----CY2017----FINAL-for- Release-5.4.18.pdf.
[2] Charlie Savage, *N.S.A. Triples Collection of Data From U.S. Phone Companies*, N.Y. TIMES (May 4, 2018), https://www.nytimes.com/2018/05/04/us/politics/nsa-surveillance-2017-annual-report.html.
[3] Charlie Savage, *N.S.A. Purges Hundreds of Millions of Call and Text Records*, N.Y. TIMES (June 29, 2018), https://www.nytimes.com/2018/06/29/us/politics/nsa-call-records-purged.html.

and communications habits will continue to evolve and adapt."[4] From your vantage point, how might this statutory authority be used in the future if it is reauthorized?

The USA Freedom Act's CDR provision imposes various limitations on the government's ability to request CDRs. It requires the government to obtain a FISA court order based on "reasonable, articulable suspicion" and permits collection only of "call detail records," which are limited to certain types of non-content information. The statute prohibits use of the CDR authority to collect the content of communications, cell-site location information, GPS information, or the names, addresses, or financial information of subscribers. If the government chose to restart two-hop CDR collection in the future, its use of this authority would be circumscribed by these statutory restrictions.

2. As noted at the hearing, to date the government has never used the "lone wolf" provision since it was added to the Foreign Intelligence Surveillance Act (FISA) in 2004. Given that the "lone wolf" provision has yet to be used, what metrics can Congress look to in assessing its intelligence value?

A recently released report by the FBI's Behavioral Analysis Unit provides a detailed statistical analysis of lone-offender terrorist attacks in the United States between 1972 and 2015. This report, entitled *Lone Offender: A Survey of Lone Offender Terrorist Attacks in the United States (1972 – 2015)*, may be informative as Congress considers the potential intelligence value of the lone-wolf provision.

Looking forward, the question is whether there is a reasonable case for preserving the lone-wolf authority in light of what is known about the international terrorist threat and how it is evolving. Military and intelligence operations overseas have degraded hierarchical terrorist organizations like al Qaeda and ISIS, while improved homeland security and heightened vigilance have made it more difficult for trained operatives to infiltrate the United States undetected and carry out a 9/11-style attack. In recent years, counterterrorism experts' concern has increasingly focused on homegrown terrorists, who may radicalize with few observable connections to established terrorist organizations. Given these developments, it is reasonable to believe that the lone-wolf provision could be useful in the future, though this is necessarily speculative.

3. During the hearing, this Committee heard testimony about the U.S. Supreme Court's recent decision in *Carpenter v. United States*.[5] As Ms. Goitein testified, "the Court in *Carpenter* essentially held that there are certain types of information that are so sensitive, so

[4] Letter from Daniel R. Coats, Dir. of Nat'l Intelligence, to Senators Richard Burr, Lindsey O. Graham, Mark Warner & Dianne Feinstein 1-2 (Aug. 14, 2019), https://int.nyt.com/data/documenthelper/1640-odni-letter-to- congress-about/20bfc7d1223dba027e55/optimized/full.pdf.
[5] 138 S. Ct. 2206 (2018).

inherently sensitive in what they reveal about a person's life that the mere fact that they are held by a third party does not eviscerate the person's Fourth Amendment interest in that information." The facts of *Carpenter* involved "several months' worth of cell phone location data."[6]

In light of *Carpenter*, what steps, if any, should Congress take in the context of reauthorizing the USA FREEDOM Act to ensure compliance with the constitutional protections described in *Carpenter*?

Carpenter held that the collection of historical cell-site location information (CSLI) covering an extended time span, in a criminal investigation, constituted a search triggering the Fourth Amendment's warrant requirement. The Court noted that its opinion was "a narrow one" that did "not consider other collection techniques involving foreign affairs or national security."

The USA Freedom Act's CDR provision expressly excludes CSLI or GPS information. Accordingly, that provision as presently drafted is consistent with the holding of *Carpenter*.

By its terms, the text of FISA's "traditional" business records provision, also up for reauthorization, could permit the government to obtain historical CSLI with an order based on less than probable cause. However, the Office of the Director of National Intelligence reports that its "current practice" is to use probable-cause-based orders available under FISA to obtain CSLI or GPS data, and that it has not used the business records authority to obtain such data since *Carpenter* was decided.

4. According to Mr. Orlando's testimony, the FBI's working definition of "tangible things" in the context of business records includes "books, records, papers, document[s], other items, airline records, hotel accommodations, storage facilities, [and] vehicle rentals. It also provides for some sensitive items such as library circulation records, book sales, book customer lists, firearm sales records, tax records, [and] educational returns." Mr. Orlando also acknowledged that medical records fall under the FBI's working definition of tangible things.[7] In that vein, Mr. Wiegmann told the Committee that "you could not get Fourth Amendment protected content with a business records order."[8]

   In light of the Supreme Court's decision in *Carpenter*, do you believe that the FBI's working definition of "tangible things" encompasses content protected by the Fourth Amendment?

   The FBI is best positioned to speak to the precise contours of its internal definition of

[6] *Senate Judiciary Committee Holds Hearing on USA FREEDOM Legislation Reauthorization*, CQ CONG. TRANSCRIPTS (Nov. 6, 2019), https://plus.cq.com/doc/congressionaltranscripts-5765239.
[7] *Id.*
[8] *Id.*

"tangible things" covered by the statute. As our Board oversees the FBI's use of FISA's business records provision to protect the nation against terrorism, the Board is conscious of the applicable Fourth Amendment principles. I am also conscious, as a policy matter, that different types of information maintained about users by third-party providers raise varying degrees of concern for privacy and other equities.

5. The USA FREEDOM Act enacted a number of reforms to Foreign Intelligence Surveillance Court proceedings, including requiring the appointment of at least five individuals to be amici curiae who are charged with helping to protect individual privacy and civil liberties.[9]

    a. What is your assessment of how well this process, in which an outside amicus argues against the government in Foreign Intelligence Surveillance Court proceedings, has worked in practice?

The institution of the amicus is an important reform that provides a valuable resource for FISC judges and enhances public confidence in the court. Several declassified FISC opinions provide evidence that amici have played a valuable role in FISC proceedings. The increase over time in the number of amicus appointments also suggests that the FISC judges value the option to hear from amici.

    b. Do you believe the amicus process has provided an adequate voice for the protection of privacy and civil liberties in Foreign Intelligence Surveillance Court proceedings?

Amici can play a valuable role in FISC proceedings that present novel or significant issues of law or policy. Other, complementary mechanisms provide additional transparency and accountability. One is the mandatory declassification of significant FISC and FISCR opinions, which allows the public and outside experts to review and comment on the development of the law by those courts. Annual transparency reports issued by the Office of the Director of National Intelligence and the Director of the Administrative Office of the U.S. Courts are another important public resource.

    c. Are there any ways in which you believe the amicus process should be changed? If so, please explain why you believe the change is needed, and how individual privacy and civil liberties would be protected.

One proposal I have made in a previous, nongovernmental capacity is that Congress mandate the appointment of an amicus to advise the FISC as it reviews each annual certification under Section 702. Because the court's oversight of Section 702 is programmatic rather than individualized, each certification proceeding is systemically significant: The rules imposed will govern thousands of targeting, minimization, and querying decisions made within IC elements implementing Section 702. By contrast, most

[9] 50 U.S.C. § 1803(*i*).

other matters on the Court's docket may more closely resemble the type of fact-intensive proceedings, comparable to an application for a search warrant, that are ordinarily conducted *ex parte* in the criminal context.