**Senate Committee on the Judiciary**

**"Continued Oversight of the Foreign Intelligence Surveillance Act"**

**October 2, 2013**

**Questions for the Record from Ranking Member Charles E. Grassley**

**Professor Laura Donohue**

1. **Do you believe that in a typical criminal investigation, the government should be required to obtain a search warrant in order to obtain telephone records or other telephone metadata, even though these materials are in the possession of a third party? If so, how would that legal rule affect these investigations, in which prosecutors currently obtain such records with a grand jury subpoena?**

*Response:*

In *Smith v. Maryland*, the Supreme Court held that a pen register placed on a telephone line did not constitute a search within the meaning of the Fourth Amendment, because persons making phone calls do not have a reasonable expectation that the numbers they dial will remain private.[1] The key sentence from the decision centered on the customer's relationship with the telephone company. Namely "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[2] It is this sentence that spawned what has come to be known as "third party doctrine."[3]

The government relies on this opinion and the resultant third party doctrine to argue that, as in a typical criminal investigation, the bulk collection of U.S. persons' records in the telephony metadata program is constitutional. In its August 2013 *White Paper*, for instance, the Department of Justice suggests that a Section 215 order is not a search, because the Supreme Court "has expressly held [that] participants in telephone calls lack any reasonable expectation of privacy under the Fourth Amendment in the telephone

[1] Smith v. Maryland, 442 U.S. 735, 743-46 (1979). For more detailed discussion of the questions posed and further exposition of the points raised in this response, *see* Laura K. Donohue, *Written Testimony*, Senate Committee on the Judiciary, Continued Oversight of the Foreign Intelligence Surveillance Act, Oct. 2, 2013; and Laura K. Donohue, *Bulk Metadata Collection:*

[2] *Id.*

[3] *See also* U.S. v. Miller, 425 U.S. 435 (1976) (extending third party doctrine to banking records). *But see* U.S. v. Warshak, 631 F.3d 266 (6th Cir. 2010) (declining to extend third party doctrine to email stored with an Internet Service Provider on the grounds that customers have a reasonable expectation of privacy in their email).

numbers dialed."[4] In *ACLU v. Clapper*, the government again cites to the Court's reasoning in *Smith v. Maryland*, that, even if a subscriber harbored a subjective expectation that the numbers dialed would remain private, it would not be reasonable, since individuals have "no legitimate expectation of privacy in information" voluntarily turned over "to third parties."[5] The government suggests that because Courts subsequently followed *Smith* to find no reasonable expectation of privacy in email to/from and Internet protocol addressing information, as well as subscriber information, "*Smith* is fatal to Plaintiffs' claim that the collection of metadata records of their communications violates the Fourth Amendment."[6]

Judge Claire Eagan of the Foreign Intelligence Surveillance Court similarly relied almost exclusively on *Smith v. Maryland* in her recently-declassified August 2013 opinion: "The production of telephone service provide metadata is squarely controlled by the U.S. Supreme Court decision in *Smith v. Maryland*."[7] In the normal course of business, she explained, telephone service providers maintain call detail records—records about which customers are aware. Customers therefore assume the risk that the telephone company will provide the information to the government.[8] That bulk collection of such information was involved was of no consequence: "[W]here one individual does not have a Fourth Amendment interest, grouping together a large number of similarly-situated individuals cannot result in a Fourth Amendment interest springing into existence *ex nihilo*."[9]

The problem with these arguments is that they fail to consider the specific facts and circumstances that the Court faced in *Smith,* in which the police targeted one suspect for a limited period of time, for a specific purpose. They also fail to address critical ways in which the privacy interests impacted by the use of pen registers and their application to broad sectors of the population have changed as technology has advanced.[10] These factors distinguish the way in which third party doctrine works in the typical criminal case contemplated by Senator Grassley's question from the way in which the government is now collecting metadata under Section 215.

In 1976, Patricia McDonough was robbed in Baltimore, Maryland. After providing a description of the robber and a 1975 Monte Carlo she had seen near the scene of the crime to the police, she started

[4] Administration White Paper: Bulk Collection of Telephony Metadata under Section 215 of the USA Patriot Act 2 (Aug. 9, 2013), at 19, *available at* https://www.documentcloud.org/documents/750211-administration-white-paper-section-215.html.
[5] Defendants' Memorandum of Law in Support of Motion to Dismiss the Complaint, ACLU v. Clapper, 13 Civ. 3994,32-33 (quoting Smith v. Maryland, 432 U.S. 735 (1979) at 743-744).
[6] *Id.* at 33.
[7] In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible things from [REDACTED], No. BR 13-109, slip op. at 6.. The only other case directly cited in her Fourth Amendment discussion appears to be a decision of the FISC court itself, with secondary citations. The details of the secret court opinion that she cites as precedent, however, are redacted.
[8] *Id*. at 7-8.
[9] *Id*. at 9.
[10] This failure underscores the absence of opposing counsel—an omission that would seem to be of particular import when assessing constitutional concerns.

receiving threatening and obscene phone calls from a man who identified himself as the robber. The caller at one point asked her to step out onto her front porch. When she did so, she saw the 1975 Monte Carlo driving slowly past her home. The police observed a car of the same description in her neighborhood. Tracing the license plate, police discovered that the car was registered to Michael Lee Smith.[11] The following day, the police asked the telephone company to install a pen register to trace the numbers called from Smith's home telephone. The company agreed, and that day Smith called McDonough's home. On the basis of this and other information, the police obtained a search warrant. Upon executing it, they found a telephone book in Smith's home, with the corner turned down to McDonough's name and number. In a six-man lineup, McDonough identified Smith as the person who robbed her.[12]

The police did not obtain a warrant prior to placing the pen register. But reasonable suspicion had been established that the target of the surveillance, Michael Lee Smith, had robbed, threatened, intimidated, and harassed Patricia McDonough. The police, accordingly, placed the pen register consistent with their reasonable suspicion that Smith was engaged in criminal wrongdoing.

This is the context of ordinary criminal investigations, which, when conducted consistent with *Smith v. Maryland*, do not require a search warrant for third party records. The telephony metadata program takes place in an entirely different context.

The National Security Agency ("NSA") is engaging in bulk collection *absent* any reasonable suspicion that individuals, whose telephone information is being collected, are engaged in *any* wrongdoing. To the contrary, the Foreign Intelligence Surveillance Court ("FISC") acknowledges that almost *all* of the information thus obtained will bear *no* relationship whatsoever to criminal activity. The government, however, wants to place a pen register and trap and trace on everyone in the United States—essentially treating every U.S. citizen as though they are Michael Lee Smith.

In *Smith v. Maryland*, the police wanted only to record the numbers dialed from the suspect's telephone. At the time the case was decided, telephone companies were treated as utilities, with local telephone calls billed by the minute. What was unique about the technology involved in the pen register was that it could identify and record the numbers dialed from a telephone—a function that the phone company itself did not have. Its purpose was specific and limited.

In contrast, the bulk collection program collects the numbers dialed, the numbers who call a particular number, trunk information, and session times. Thus, while the police in 1979 were concerned with whether Michael Lee Smith was calling a particular number, the NSA metadata program now collects all

[11] 442 U.S. 735 (1979).
[12] *Id*.

numbers called—in the process obtaining significant amounts of information about individuals. Calls to a rape crisis line, an abortion clinic, a suicide hotline, or a political party headquarters reveal significantly more information than what was being sought in *Smith*. This makes the amount of information available significantly different.

Trunk information, moreover, reveals not just the target of a particular telephone call, but where the callers (and receivers) are located. At the time of *Smith*, the police were only able to tell when someone was located at Smith's home. The telephone did not follow Smith around. What mobile technologies mean is that the police can now ascertain where people are located—creating a second layer of surveillance based simply on trunk identifier information. The bulk collection of records means that the government has the ability to do that for not just one person, but for the entire country.

Further characteristics distinguish the case. In *Smith v. Maryland*, the police sought the information for a short period. The bulk metadata collection program, in contrast, while continued at 90-day intervals, has been operating for seven years now—and, the NSA argues—should be a permanent part of the government surveillance program.

Perhaps the most important difference between the two situations lies in the realms of technology and social construction. The extent to which we rely on electronic communications to conduct our daily lives is of a fundamentally different scale and complexity than the situation that existed at the time the Court heard arguments in *Smith*. Resultantly, the information that can be learned about not just individuals, but neighborhoods, political parties, Girl Scout troops—indeed, any social, political, or economic network—simply by the placement of a pen register or trap and trace, is light years ahead of what the Court contemplated in 1979.

The volume of communications being monitored further distinguishes the telephony metadata program from the question posed by Senator Grassley with regard to criminal investigations. Although the FISC orders that have been released and acknowledged by the government relate solely to one company (Verizon), officials have also acknowledged that the acquisition of telephony metadata extends to the largest telephone service providers in the United States: Verizon, AT&T, and Sprint.[13] This means that every time most U.S. citizens make a telephone call, the NSA is collecting the location, the number called, the time of the call, and the length of the conversation.[14] The numbers are worth noting. According to the *Wall Street Journal,* Verizon has 98.9 million wireless customers and 22.2 million

[13] Siobhan Gorman et al, *U.S. Collects Vast Data Trove*, WALL ST. J., June 7, 2013, at A1, *available at* http://on.wsj.com/11uDoue.
[14] *Id.*

landline customers; AT&T has 107.3 million wireless customers and 31.2 million landline customers, and Sprint has 55 million customers in total.[15] The program monitors hundreds of millions of people.

As for the type of information obtained, the FISC order requests that the telephone service providers give the government all "call detail information", a term that is defined by regulatory provision as:

> Any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called the time, location, or duration of any call and, for inbound calls, the number from which the call was placed and the time, location, or duration of any call.[16]

The FISC order further directs that the company provide "session identifying information", such as originating and terminating number, International Mobile Subscriber Identity number, and the International Mobile station Equipment Identity number. For most Americans, these numbers are connected to the identity of the user.[17] In addition, the FISC order directs the company to provide trunk identifier information. This data traces the route a telephone call takes, in the process establishing the location of the people taking part in the conversation.[18]

What can be done with this information is a significantly deeper intrusion on Americans' right to privacy than was at issue in *Smith*. It is easier to aggregate and analyze telephony metadata than content information precisely because it is structured.[19] Sophisticated data-mining and link-analysis programs can be applied this information, and it can do so faster, deeper, and more cheaply than in the past. Even the amount of data that can be retained for such analysis is of a radically different scale than was conceivable in 1979. From this information, the government can determine patters and relationships, such as personal details, habits, and behaviors that U.S. citizens had no intention or expectation of sharing.[20] The government can also obtain content.[21]

Even if U.S. citizens wanted to opt out of having this information collected, it would be virtually impossible to do so. There have been advances in encryption. But these technologies all revolve around content—not the metadata. Although some technologies are focused on metadata, these are not

---

[15] *Id.*
[16] 47 C.F.R. §64.2003 (2012). Senior intelligence officials have repeatedly asserted that, while they have the authority to collect GPS data, and have in the past, they are not currently doing so under the section 215 telephony metadata program. See, e.g., Statements of General Keith Alexander and Director of National Intelligence Clapper, Senate Judiciary Committee Hearing, Oct. 2, 2013; Siobhan Gorman & Julian E. Barnes, *Officials: NSA Doesn't Collect Cellphone-Location Records*, WALL ST. J., June 16, 2013, http://onlwsj.com/13MnSsp.
[17] *Continued Oversight of the Foreign Intelligence Surveillance Act, Hearing Before the S. Comm. on the Judiciary,* 113 Cong. 3 (2013) (written testimony by Edward W. Felten).
[18] *Id.*
[19] *Id.*, at 4.
[20] *Id.*, at 5.
[21] *Id.*, at 8-9.

sufficiently advanced to allow for real-time communication.[22] The option is therefore not to use a telephone. The cost of doing so, however, would lean towards divesting oneself of a role in the modern world—impacting one's social relationships, employment, and ability to conduct financial and personal affairs.

Notably, all of these considerations are focused on telephony metadata. But the logic of the government's argument, as applied to metadata generally, has virtually no limit. One could equally argue that all financial flows, Internet usage, and email exchanges are relevant to ongoing terrorism investigations under Section 215. Almost all forms of metadata could be at stake.

In summary, the situation is fundamentally different than that which prevails with regard to third party data in ordinary criminal investigations, in the course of which, consistent with *Smith v. Maryland*, the government is not required to obtain a search warrant to obtain pen register information.

2. **There is some precedent in the law for the government to collect large categories of records in bulk that may be relevant to an investigation and then to later analyze those records to determine what specific items are in fact relevant. For example, in one case a federal appeals court upheld the use of a grand jury subpoena to acquire all money order applications from a particular location above a certain monetary threshold over a period of years. The court upheld the subpoena even though, inevitably, most of the records acquired would not be associated with any criminal activity. That case is *In Re Grand Jury Proceedings: Subpoena Duces Tecum*, 827 F.2d 301 (8th Cir. 1987). Obviously, bulk collection of metadata under Section 215 is much broader than that example. Are there other ways you would distinguish cases like this, in which this type of collection has been upheld as legal, from the government's acquisition of telephone metadata under Section 215, which you contend is illegal? Would you contend that cases such as the above are wrongly decided?**

[22] *Id.*, at 7-8.

*Response:*

In *In Re Grand Jury Proceedings*, the government served two grand jury subpoenas *duces tecum* on Western Union.[23] The first required production of monthly wire transactions at the Royalle Inn, Kansas City, Missouri, for a period of 13 months.[24] The second required production of Telegraphic Money Order Applications above $1,000 from the Royalle Inn, Kansas City, Missouri, between January 1984 and February 1986.[25] Western Union moved to quash the subpoenas on the ground that they amounted to an unreasonable search and seizure in violation of the fourth amendment.[26] The government responded by alleging that drug dealers in Kansas City were using Western Union to transmit money.[27]

The 8th Circuit Court of Appeals noted that it had previously held that Western Union customers have no privacy interest in Western Union records.[28] The Court cited the Supreme Court's holding in *United States v. Miller,* in which the Supreme Court determined, consistent with *Smith v. Maryland*, that bank customers do not enjoy a legitimate expectation of privacy in bank records subject to subpoena.[29]

The Court in *In re Grand Jury* specifically noted that the request at issue—namely, the production of records from Royalle Inn—was not as sweeping as subpoenas that the judiciary had found to be outside the bounds of acceptability. In *Federal Trade Commission v. American Tobacco Co*., for instance, the Supreme Court refused to uphold the FTC's direction to two tobacco companies to produce letters and contracts.[30] The FTC had claimed "an unlimited right of access to the respondents' papers. . . relevant or irrelevant, in the hope that something [would] turn up."[31] The 8th circuit similarly declined to uphold a subpoena calling for an attorney's records over a ten-year period.[32]

The collection of all U.S. persons' telephony metadata is more properly considered in the same league as *FTC v. American Tobacco Co.* and *Schwimmer v. United States*, in which the Court recognized the overbroad use of government authority, as opposed to the more limited collection of information at issue in *In Re Grand Jury Proceedings*.

---

[23] *In Re Grand Jury Proceedings: Subpoena Duces Tecum*, 827 F.2d 301 (8th Cir. 1987).
[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] United States v. Gross, 416 F.2d 1205, 1213 (8th Cir.), *cert. denied*, 397 U.S. 1013, 90 S.Ct. 1245, 25 L.Ed.2d 427 (1969); accord, Newfield v. Ryan, 91 F.2d 700, 703 (5th Cir.), *cert denied,* 302 U.S. 729, 58 S.Ct. 54, 82 L.Ed. 563 (1937).
[29] United States v. Miller, 425 U.S. 435, 440-443, 96 S. Ct. 1619, 48 L.Ed.2d 71 (1976).
[30] FTC v. American Tobacco Co., 264 U.S. 298, 305, 44 S.Ct. 336, 337, 68 L.Ed. 696 (1924).
[31] Oklahoma Press Publishing Co. v. Walling, 327 U.S. 186, 207 n. 40, 66 S.Ct. at 505 n. 40 (quoting FTC, 264 U.S. at 305, 44 S.Ct. at 337).
[32] Schwimmer v. United States, 232 F.2d 855, 861-62 (8th Cir.), *cert denied*, 352 U.S. 833, 77 S.Ct. 48, 1 L.Ed. 2d 52 (1956).

Three points help to further distinguish the bulk collection of telephony metadata from ordinary use of subpoenas *duces tecum*: they are not to be used for fishing expeditions, they are specific, and they relate to past crimes. Remarkably, even FISC recognizes that the information collected as part of the bulk metadata program under Section 215 could not otherwise be obtained—including via subpoena *duces tecum*.

The government's contention, consistent with *United States v. R. Enters, Inc*., is that to fall outside the statutory confines, there must be no reasonable possibility that the category of materials sought under Section 215 will produce relevant information.[33] The government is correct that *United States v. R. Enters, Inc*. gave a fair amount of latitude to the standard of relevancy applied to grand jury subpoenas. But the case also established important limits. "Grand juries," the Court wrote, "are not licensed to engage in arbitrary fishing expeditions."[34]

Subpoenas may not be used to try to obtain massive amounts of information whence evidence of wrongdoing—absent prior suspicion—can be derived.[35] A grand jury, for example, could not convene in Cedar Rapids, Iowa, and simply begin collecting telephony metadata, which it could subsequently mine to find evidence of criminal behavior. To the contrary, an investigator must have a reasonable suspicion that some document or communication exists, and that it is directly relevant to the investigation in question, in order for the Court to order its production.

The courts have used this logic to quash a subpoena *duces tecum* requiring that computer hard drives and floppy disks be produced. The request was overbroad because the materials "contain[ed] some data concededly irrelevant to the grand jury inquiry."[36] In that case, the government acknowledged that irrelevant material was included in the sweep.[37] Judge Michael Mukasey quashed the subpoena on the grounds that the government could narrow the documents requested prior to acquisition. He also rejected the claim that a broad sweep of information was justified by the breadth of the investigation underway: even an "expanded investigation" did "not justify a subpoena which encompassed documents "completely irrelevant to its scope."[38]

---

[33] *See also* Daubert v. Merrell Dow Pharm., Inc., 509 U.S. 579, 587 (1993).
[34] United States v. R. Enterprises, Inc., 498 U.S. 29, 2992 (1991).
[35] *Id.*.
[36] In re Grand Jury Subpoena Duces Tecum Dated Nov. 15, 1993, 846 F. Supp. 11, 12 (S.D.N.Y. 1994).
[37] *Id*. at 13.
[38] *Id.* (quotation marks omitted). *See also* Cessante v. City of Pontiac, No. CIV. A. 07-cv-15250, 2009 WL 973339, at *7 (E.D. Mich. Apr. 9, 2009) ("While some of the information sought may be relevant or lead to relevant information, the request for 'anything and everything' is overly broad and not narrowly tailored to meet the relevancy requirements of Fed. R. Civ. P. 26(b)."); Hale v. Henkel, 201 U.S. 43, 76-77 (1906) (finding a "*subpoena duces tecum*. . . far too sweeping in its terms to be regarded as reasonable" where it did not "require the production of a single contract, or of contracts with a particular corporation, or a limited number of documents, but all understandings, contracts, or correspondence between" a company and six others, over

Almost none of the telephony metadata collected under Section 215 is related to criminal activity. In Judge Reggie Walton's words, "Ordinarily, this alone would provide sufficient grounds for a FISC judge to deny the application.[39] The principle at work here was recognized by the Eastern District of New York: "While the standard of relevancy [as applied to subpoenas] is a liberal one, it is not so liberal as to allow a party 'to roam in shadow zones of relevancy and to explore matter which does not presently appear germane on the theory that it might conceivably become so.'"[40] A subpoena *duces tecum* may not be used to compel the production of records simply because at some point, in the future, they might become relevant.

In a world limited by the physical manifestation of evidence, practicality helped to cabin the scope of subpoenas. Technology may have changed what is possible in terms of the volume and nature of records that can be obtained and stored, and the level of insight that can be gleaned. But it does not invalidate the underlying principle. Subpoenas, even those issued by grand juries, may not be used to engage in fishing expeditions.

Grand jury investigations also are specific. That is, they represent investigations into particular individuals, or particular entities, in relation to which there is reasonable suspicion that some illegal behavior has occurred. The compelled production of records or items is thus limited by reference to the target of the investigation.

If a grand jury were, for instance, focused on the potentially criminal acts of the head of a crime family in Des Moines, absent reasonable suspicion of some sort of connection to the syndicate, it would not issue a subpoena for the telephone records of the Parent-Teacher's Association at Clark Elementary School in Sioux City.

In contrast, the Section 215 orders are broad and non-specific. That is, on the basis of no particular suspicion, all call records, the "vast majority" of which (according to FISC's own language) are of a purely local nature, are swept up by the NSA.[41]

Grand jury investigations are also targeted at current and prior criminal activity. The telephony metadata orders, in contrast, are both past and forward-looking, in that they anticipate the possibility of illegal

---

a multi-year period); Ealy v. Littlejohn, 569 F.2d 219, 227 (5th Cir. 1978) ("When the grand jury goes on a fishing expedition in forbidden waters, the courts are not powerless to act.") Cases cited in Memorandum of Law in Support of Plaintiffs' Motion for a Preliminary Injunction, ACLU v. Clapper, 13 CV0399411-12.

[39] In Re Production of Tangible Things from [REDACTED], No. BR 08-13, Order at 9, 12 (FISA Ct.2009), *available at* http://www.dni.gov/files/documents/section/pub_March%202%202009%20Order%20from%20FISC.pdf.

[40] In re Fontaine, 402 F. Supp. 1219, 1221 (E.D.N.Y. 1975) (quoting In re Surety Ass'n of Am., 388 F.2d 412, 414 (2d Cir. 1967)).

[41] In re Application of the Federal Bureau of Investigation for an Order Requiring the production of Tangible Things, No. BR 06-05.

behavior in the future. Most of the individuals in the database are suspected of no wrongdoing whatsoever. Yet the minimization procedures allow for any information obtained from mining the data to then be used in criminal prosecution. This is an unprecedented use of subpoena information-gathering authority. It amounts to a permanent, ongoing grand jury investigation into all, possible, future criminal acts.

Remarkably, FISC itself, despite the statutory language, has recognized that the information it obtains from the metadata program could not otherwise be collected with any other legal instrument—including a subpoena *duces tecum*. In a secret opinion issued in March 2009 Judge Reggie Walton wrote:

> Because the collection would result in NSA collecting call detail records pertaining to [REDACTED] of telephone communications, including call detail records pertaining to communications of United States (U.S.) persons located within the U.S. who are not the subject of any FBI investigation and whose metadata *could not otherwise be legally captured in bulk*, the government proposed stringent minimization procedures that strictly controlled the acquisition, accessing, dissemination, and retention of these records by the NSA and FBI.[42]

Later in the document, he again noted that the information "otherwise could not be legally captured in bulk by the government".[43] This assertion directly contradicts the statutory requirement that the information could otherwise be obtained via subpoena *duces tecum*. It amounts to an admission, by the Court, that the program violated the statute.

What makes the failure of the Court to prevent the illegal program from continuing even more concerning is Judge Walton's explanation of why, even though the information could not legally be obtained in any other way, FISC allowed the government to proceed. He continues,

> Nevertheless, the FISC has authorized the bulk collection of call detail records in this case based upon: (1) the government's explanation, under oath, of how the collection of and access to such data are necessary to analytical methods that are vital to the national security of the United States; and (2) minimization procedures that carefully restrict access to the BR metadata and includes specific oversight requirements.[44]

In other words, FISC allowed an illegal program to operate because the government (1) promised that it was vital to U.S. national security, and (2) was directed by the court to police its own house by following

[42] In re Production of Tangible Things *From* [REDACTED], Order, No. BR 08-13, at 2-3 (FISA Ct. Mar. 2, 2009), *available at* http://www.dni.gov/files/documents/section/pub_March%202%202009%20Order%20from%20FISC.pdf.
[43] *Id.* at 12.
[44] *Id.*

the minimization procedures. The former is legally insufficient to justify violation of a Congressional statute. The latter highlights the extent to which FISC, precisely because of the size of the collection program in question, has become dependent on the NSA to conduct its own oversight—thus abdicating its responsibilities to the Executive Branch.[45] This further underscores the inapposite nature of the bulk collection program in light of the requirements of grand jury subpoenas, issued in the course of an investigation overseen by the judicial instruments of the state.

[45] *Id. (*"[I]n light of the scale of this bulk collection program, the Court must rely heavily on the government to monitor this program to ensure that it continues to be justified. . . and that it is being implemented in a manner that protects the privacy interests of U.S. persons.")

**"Continued Oversight of the Foreign Intelligence Surveillance Act" Hearing**
**Senator Franken Questions for the Record**

**(1) Professor DONOHUE, in August the Office of the Director of National Intelligence announced that it would start annually disclosing to the public the number of orders issued under key surveillance authorities, as well as the number of quote, "targets" affected by these orders. Are these promised disclosures enough? Or are actual changes to the law necessary to achieve greater transparency?**

*Response:*

While welcome, the voluntary disclosure of the number of orders issued under key surveillance authorities, as well as the number of "targets" affected by these orders, is far from adequate. The release of such numbers, as can be seen from the current statistical updates provided by the Department of Justice, may provide some information, but its value is limited. The specific type of information being volunteered, moreover, is dwarfed by the claim that all telephony metadata is relevant to terrorism investigations. Any one order can result in millions of pages of data being released to the National Security Agency ("NSA"), suggesting that over-reliance on the reporting of the number of orders issued can be misleading. Similarly, reporting the number of targets, while contributing some information, fails to deliver meaningful data on the extent to which surveillance authorities are being used. The voluntary provision of such data, in addition, would not be subject to judicial review and could be altered absent Congressional approval, making the offer insufficiently grounded in the law. Actual statutory changes that address the quantitative and qualitative nature of the surveillance programs underway are essential to achieving greater transparency.

The Department of Justice ("DOJ") currently provides Congress with statistical information on the number of applications to the Foreign Intelligence Surveillance Court ("FISC"). This information has value. The numbers reveal that over the first two and a half decades FISC approved nearly every application without any modification.[1] (Between 1979 and 2003, FISC denied only 3 out of 16,450 applications.)[2] Looking more recently, since 2003, FISC has issued a ruling on 18,473 applications for electronic surveillance and/or physical search (2003-2008), and electronic surveillance (2009-2012). Only 11 applications have been denied in whole or part. (See *Fig. 1*) This means that only 0.06 percent of all applications are denied in whole or part. Looking at this data, scholars have observed that the rate of

[1] *See* DAVID S. KRIS AND J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS ch. 12 (2d ed. 2012), at 469. Letter from Attorney General William French Smith to Director, Administrative Office of the U.S. Courts (Apr. 22, 1981, *available at* http://www.fas.org/irp/agency/daj/fisa/1980-powell.pdf (No orders were entered which modified or denied the

[2] Letter from Attorney General William French Smith to Director, Administrative Office of the U.S. Courts (Apr. 22, 1981, *available at* http://www.fas.org/irp/agency/doj/fisa/1980-powell.pdf (No orders were entered which modified or denied the

success enjoyed by the government in its applications to FISC is "unparalleled in any other American court."[3]

FISC RULINGS ON ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCH (2003-2008) AND ELECTRONIC SURVEILLANCE (2009 – 2012)[4]

| Year | # of Applications on which FISC ruled | # Approved | # Modified | # Denied in Part | # Denied in Whole | # w/drawn by Gov't prior to FISC ruling |
|---|---|---|---|---|---|---|
| 2003[5] | 1,727 | 1,724 | 79 | 0 | 3 [6] | 0 |
| 2004[7] | 1,756[8] | 1,756 | 94 | 0 | 0 | 3 |
| 2005[9] | 2,072[10] | 2,072 | 61 | 0 | 0 | 2 |
| 2006[11] | 2,176[12] | 2,176 | 73 | 1 | 0 | 5 |
| 2007[13] | 2,371 | 2,370 | 86 | 1 | 3[14] | 0 |
| 2008[15] | 2,082 | 2,083[16] | 2 | 0 | 1 | 0 |
| 2009[17] | 1,321[18] | 1,320 | 14 | 1 | 1 | 8 |
| 2010[19] | 1,506[20] | 1,506 | 14 | 0 | 0 | 5 |
| 2011[21] | 1,674[22] | 1,674 | 30 | 0 | 0 | 2 |

[3] Theodore W. Ruger, *Chief Justice Rehnquist's Appointments to the FISA Court: An Empirical Perspective*, 101 NW. U. L. REV. 239, 245 (2007).

[4] Starting in 2009, the Department of Justice began providing the breakdown of the number approved, modified, denied in part, denied in whole, or withdrawn by the government prior to the FISC ruling only for those applications involving electronic communications. Prior to that time, these numbers were combined.

[5] Letter from William E. Moschella, Assistant Attorney Gen., to Mr. L. Ralph Mecham, Dir., Admin. Office of the U. S. Courts (Apr. 30, 2004), *available at* https://www.fas.org/irp/agency/doj/fisa/2003rept.pdf.

[6] An addition application was initially denied but later approved. *Id.*

[7] Letter from Office of Legislative Affairs, U.S. Department of Justice, to The Honorable J. Dennis Hastert, Speaker, U.S. House of Representatives, (Apr. 1, 2005), *available at* https://www.fas.org/irp/agency/doj/fisa/2004rept.pdf.

[8] 1758 submitted, 3 of which were withdrawn prior to FISC ruling and 1 of which was resubmitted. *Id.*

[9] Letter from William E. Moschella, Assistant Attorney Gen., Office of Legislative Affairs, U.S. Department of Justice, to The Honorable J. Dennis Hastert, Speaker, U.S. House of Representatives (Apr. 28, 2006), *available at* https://www.fas.org/irp/agency/doj/fisa/2005rept.html.

[10] 2,074 submitted, 2 of which were withdrawn prior to FISC ruling, and 1 of which was resubmitted. *Id.*

[11] Letter from Richard A. Hertling, Acting Assistant Attorney Gen., to the Honorable Nancy Pelosi, Speaker, U.S. House of Representatives (Apr. 27, 2007), *available at* https://www.fas.org/irp/agency/doj/fisa/2006rept.pdf.

[12] 2,181 submitted, 5 of which were withdrawn prior to FISC ruling. *Id.*

[13] Letter from Brian A. Benczkowski, Principal Deputy Assistant Attorney Gen., Office of Legislative Affairs, U.S. Department of Justice, to the Honorable Nancy Pelosi, Speaker, U.S. House of Representatives (Apr. 30, 2008), *available at* https://www.fas.org/irp/agency/doj/fisa/2007rept.pdf.

[14] Discrepancy in the numbers stems in part from holdover applications and denials. Two applications, for instance, filed in CY 2006 were not approved until 2007. *Id.*

[15] Letter from Ronald Weich, Assistant Attorney Gen., Office of Legislative Affairs, U.S. Department of Justice, to the Honorable Harry Reid, Majority Leader, U.S. Senate (May 14, 2009) *available at* https://www.fas.org/irp/agency/doj/fisa/2008rept.pdf.

[16] Discrepancy in the numbers stems in part from holdover applications and denials. Two applications filed in CY 2007 were not approved until CY 2008).

[17] Letter from Ronald Weich, Assistant Attorney Gen., Office of Legislative Affairs, U.S. Department of Justice, to The Honorable Joseph R. Biden, Jr., President, U.S. Senate (Apr. 30, 2010), *available at* https://www.fas.org/irp/agency/doj/fisa/2009rept.pdf.

[18] For the first time since 2003, no numbers are available for modifications/denials for the full number of applications submitted (physical search, electronic surveillance, and combined applications). Instead, the report notes that of the 1,376 in total submitted in the former three categories, 1,329 were related to electronic surveillance. It was eight of these applications that were withdrawn, 1 denied in whole, 1 denied in part, and 14 modifications, with 1,320 approved. The number of applications is thus missing the numbers for physical search and physical search combined applications. *Id.*

[19] Letter from Ronald Weich, Assistant Attorney Gen., Office of Legislative Affairs, U.S. Department of Justice, to the Honorable Harry Reid, Majority Leader, U.S. Senate, (Apr. 29, 2011), *available at* https://www.fas.org/irp/agency/doj/fisa/2010rept.pdf.

[20] Total number of electronic surveillance, physical search, and combined applications was 1,579. The report, however, isolates the electronic applications (1,511), and provides breakdowns for modifications, denials, etc., for just that category. Of the total of 1,511, five were withdrawn by the Government prior to FISC ruling. *Id.*

| | | | | | | |
|---|---|---|---|---|---|---|
| 2012[23] | 1,788[24] | 1,788 | 40 | 0 | 0 | 1 |
| ***Totals*** | ***18,473*** | ***18,469*** | ***493*** | ***3*** | ***8*** | ***26*** |

*Figure 1*

Statistics provided by DOJ similarly demonstrate significant deference extended by FISC to the government with regard to applications under Section 215. From the numbers provided publicly to Congress, it appears that FISC has *never* denied an application for an order under this section. That is, of 751 applications since 2005, all 751 have been granted. (See *Fig. 2*)

ORDERS FOR THE PRODUCTION OF TANGIBLE GOODS

| **Year** | **Number of Applications to FISC under 50 U.S.C. §1862(c)(2)** | **Number of Applications Granted by FISC** |
|---|---|---|
| 2005[25] | 155 | 155 |
| 2006[26] | 43 | 43 |
| 2007[27] | 6 | 6 |
| 2008[28] | 13 | 13 |
| 2009[29] | 21 | 21 |
| 2010[30] | 96 | 96 |
| 2011[31] | 205 | 205 |
| 2012[32] | 212 | 212 |
| ***Totals*** | ***751*** | ***751*** |

*Figure 2*

These numbers illustrate both the advantage of reporting requirements and the limited value of such information. Critics of the FISC process, for instance, point to the numbers as evidence of the risk of capture presented by in camera, ex parte proceedings. Court supporters, in turn, note that a number of the

[21] Letter from Ronald Weich, Assistant Attorney Gen., to The Honorable Joseph R. Biden, Jr., President, U.S. Senate (Apr. 30, 2012), , *available at* https://www.fas.org/irp/agency/doj/fisa/2011rept.pdf.

[22] Note that there were 1,745 total applications that included electronic surveillance and/or physical searches for foreign intelligence purpose. It appears that approximately 70 of the orders related solely to physical search, since the breakdown for electronic surveillance is only done for the 1,674. Two of the initial orders were withdrawn prior to FISC ruling. *Id.*

[23] Letter from Peter J. Kadzik, Principal Deputy Assistant Attorney Gen., to the Honorable Harry Reid, Majority Leader, U.S. Senate (Apr. 30, 2013), *available at* https://www.fas.org/irp/agency/doj/fisa/2012rept.pdf.

[24] The government made a total of 1,856 applications for electronic surveillance and/or physical searches; of those, 1,789 included requests for electronic surveillance. Of those, one was withdrawn by the Government prior to FISC ruling. *Id.*

[25] Letter from William E. Moschella, Assistant Attorney Gen., to the Honorable Richard B. Cheney, President, United States Senate (Apr. 28, 2006), *available at* http://www.justice.gov/nsd/foia/foia_library/2005fisa-ltr.pdf.

[26] Letter from Richard A. Hertling, Acting Assistant Attorney Gen., to the Honorable Richard B. Cheney, President, United States Senate (Apr. 27, 2007), *available at* http://www.justice.gov/nsd/foia/foia_library/2006fisa-ltr.pdf.

[27] Letter from Brian A. Benczkowski, Principal Deputy Assistant Attorney Gen., to the Honorable Richard B. Cheney (Apr. 30, 2008), *available at* http://www.justice.gov/nsd/foia/foia_library/2007fisa-ltr.pdf.

[28] Letter from Ronald Weich, Assistant Attorney Gen.l, to the Honorable Joseph R. Biden, Jr., President, United States Senate (May 14, 2009), *available at* http://www.justice.gov/nsd/foia/foia_library/2008fisa-ltr.pdf.

[29] Letter from Ronald Weich, Assistant Attorney Gen., to the Honorable Joseph R. Biden, Jr., President, United States Senate (Apr. 30, 2010), *available at* http://www.justice.gov/nsd/foia/foia_library/2009fisa-ltr.pdf.

[30] Letter from Ronald Weich, Assistant Attorney Gen., Department of Justice, to the Honorable Joseph R. Biden, Jr., President, U.S. Senate( Apr. 29, 2011), *available at* http://www.justice.gov/nsd/foia/foia_library/2010fisa-ltr.pdf.

[31] Letter from Ronald Weich, Assistant Attorney Gen., Department of Justice, to the Honorable Joseph R. Biden, Jr., President, U.S. Senate (Apr. 30, 2012), *available at* http://www.justice.gov/nsd/foia/foia_library/2011fisa-ltr.pdf.

[32] Letter from Peter J. Kadzik, Principal Deputy Assistant Attorney Gen., Department of Justice, , to the Honorable Joseph R. Biden, Jr., President, U.S. Senate(Apr. 30, 2013), *available at* http://www.justice.gov/nsd/foia/foia_library/2012fisa-ltr.pdf.

applications for electronic surveillance or physical search are either modified or withdrawn by the government prior to FISC ruling, suggesting the presence of an informal process whereby FISC provides a check on the Executive. Critics counter by, again, appealing to the numbers. Looking at electronic surveillance and physical search applications, 493 modifications over the past decade still only comes to 2.6% of the total number of applications. (See *Fig. 1*). The numbers further show that only 26 applications have been withdrawn by the government prior to FISC ruling—approximately one tenth of one percent of all applications to the Court. (See *Fig. 1*).

In other words, the numbers raise concern about the role performed by FISC and indicate the presence of some informal process whereby FISC appears to be influencing the contours of applications. They also raise question about the extent of this informal process itself. But without further qualitative information and contextual data, it is extremely difficult to evaluate the information.

The release of statistical information regarding the number of orders approved by FISC would suffer from a similar lack of contextual information and raise concern about the extent to which such information might be misleading. The government argues that all telephony metadata is relevant to terrorism investigations. It also argues that Section 215 orders can be used to obtain massive amounts of data. This means that any *one* order can require telephone service providers to turn over millions of pages of data. Thus, while it would provide more information than is currently conveyed with regard to the number of applications to FISC under 50 U.S.C. §1862(c)(2), provision of this information would still fail to deliver meaningful data on the extent of surveillance programs underway.

Similarly, the provision of the number of individuals targeted by the government would generate more, but still insufficient information. In the process of targeting specific groups or individuals, the government claims the concurrent authority to draw in wide swathes of U.S. persons' information. So what may appear to be a limited number of targets may, in fact, be masking significant surveillance programs.

As a final note of caution, the voluntary provision of such data would be merely a policy adopted by the Executive Branch. Resultantly, it would not be subject to judicial review and it could be altered without any action from—or even notice to—Congress. It is thus an extremely weak way to ensure greater transparency within the Executive Branch. Actual statutory changes that require DOJ to convey both the quantitative and the qualitative nature of the surveillance programs underway are essential for achieving greater transparency.