Written Questions for Elizabeth Goitein
Submitted by Senator Patrick Leahy
Wednesday, November 13, 2019

1. The NSA has had to twice dump the information it had over-collected under Section 215.

    a. **Given the problems the NSA has faced with repeated over-collection, should we let the government restart its CDR program at its discretion and without additional Congressional review?**

    b. **Is there a reason we should not require the government to first come to Congress and demonstrate that it can restart the program without violating the law before reauthorizing CDR?**

The answer to both questions is no. On June 28, 2018, the NSA announced that it had been collecting information it was not authorized to collect under the CDR program. While the agency still has not publicly revealed the nature of that information or how widespread the problem was, it was prevalent enough that the agency chose to delete *all* of the data it had collected—encompassing hundreds of millions of records—since the program went into effect in 2015. At the time, the agency represented that "[t]he root cause of the problem has since been addressed for future CDR acquisitions," but four months later, the problem happened again. This time, the agency did not publicly reveal the overcollection, nor did it reveal its decision to stop operating the program; these events were discovered and made public as a result of Freedom of Information Act requests and investigative reporting.

The bar should be high for allowing the NSA to restart this program. It took the agency three years to discover what appears to have been a systemic overcollection program. Within four months, the problem the agency claimed to have fixed had recurred, and it is not publicly known how much time then elapsed before the NSA suspended the program's operation. This is not "harmless error": the quantity of information that was improperly collected during this time period, and therefore was subject to being queried and used against Americans in all types of investigations and legal proceedings, is likely to have been immense. The ODNI's own Office of Civil Liberties, Privacy, and Transparency determined that the overcollection had "a significant impact on civil liberties and privacy." If Congress were to simply allow the NSA to resume collection, this sequence of events could very well repeat itself.

If the government wants Congress to consider reauthorizing the program, it should begin by providing a detailed public explanation of the events leading to the suspension of the CDR program. This would include a description of how the problem occurred; what type of information was improperly collected; an estimate of how many records were collected that the NSA was not authorized to collect; the likely length of time that the problem went undetected, and the explanation for any delay; why the problem continued despite assurances that it was solved; when the NSA stopped collecting CDRs under the program; and why the government did not publicly report the recurrence of the problem or the suspension of the program.

In addition, the government should engage in remediation efforts beyond those it has apparently taken so far (i.e., notification to oversight bodies and review/revision of intelligence reports). To the extent it still has access to this information, the government should notify anyone whose records were improperly collected. At a minimum, it must notify individuals involved in legal proceedings if, during the course of the investigation leading up to the proceeding, the government made any use of information that was or could have been improperly obtained under the CDR program.

Of course, reauthorization should not occur if there is a possibility that similar overcollection could happen again. Given that the NSA's previous assertions that it had fixed the problem proved to be inaccurate, Congress should not simply accept the government's representations on this point. The government should be required to make a detailed demonstration to Congress, and this demonstration must be subject to evaluation by independent technical experts, who should be granted whatever clearances are necessary to perform this task.

It is not enough, however, for the government to show that the overcollection problem has been addressed. Even if that problem were solved, the CDR program would still represent a significant intrusion on Americans' privacy. According to the ODNI's annual statistical report, there were only 14 targets of collection in 2018; yet the NSA obtained almost half a million records, including information that was communicated by more than *19 million* different phone numbers. These numbers indicate that the program is sweeping in the personal information of a massive number of presumptively innocent Americans who are not themselves the target of any investigation. This is another form of "overcollection," albeit one that is written into the law.

Such a significant intrusion could be justified, if at all, only by overriding national security necessity, and only if strict minimization requirements were in place and were being scrupulously followed. It appears, however, that the program offered minimal national security benefit. Despite diligent questioning by members of Congress, the government has failed to identify even a single instance in which the CDR program contributed meaningfully to counterterrorism efforts. Indeed, according to news reports, the NSA recommended that the White House not seek renewal of the authority to conduct to CDR program. Although the administration nonetheless decided to request reauthorization, the Director of National Intelligence (DNI), in making this request, made clear that the program's costs currently outweigh any benefits, and that the request for reauthorization was based on the possibility that this could change in the future. As for minimization requirements, Congress did not include any age-off requirement for CDRs, instead relying on the agencies to "prompt[ly]" destroy records "that the Government determines are not foreign intelligence information." According to the Privacy and Civil Liberties Oversight Board (PCLOB), a similar requirement in the NSA's Section 702 minimization procedures has proven toothless in practice.

Accordingly, before even considering the reauthorization of such "bulky" collection, Congress would need proof that the program is truly necessary for our national security. More specifically, there would have to be a finding by an independent reviewer, such as the PCLOB, that the CDR program provided significant national security benefit—i.e., that in a substantial number of cases, the program provided information that otherwise could not have been obtained (e.g., using ordinary Section 215 or pen register/trap-and-trace authorities) and that was

instrumental in identifying a terrorist and/or preventing a terrorist attack. Given the government's willingness to suspend the program and its conspicuous unwillingness to say that the program made important contributions to counterterrorism efforts, it seems extremely unlikely that any such finding is forthcoming.

In addition, whether or not Congress considers reauthorizing the CDR program, Congress needs information about the effectiveness of its statutory minimization requirements. To that end, Congress should request that the government disclose how many call detail records were destroyed pursuant to the statutory minimization requirement (i.e., prior to the deletion of records in 2018); in addition, the government should disclose how many of the records that were not destroyed pursuant to the statutory minimization requirement were affirmatively determined to be foreign intelligence information. If it turns out that only a very small proportion of records were destroyed and that only a very small proportion were determined to be foreign intelligence information, that would indicate that the statutory minimization requirement is insufficient—a point that should inform legislation on other foreign intelligence authorities.

There is no reason not to require the above showings, findings, and disclosures before reauthorizing the CDR program. Indeed, the opposite is the case: there is no conceivable reason to reauthorize the program before these measures are taken. As noted above, all indications are that the program was providing minimal, if any, counterterrorism benefit. This is not a situation where allowing the authority to lapse, at least until the government can show that it is necessary and can be operated consistently with the law, would leave intelligence agencies without a critical intelligence-gathering tool. Not even the government has made this claim; officials have instead posited that the program might be useful in the future. That speculation is woefully insufficient to justify reauthorizing a program with such a troubled history—particularly in light of the government's ability to obtain call detail records under other authorities, including "traditional" Section 215, pen register/trap-and-trace, and national security letters.

2. Seemingly with every public disclosure of a FISA court opinion, the public learns of additional instances of noncompliance pertaining to Section 215, Section 702, and the FISA pen register statute.

a. What are the current limitations of Section 215 oversight?

b. How should oversight and transparency be strengthened in any reauthorization of these authorities?

As this question indicates, the government has a dismal record of compliance with the limits on collecting, accessing, sharing, and retaining information collected under foreign intelligence authorities. Moreover, contrary to claims by government officials that there has been no deliberate abuse of these programs, a recently released FISA Court opinion recounts instances of FBI officials querying Section 702 data for personal reasons—e.g., to access the communications of colleagues or relatives. Chillingly, the FISA Court suggested that such abuse was inevitable: "It would be difficult to completely prevent personnel from querying data for personal reasons."

These same opinions posit some reasons why internal oversight mechanisms are not working well. For one thing, overseers are able to review only a small fraction of what takes place under these programs. Some FBI field offices, for instance, go for periods of two years or more between oversight visits. The FISA Court also noted that the FBI sends its agents mixed messages, encouraging maximal use of data while simultaneously purporting to impose "minimization" requirements.

As for external oversight mechanisms—such as Congress, the FISA Court, and the PCLOB—these entities have little independent ability to detect noncompliance incidents; they are instead limited by what information the agencies provide and when they provide it. In case after case, the government did not detect and/or report violations to the FISA Court until long after the fact (and there is no reason to think it was any more prompt in notifying Congress or the PCLOB in those instances). The FISA Court has attributed the delayed reporting to "institutional lack of candor." Needless to say, institutional lack of candor with external overseers greatly inhibits oversight.

Moreover, even when the government reports violations, both Congress and the FISA Court have been extremely reluctant to impose meaningful consequences on intelligence agencies (and the PCLOB has no power to do so). The recently released FISA Court opinions, for instance, are full of harsh words, but require only more recordkeeping. Even when it emerged that the NSA had been collecting Americans' telephone calls in bulk—a massive abuse of Section 215—Congress allowed the NSA to retain a scaled-down version of bulk collection in the form of the CDR program. Oversight is far less effective when not coupled with accountability.

I recommended some enhancements to oversight and transparency provisions in my written testimony. Not all of these changes would necessarily help in detecting or deterring noncompliance. However, they would provide important information to lawmakers and the public regarding how the government interprets and implements its authorities—information that is critical to the democratic decisionmaking process. These measures include:

- As outlined in response to Question 3, below, provisions relating to the use of FISA Court *amici* and disclosure of FISA Court opinions should be strengthened.
- As set out in my written testimony, the government should be required to disclose an estimate of how many individuals are encompassed within the SSTs it employs, within bands of 100 (e.g., "ten section 215 orders were based on SSTs that likely encompassed between 101-200 individuals"). It should also be required to provide a comprehensive list of the types of "tangible things" obtained under Section 215.
- The FBI should be required to report the number of U.S. person queries it conducts of databases containing communications obtained under Section 702.
- The DNI should be required to provide a good faith estimate of the number of communications collected under Section 702 in which at least one of the communicants is a U.S. person.
- The current statutory requirement to report how many "unique identifiers used to communicate information collected" fails to capture the true number of individuals

affected by Section 215 collection. Congress should replace or supplement this metric with a requirement to provide an estimate, based on any type of unique identifiers appearing in the records, of the number of individuals about whom information is collected.

- Congress should require the government to provide notice to parties in legal proceedings when using evidence "derived from" Section 215, and it should define "derived from" to prohibit the practice of parallel construction and to bar assertions of "inevitable discovery."

Although these changes would be helpful, it is critical to remember that oversight and transparency are not ends in themselves. The main purposes of oversight and transparency are to ensure compliance with the applicable rules, and to shed light on ways in which those rules are operating in practice. If, as a result of oversight and transparency measures, we learn that the substantive rules governing the programs are not sufficient to protect Americans' privacy (e.g., because they still permit the collection large amounts of innocuous information), more oversight and transparency will not solve this problem. Similarly, if the government repeatedly proves to be incapable of consistent compliance even when elaborate oversight mechanisms have been imposed, continuing to layer on more oversight is not an adequate solution. At some point, the government's long history of systemic noncompliance with the rules designed to protect Americans' privacy must inform, not just what oversight measures are necessary, but what surveillance authority Congress is willing to give the government in the first instance.

3. The USA FREEDOM Act mandated that the FISA Court appoint amici in cases involving novel or significant interpretations of law.

    a. Would it be beneficial to the FISA Court process to expand the cases in which amici may participate, for example to cases involving novel applications of technology?

Yes. Currently, the appointment of amici is required (absent a written finding that participation would be "not appropriate") in cases presenting "a novel or significant interpretation of the law." The rationale for this requirement is that the FISA Court would benefit from hearing more than one perspective in cases that raise new and unsettled legal issues. The same is true, however, for cases that are novel in other ways, including cases that involve the application of new surveillance technologies or those that involve novel applications of existing technologies. The argument for appointing amici is particularly strong in cases that address programmatic surveillance authorities, such as Section 702, as the approval of program-wide policies—unlike the approval of individual warrant applications—is not the type of activity courts normally conduct *ex parte*.

Accordingly, Congress should require the FISA Court to appoint amici—including at least one amicus with expertise in civil liberties, as discussed in my written testimony—when considering cases that involve either the application of new surveillance technologies, novel applications of existing technologies, or approval of programmatic surveillance.

b. Should a schedule exist that requires novel or significant opinions from the FISA Court be released within a certain period of time?

Yes. The timing of last month's release of FISA Court opinions, which included an initial decision issued in October 2018, a decision on appeal issued in July 2019, and a follow-up order issued in September 2019, strongly suggests that the government delayed disclosure of the initial decision in the hope that it would prevail in its appeal to the Foreign Intelligence Surveillance Court of Review (FISCR). The opinions were not released until the FISCR rejected the government's appeal and the FISA Court approved revised procedures submitted by the government in response to these holdings. That is an unacceptable reason for delay, and it underscores the necessity of imposing a deadline. Congress should require, at a minimum, some public disclosure within six months of the issuance of a significant decision. If the declassification review is not completed by that time, the Director of National Intelligence should be required to issue an interim public statement disclosing the existence of the ruling and as fulsome a summary as the DNI is able to provide. In no instance should disclosure of the opinion be delayed beyond the period required to perform a declassification review.

Congress should also consider requiring declassification and release (on a timely basis) of the briefs filed in these cases, including those of the government and any amici. These materials would provide important context for understanding and evaluating the Court's opinions. They would also assist lawmakers and the public in understanding how the non-adversarial nature of FISA Court proceedings affects the government's submissions, and how the amicus provisions of the law are functioning in practice.

Senate Judiciary Committee
"Reauthorizing the USA FREEDOM Act of 2015"
Questions for the Record
November 13, 2019
Senator Amy Klobuchar

Question for Elizabeth Goitein, Brennan Center for Justice

In your testimony, you expressed concerns about the surveillance programs that the USA FREEDOM Act would reauthorize and recommended prohibiting the government from using race, religion, ethnicity, nationality, or any other constitutionally protected characteristic as a consideration in deciding whether to conduct surveillance.

- Can you describe how surveillance that is predicated on these types of protected characteristics could negatively affect the quality of our intelligence gathering and law enforcement efforts?

Surveillance that is predicated, either in whole or in part, on constitutionally protected characteristics or activities directly harms the targeted individuals, stigmatizes their communities, and inhibits their freedom of expression, religion, and assembly. More generally, it erodes the constitutional values upon which this country is based. It goes against what our nation stands for.

As this question recognizes, however, the damage does not end there. Surveillance based on race, religion, ethnicity, nationality, or First Amendment-protected activity harms our security by diverting resources and attention from true threats, making it more likely that actual terrorists and criminals will go undetected. Every hour that an FBI agent spends monitoring a peaceful protest is an hour not spent following up on leads pertaining to actual criminal activity. Discriminatory surveillance also undermines the public's trust in law enforcement and intelligence agencies, which in turn inhibits community partnerships that are vital to effective intelligence collection. And perceptions that the United States engages in discriminatory surveillance could make our foreign partners less willing—or even less able, under their own laws—to cooperate in intelligence collection efforts.

Government officials deny that intelligence and law enforcement agencies base investigative actions and priorities on factors such as race or political beliefs. But there is ample evidence that they have done so, not just during the J. Edgar Hoover decades but in modern times as well. Examples include post-9/11 FBI policies of "ethnic mapping"[1] and sending informants into mosques simply to report on what attendees were saying;[2] extensive monitoring,

[1] *See* Charlie Savage, *F.B.I. Scrutinized for Amassing Data on American Communities*, N.Y. TIMES (Oct. 20, 2011), *available at* https://www.nytimes.com/2011/10/21/us/aclu-releases-fbi-documents-on-american-communities.html.
[2] *See* Trevor Aaronson, *The Informants*, MOTHER JONES (Sept./Oct. 2011), *available at* https://www.motherjones.com/politics/2011/07/fbi-terrorist-informants/.

in recent years, of activists engaged in peaceful protests regarding immigration policies,[3] climate change,[4] and racial justice;[5] and the creation of a fictional ideology labeled "Black Identity Extremism" to justify race-based investigative activity.[6]

Congress should enact a strong statutory prohibition on such practices. Foreign intelligence authorities currently include no express prohibition on collection that is based on constitutionally protected characteristics. While they bar intelligence collection based "solely" on activities protected by the First Amendment, that leaves room for surveillance that is partly or even mostly based on protected speech, association, or religious belief. There is no principled reason why "a little discrimination" should be tolerated. Congress should prohibit the government from engaging in surveillance with the intent or effect of discriminating on the basis of race, religion, ethnicity, nationality, or any other protected characteristic. In addition, Congress should prohibit surveillance that is motivated or predicated to any degree on conduct, expression, or other activity that is protected by the First Amendment.

---

[3] Jana Winter & Hunter Walker, *Exclusive: Document Reveals the FBI Is Tracking Border Protest Groups as Extremist Organizations*, Yahoo News (Sept. 4, 2019), *available at* https://news.yahoo.com/exclusive-document-reveals-the-fbi-is-tracking-border-protest-groups-as-extremist-organizations-170050594.html.

[4] Adam Federman, *Revealed: FBI Kept Files on Peaceful Climate Change Protesters*, THE GUARDIAN (Dec. 13, 2018), *available at* https://www.theguardian.com/us-news/2018/dec/13/fbi-climate-change-protesters-iowa-files-monitoring-surveillance-.

[5] George Joseph, *Exclusive: Feds Regularly Monitored Black Lives Matter Since Ferguson*, THE INTERCEPT (July 24, 2015), *available at* https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson/.

[6] Benjamin Fearnow, *FBI Ranks 'Black Identity Extremists' Greater Threat than Al Qaeda, White Supremacists: Leaked Documents*, Newsweek (Aug. 8, 2019), available at https://www.newsweek.com/fbi-leak-black-identity-extremist-threat-1453362.

Ms. Elizabeth Goitein –
Reauthorizing the USA FREEDOM Act of 2015
Questions for the Record
Submitted November 13, 2019

QUESTIONS FROM SENATOR COONS

1. While the Supreme Court was careful to limit its decision in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), to a domestic criminal case, it does set out a class of information that triggers Fourth Amendment privacy protections, even when that information is held by a third party. What information falls into this category?

The Supreme Court's holding in *Carpenter* was, on its face, a narrow one: "Whether the Government employs its own surveillance technology . . . or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI [cell site location information]." The Court listed several questions that it was neither addressing nor resolving in its decision:

> Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or "tower dumps" (a download of information on all the devices that connected to a particular cell site during a particular interval). We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information. Further, our opinion does not consider other collection techniques involving foreign affairs or national security. As Justice Frankfurter noted when considering new innovations in airplanes and radios, the Court must tread carefully in such cases, to ensure that we do not "embarrass the future." Northwest Airlines, Inc. v. Minnesota, 322 U. S. 292, 300 (1944).

Accordingly, the only practice that is specifically prohibited by *Carpenter* is the warrantless collection of historical cell site location information. Note that such collection is barred in both criminal and foreign intelligence investigations; while the Court stated that its decision did not reach "*other* collection techniques involving foreign affairs or national security" (emphasis added), it made no such disclaimer with respect to the collection technique at issue in the case (i.e., obtaining historical CSLI from wireless providers).

While it makes sense for courts to avoid ruling on fact patterns that are not immediately before them, Congress does not have that luxury. It is incumbent upon Congress, when renewing Section 215 and other collection authorities, to assess how the principles articulated in *Carpenter* apply to the practices being authorized. Several clear principles emerge from the Court's decision:

- Case law developed long before the digital era does not necessarily map onto today's high-tech surveillance techniques. (The Court cautioned that *Smith v. Maryland* and *United States v. Miller*, the cases establishing the so-called "third-party doctrine," should

not be "mechanically" applied to "novel circumstances" that that "few could have imagined" in 1979, when those cases were decided.)

- The "third-party doctrine" is not absolute. ("[T]he fact that . . . information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection.")

- The sharing of information is not truly voluntary, and therefore does not constitute a waiver of privacy rights, if disclosure to a third party is necessary to participate in modern society. (The Court noted that, unlike the information at issue in *Smith* and *Miller*, cell phone location information is not truly "shared" with wireless providers, as the term is normally understood, in part because "cell phones and the services they provide are such a pervasive and insistent part of daily life that carrying one is indispensable to participation in modern society" (internal quotation marks omitted).)

- Whether a person retains a reasonable expectation of privacy in records held by third parties also depends on the information reflected in those records. (The Court observed that *Smith* and *Miller* "did not rely solely on the act of sharing. Instead, they considered 'the nature of the documents sought' to determine whether 'there is a legitimate "expectation of privacy" concerning their contents.'")

- The more sensitive and revealing the third-party records, the more likely it is that a person retains a reasonable expectation of privacy in them. (The Court held that Carpenter had a reasonable expectation of privacy in the seized data in part because such historical CSLI "provides an intimate window into a person's life" and "hold[s] for many Americans the privacies of life" (internal quotation marks omitted).)

- The ease with which the government can collect large amounts of data is relevant to the intrusion on privacy. ("[C]ell phone tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools. With just a click of a button, the Government can access each carrier's deep repository of historical location information at practically no expense.")

- Also relevant to the privacy calculus is the government's ability to capture retrospective data that would otherwise be lost. ("[T]he retrospective quality of the data here gives police access to a category of information otherwise unknowable.")

Applying these principles, it is clear that some collection techniques that are currently authorized under Section 215, pen register/trap-and-trace (PR/TT), and national security letters (NSLs) implicate the Fourth Amendment and should require a warrant. Section 215 itself helpfully identifies types records that are particularly sensitive (and therefore require higher-level internal sign-off to collect under the statute): library circulation records, library patron lists, books sales records, book customer lists, firearm sales records, tax return records, educational records, and medical records containing information that would identify a person. Congress should require a warrant to obtain these records. It should also require a warrant for geolocation information collected through any means, biometric information, records reflecting web

browsing activity, and any records that shed light on Americans' exercise of constitutional rights, such as records of participation in political organizations or events. The sensitivity of these types of information is self-evident.

This list is not and cannot be comprehensive; Section 215 authorizes the collection of "any tangible thing," and it is impossible to posit every "thing" the government might attempt to obtain. Therefore, in addition to specifying that the above categories of information may only be obtained with a warrant, Congress should provide that the government's authority to obtain information or other tangible things without a warrant under Section 215, PR/TT, and NSLs cannot extend beyond the government's authority to obtain the same information/items without a warrant in a criminal investigation, using means other than a grand jury subpoena. As noted in my written testimony, a grand jury subpoena is not an apt comparison because it carries with it protections that are not present in foreign intelligence investigations—most notably, the limited function of the grand jury itself and its role as a check on law enforcement powers.

The government will likely argue that, even if the Fourth Amendment applies to these types of records, warrants are unnecessary under the "foreign intelligence exception" to the warrant requirement. Not even the FISA Court, however, has held that the foreign intelligence exception applies in cases where the target is an American who is not acting an agent of a foreign power. And even for American targets who *are* acting as agents of a foreign power, Congress has required the government to obtain a form of warrant (namely, a FISA Title I order based on an individualized "probable cause" showing) when collecting highly sensitive information, namely, electronic communications. Accordingly, there should be no exception to the warrant requirement for the types of information identified above.

2. You have, in past writings, indicated that you do not believe that the process protections implemented by the Federal Bureau of Investigation are sufficient to protect against future misuse of Section 702 data. Are there protections, other than limiting collection, which you believe would be effective in properly limiting queries?

As I have written, I believe that the Fourth Amendment requires the government to obtain a warrant before using search terms associated with U.S. persons to query data obtained under Section 702. Even if a warrant is not *constitutionally* required, however, Congress can and should require the government to obtain one. It has become abundantly clear that nothing short of a warrant will provide sufficient protection for Americans' privacy interests.

For one thing, the standard that agencies have adopted for querying data is far too low. Agencies may run U.S. person queries against Section 702 data as long as the queries are "reasonably likely" to return "foreign intelligence information." The FBI can also run U.S. person queries that are "reasonably likely" to return "evidence of a crime." The FBI is permitted to run these queries at the assessment phase of an investigation—i.e., before there is *any factual predicate* to support suspicion of criminal activity, let alone probable cause. On this extremely low standard, the government is permitted to read Americans' e-mails and texts and listen to their phone calls—the most personal and sensitive information imaginable.

Moreover, multiple FISA Court opinions have shown that agencies have continually failed to adhere even to this unreasonably low standard. Most recently, a set of FISA Court opinions released in October 2019 revealed that FBI officials had conducted a "large number" of queries that "were not reasonably likely to return foreign-intelligence information or evidence of a crime." This was not the first time the FBI had failed to adhere to the rules governing the handling of, and access to, information collected under Section 702. As elaborated in my written testimony, the government systematically failed to properly minimize and limit access to data obtained through "upstream collection" from the very inception of the program until "abouts" collection was terminated in 2017. It is no exaggeration to say that the government has *never* been in full compliance with the rules that govern the handling and querying of Section 702 data, despite the elaborate internal oversight structures the government often cites.

Under these circumstances, it is plainly insufficient to rely on self-policing by the agencies punctuated by periodic programmatic review by the FISA Court. Nor is there any legitimate policy reason to allow the government freer access to Americans' most sensitive information—their personal correspondence—under Section 702 than under other surveillance authorities. Accordingly, before accessing Americans' communications, the government should be required to show probable cause to a neutral magistrate, on an individualized basis, that the communications contain evidence of criminal activity or that the American is a foreign power or agent of a foreign power.

Elizabeth Goitein
Director
Liberty & National Security Program
Brennan Center for Justice at
New York University School of Law
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?

I'm not aware of any such instance.

   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?

That description could potentially apply to "abouts" collection—i.e., the collection of communications that are neither *to* nor *from* the target, but that merely include certain information (such as e-mail addresses or phone numbers) associated with the target. "Abouts" collection was a feature of "upstream" collection—i.e., the collection of communications as they transit the Internet backbone. Partly as a result of "abouts" collection, the government was obtaining tens and thousands of purely domestic communications that it was not authorized to acquire under Section 702. The FISA Court thus required the government to adopt special procedures for segregating, storing, retaining, and accessing communications obtained through "upstream" collection. The government, however, proved incapable of complying with these rules, and so ended the practice of "abouts" collection in the spring of 2017.

Civil liberties advocates have argued that "abouts" collection was contrary to both Section 702 and the Fourth Amendment. They urged Congress, when considering

reauthorization of Section 702 at the end of 2017, to expressly bar the government from resuming the practice. Instead, Congress for the first time expressly *permitted* the government to engage in "abouts" collection, as long as it obtained the FISA Court's permission—which it would have had to do anyway—and gave Congress 30 days' advance notice.

Subsequently, the issue of "abouts" collection came before the FISA Court. The government and amici disagreed about whether a particular type of collection in which the government was engaged constituted "abouts" collection, undertaken without the necessary permissions or notifications. In an October 2018 ruling, the FISA Court ruled in favor of the government on this question. Other aspects of the court's decision went against the government, and the government appealed to the Foreign Intelligence Surveillance Court of Review (FISCR). Amici, however, have no right to appeal rulings in the government's favor, and so the FISCR did not consider the "abouts" issue. The government has provided no public information about the collection practice that caused the controversy.

c. 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?

In its June 2018 announcement, the NSA stated only that it had noticed "technical irregularities in some data received from telecommunications service providers," and that these "irregularities also resulted in the production to NSA of some CDRs that NSA was not authorized to receive." A *New York Times* article covering the announcement stated that, according to an interview with the NSA's general counsel, "one or more telecom providers . . . had responded to court orders for targets' records by sending logs to the agency that included both accurate data and also some numbers of people the targets had not been in contact with. As a result, when the agency then fed those phone numbers back to the telecoms to get the communications logs of all of the people who had been in contact with its targets, the agency also gathered some data of people unconnected to the targets."

Beyond these statements and various reiterations of them, the government has notably failed to make any public disclosure regarding the type of information that was wrongly collected and the extent of the problem. Observers have developed differing theories, but until further information is obtained from the government, we have no definitive answers. In his hearing testimony, Privacy and Civil Liberties Oversight Board (PCLOB) Chair Adam Klein stated that the PCLOB had recently submitted a 116-page draft report to the intelligence community for declassification review, and that the report contained a "comprehensive account" of the technical and operational issues cited by the NSA in its public statements. Members of the committee should put pressure on the Acting Director of National Intelligence to ensure that this review is conducted as quickly as possible, and that the report is declassified and made public to the maximum extent possible consistent with national security.

d. 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 and communications habits will continue to evolve and adapt."[1] From your vantage point, how might this statutory authority be used in the future if it is reauthorized?

The specter of changing technology and an evolving threat is routinely invoked by the government when seeking to retain authority for activities with no proven national security value. Unfortunately, the government rarely provides any specifics that would enable Congress to evaluate this claim—and it has not done so here. How, exactly, might technology change in a way that would render the CDR program valuable? Members of Congress are left to speculate about what kinds of changes the DNI was referring to, and how likely those changes are.

Ultimately, such speculation is unnecessary. If a surveillance program that has been used to acquire more than a billion phone records associated with more than 19 million phone numbers is not currently providing much counterterrorism value, it should not be reauthorized. If, in the future, there are specific changes in factual circumstances that would directly bear on the program's usefulness, nothing prevents the government from returning to Congress to seek reinstatement of the authority. In the meantime, the government is able to obtain CDRs using multiple other authorities, including "traditional" Section 215, pen register/trap-and-trace, and national security letters.

[1] 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.

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?

The fact that the government has never used the "lone wolf" provision *is* the metric that Congress can and should use in assessing its intelligence value. In recent testimony, government officials have argued that this authority is important because it enables surveillance of individuals who are radicalizing online, without any direct connection to an international terrorist group. But this type of online radicalization has been a central focus of our law enforcement and intelligence agencies for well over a decade. The fact that the government has not used this authority even once in 15 years is conclusive evidence that it has sufficient authority to conduct surveillance of so-called "lone wolves" under other statutory provisions.

Indeed, given how lone wolves are defined in the statute—i.e., "any person other than a United States person" who "engages in international terrorism or activities in preparation therefore"—it is clear that the government could obtain ordinary criminal warrants to conduct surveillance in these cases. Acts of international terrorism are crimes under U.S. law. Accordingly, if the government can show probable cause that someone is engaged or is preparing to engage in international terrorism, as would be required to activate the "lone wolf" authority, it follows that the government can show probable cause of criminal activity. This presumably explains why the government has never felt the need to invoke the "lone wolf" provision.[2]

3. During the hearing, this Committee heard testimony about the U.S. Supreme Court's recent decision in *Carpenter v. United States*.[3] As you testified, "the Court in *Carpenter* essentially held that there are certain types of information that are so sensitive, so 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."[4]

   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*?

The Supreme Court's holding in *Carpenter* was, on its face, a narrow one: "Whether the Government employs its own surveillance technology . . . or leverages the technology of

[2] In my written testimony, I addressed another provision of the USA PATRIOT Act that is scheduled to expire: the so-called "roving wiretap" provision. Two of the footnotes in that part of my testimony contained erroneous citations. The "ascertainment" requirement in the criminal counterpart to the roving wiretap authority appears at 18 U.S.C. § 2518(11)(b)(iv), not at 18 U.S.C. § 2518(11), (12) as stated in footnote 140. Additionally, in the criminal provision, the requirement that the government specify the identity of the target (in cases where the facility is not specified) appears at 18 U.S.C. § 2518(b)(ii), not 18 U.S.C. § 2511(b)(ii) as stated in footnote 141.
[3] 138 S. Ct. 2206 (2018).
[4] *Senate Judiciary Committee Holds Hearing on USA FREEDOM Legislation Reauthorization*, CQ CONG. TRANSCRIPTS (Nov. 6, 2019), https://plus.cq.com/doc/congressionaltranscripts-5765239.

a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI [cell site location information]." The Court listed several questions that it was neither addressing nor resolving in its decision:

> Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or "tower dumps" (a download of information on all the devices that connected to a particular cell site during a particular interval). We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information. Further, our opinion does not consider other collection techniques involving foreign affairs or national security. As Justice Frankfurter noted when considering new innovations in airplanes and radios, the Court must tread carefully in such cases, to ensure that we do not "embarrass the future." Northwest Airlines, Inc. v. Minnesota, 322 U. S. 292, 300 (1944).

Accordingly, the only practice that is specifically prohibited by *Carpenter* is the warrantless collection of historical cell site location information. Note that such collection is barred in both criminal and foreign intelligence investigations; while the Court stated that its decision did not reach "*other* collection techniques involving foreign affairs or national security" (emphasis added), it made no such disclaimer with respect to the collection technique at issue in the case (i.e., obtaining historical CSLI from wireless providers).

While it makes sense for courts to avoid ruling on fact patterns that are not immediately before them, Congress does not have that luxury. It is incumbent upon Congress, when renewing Section 215 and other collection authorities, to assess how the principles articulated in *Carpenter* apply to the practices being authorized. Several clear principles emerge from the Court's decision:

- Case law developed long before the digital era does not necessarily map onto today's high-tech surveillance techniques. (The Court cautioned that *Smith v. Maryland* and *United States v. Miller*, the cases establishing the so-called "third-party doctrine," should not be "mechanically" applied to "novel circumstances" that that "few could have imagined" in 1979, when those cases were decided.)

- The "third-party doctrine" is not absolute. ("[T]he fact that . . . information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection.")

- The sharing of information is not truly voluntary, and therefore does not constitute a waiver of privacy rights, if disclosure to a third party is necessary to participate in modern society. (The Court noted that, unlike the information at issue in *Smith* and *Miller*, cell phone location information is not truly "shared" with wireless providers, as the term is normally understood, in part because "cell phones and the services they

provide are such a pervasive and insistent part of daily life that carrying one is indispensable to participation in modern society" (internal quotation marks omitted).)

- Whether a person retains a reasonable expectation of privacy in records held by third parties also depends on the information reflected in those records. (The Court observed that *Smith* and *Miller* "did not rely solely on the act of sharing. Instead, they considered 'the nature of the documents sought' to determine whether 'there is a legitimate "expectation of privacy" concerning their contents.'"

- The more sensitive and revealing the third-party records, the more likely it is that a person retains a reasonable expectation of privacy in them. (The Court held that Carpenter had a reasonable expectation of privacy in the seized data in part because such historical CSLI "provides an intimate window into a person's life" and "hold[s] for many Americans the privacies of life" (internal quotation marks omitted).)

- The ease with which the government can collect large amounts of data is relevant to the intrusion on privacy. ("[C]ell phone tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools. With just a click of a button, the Government can access each carrier's deep repository of historical location information at practically no expense.")

- Also relevant to the privacy calculus is the government's ability to capture retrospective data that would otherwise be lost. ("[T]he retrospective quality of the data here gives police access to a category of information otherwise unknowable.")

Applying these principles, it is clear that some collection techniques that are currently authorized under Section 215, pen register/trap-and-trace (PR/TT), and national security letters (NSLs) implicate the Fourth Amendment and should require a warrant. Section 215 itself helpfully identifies types records that are particularly sensitive (and therefore require higher-level internal sign-off to collect under the statute): library circulation records, library patron lists, books sales records, book customer lists, firearm sales records, tax return records, educational records, and medical records containing information that would identify a person. Congress should require a warrant to obtain these records. It should also require a warrant for geolocation information collected through any means, biometric information, records reflecting web browsing activity, and any records that shed light on Americans' exercise of constitutional rights, such as records of participation in political organizations or events. The sensitivity of these types of information is self-evident.

This list is not and cannot be comprehensive; Section 215 authorizes the collection of "any tangible thing," and it is impossible to posit every "thing" the government might attempt to obtain. Therefore, in addition to specifying that the above categories of information may only be obtained with a warrant, Congress should provide that the government's authority to obtain information or other tangible things without a warrant under Section 215, PR/TT, and NSLs cannot extend beyond the government's authority to obtain the same information/items without a warrant in a criminal investigation, using means other than a grand jury subpoena. As noted in my written testimony, a grand jury subpoena is not an apt comparison because it carries with it protections that are not present in foreign

intelligence investigations—most notably, the limited function of the grand jury itself and its role as a check on law enforcement powers.

The government will likely argue that, even if the Fourth Amendment applies to these types of records, warrants are unnecessary under the "foreign intelligence exception" to the warrant requirement. Not even the FISA Court, however, has held that the foreign intelligence exception applies in cases where the target is an American who is not acting an agent of a foreign power. And even for American targets who *are* acting as agents of a foreign power, Congress has required the government to obtain a form of warrant (namely, a FISA Title I order based on an individualized "probable cause" showing) when collecting highly sensitive information, namely, electronic communications. Accordingly, there should be no exception to the warrant requirement for the types of information identified above.

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.[5] In that vein, Mr. Wiegmann told the Committee that "you could not get Fourth Amendment protected content with a business records order."[6]

   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?

Yes. Section 215 itself contemplates the acquisition of "library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person." As discussed above in my answer to Question 3, under the general principles articulated in *Carpenter,* these types of highly sensitive information are likely protected by the Fourth Amendment even when held by third parties.

Mr. Wiegmann's statement that "you could not get Fourth Amendment protected content with a business records order" begs the question of what information the government interprets as meriting Fourth Amendment protection in light of the *Carpenter* decision. According to government officials, the Department of Justice has issued no general guidance on this point; it is addressing the matter on a case-by-case basis, and is not making the resulting analyses (if any) public. However, it can be inferred from Mr. Wiegmann's statement that the government does *not* believe that library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records merit Fourth Amendment protection. This merely underscores the importance of Congress taking *Carpenter* into account when reauthorizing

[5] *Id.*
[6] *Id.*

Section 215 and other authorities, as the executive branch is likely to apply an unduly cramped reading of that case.

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.[6]

    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?

    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?

    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.

The amicus provisions of the USA FREEDOM Act were a critical innovation and have proven to be beneficial in practice. Nonetheless, the past four years have revealed some key shortcomings in these provisions. There are several steps Congress should take to ensure that the full potential of this concept is realized.

The first problem relates to the qualifications and role of amici. Under the USA FREEDOM Act, appointed amici need not possess expertise in privacy and civil liberties; they are eligible if they possess expertise "in privacy and civil liberties, intelligence collection, communications technology, *or* any other area that may lend legal or technical expertise" (emphasis added). While FISA Court opinions suggest that amici have occasionally presented forceful arguments for strong civil liberties protections, they have at other times taken positions that fall far short of what an advocate for the target of surveillance would have argued. This is perhaps unsurprising, as some of the appointed amici have no significant background in civil liberties, and the law does not require them to assume the role of the government's adversary.

This state of affairs does not cure the fundamental problem that the *amicus* provision was meant to address: the lack of adversariality in the proceedings resulting from the fact that the target of surveillance is not represented. Congress should therefore require the FISA Court, in every significant case, to appoint an amicus with expertise in civil liberties. While that person would not be representing the target of surveillance, Congress should specify that his or her role is to articulate any constitutional or other civil liberties concerns with the government's position. If the Court is interested in hearing from other types of experts, it can appoint additional amici.

Second, the USA FREEDOM Act requires the FISA Court to appoint an amicus in any case that, in the Court's view, "presents a novel or significant interpretation of law," unless the Court issues a finding that such appointment is "not appropriate." The rationale for

this requirement is that the Court would benefit from hearing more than one perspective in cases that raise new and unsettled legal issues. The same is true, however, for cases that are novel in other ways, including cases that involve the application of new surveillance technologies or those that involve novel applications of existing technologies. The case for appointing amici is particularly strong in cases that address programmatic surveillance authorities, such as Section 702, as the approval of program-wide policies—unlike the approval of individual warrant applications—is not the type of activity courts normally conduct *ex parte*. Accordingly, Congress should require the FISA Court to appoint amici when considering cases that involve either the application of new surveillance technologies, novel applications of existing technologies, or approval of programmatic surveillance.

Third, the USA FREEDOM Act provides that amici must have access to any legal precedent the Court deems relevant; access to other classified information is permitted "only if [the amicus] is eligible for access to classified information and to the extent consistent with the national security of the United States." Congress should revise this provision to ensure that amici have full access to the materials before the Court. The law already limits amici to "persons who are determined eligible for access to classified information necessary to participate in matters before the [FISA Court]." There is no legitimate reason to deny access to amici who have been given the necessary clearances.

Fourth, amici have no right to appeal a decision, regardless of the novelty of significance of the issue, and the FISA Court generally has not availed itself of the option to certify questions to the Foreign Intelligence Surveillance Court of Review (FISCR). The very existence of a FISCR, however, confirms what is intuitively clear: that courts can reach erroneous conclusions of law or fact, and that appellate review is critical for correction of such errors. Under the current system, erroneous decisions against the government are subject to correction on appeal, but erroneous decisions in the government's favor will remain on the books, undermining the integrity and quality of the case law. Congress should address this problem by requiring FISA Court judges to certify cases to the FISCR for review if the Court has rejected arguments made by amici.