

UNCLASSIFIED

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY)
INFORMATION CENTER,)
)
Plaintiff,)
)
v.)
)
DEPARTMENT OF JUSTICE,)
)
Defendant.)
_____)

Case No. 1:13-cv-01961-KBJ

DECLARATION OF DAVID J. SHERMAN

I, DAVID J. SHERMAN, hereby declare and state:

1. I am the Associate Director for Policy and Records at the National Security Agency ("NSA" or "Agency"), an intelligence agency within the Department of Defense. I have been employed with NSA since 1985. Prior to my current assignment, I held various senior and supervisory positions at NSA and elsewhere in the Executive Branch, to include serving as the Deputy Chief of Staff in the Agency's Signals Intelligence Directorate, its representative to the Department of Defense, Deputy Associate Director for Foreign Affairs, and Director for Intelligence Programs at the National Security Council. As the Associate Director for Policy and Records, I am responsible for, among other things, the processing of all requests made pursuant to the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, for NSA records.

2. In addition, I am a TOP SECRET original classification authority pursuant to Section 1.3 of Executive Order ("E.O.") 13526, dated 29 December 2009 (75 Fed. Reg. 707). It is my responsibility to assert the FOIA exemptions over NSA

UNCLASSIFIED

UNCLASSIFIED

information in the course of litigation. Through the exercise of my official duties, I have become familiar with the current litigation arising out a Freedom of Information Act ("FOIA") request for information filed by the Plaintiff, Electronic Privacy Information Center.

3. Through the exercise of my official duties, I have become familiar with this civil action and the underlying FOIA request. I make the following statements based upon my personal knowledge and information made available to me in my official capacity.

4. I submit this declaration in support of the U.S. Department of Justice's ("DoJ") Motion for Summary Judgment in this proceeding. The purpose of this declaration is to explain and justify, to the extent possible on the public record, the withholdings taken by the NSA in responding to plaintiff's request for information under the FOIA, 5 U.S.C. § 552. To the extent that the Court requires additional information regarding particular withholdings, the Agency will submit an *in camera, ex parte* classified declaration upon request to provide further explanation of the harm to the national security that could reasonably be expected to occur if certain information were to be released.

I. ORIGIN AND MISSION OF NSA

5. The NSA was established by Presidential Directive in October 1952 as a separately-organized agency within the Department of Defense under the direction, authority, and control of the Secretary of Defense. NSA's foreign intelligence mission includes the responsibility to collect, process, analyze, produce, and disseminate signals intelligence ("SIGINT") information for foreign intelligence and counterintelligence

UNCLASSIFIED

purposes to support national and departmental missions and for the conduct of military operations. *See* E.O. 12333, section 1.7(c), as amended.

6. In performing its SIGINT mission, NSA exploits foreign electromagnetic signals to obtain intelligence information necessary to the national defense, national security, or the conduct of foreign affairs. NSA has developed a sophisticated worldwide SIGINT collection network that acquires foreign and international electronic communications. The technological infrastructure that supports NSA's foreign intelligence information collection network has taken years to develop at a cost of billions of dollars and untold human effort. It relies on sophisticated collection and processing technology.

II. IMPORTANCE OF SIGINT TO THE NATIONAL SECURITY

7. There are two primary reasons for gathering and analyzing intelligence information. The first, and most important, is to gain the information required to direct U.S. resources as necessary to counter threats to the nation and its allies. The second reason is to obtain the information necessary to direct the foreign policy of the United States. Foreign intelligence information provided by the NSA is routinely distributed to a wide variety of senior Government officials, including the President; the President's National Security Advisor; the Director of National Intelligence; the Secretaries of Defense, State, Treasury, and Commerce; U.S. ambassadors serving in posts abroad; the Joint Chiefs of Staff; and the Unified and Specified Commanders. In addition, SIGINT information is disseminated to numerous agencies and departments, including, among others, the Central Intelligence Agency; the Federal Bureau of Investigation; the Drug Enforcement Administration; the Departments of the Army, Navy, and Air Force; and

UNCLASSIFIED

UNCLASSIFIED

various intelligence components of the Department of Defense. Information provided by NSA is relevant to a wide range of important issues, including, but not limited to, military order of battle, threat warnings and readiness, arms proliferation, terrorism, and foreign aspects of international narcotics trafficking. This information is often critical to the formulation of U.S. foreign policy and the support of U.S. military operations around the world. Moreover, intelligence produced by NSA is often unobtainable by other means.

III. CATEGORIES OF INFORMATION WITHHELD

8. The purpose of this declaration is to advise the Court that the NSA withheld certain information, as set forth below, because it is properly exempt from disclosure under the FOIA based on Exemptions 1 and 3, 5 U.S.C. §§ 552(b)(1), (3), respectively. This is so because the information remains currently and properly classified in accordance with E.O. 13526 and protected from release by statutes, specifically Section 6 of the National Security Agency Act of 1959 (Pub. L. No. 86-36) (codified at 50 U.S.C. § 3605) ("NSA Act"); 18 U.S.C. § 798, and Section 102A(i)(1) of the National Security Act of 1947, as amended (codified at 50 U.S.C. § 3024).

9. The records at issue for the cross-motions for summary judgment that contain NSA information withheld from release under FOIA are:¹ Documents 002, 003, 004, 005, 006, 007, 008, 009, 010, 011, 030, 031, 032, 033, 034, 035, 036, 037, 038, 039, 040, 041, 042, 044, 045, 046, 047, 048, 049, 051, 054, 056, 059, 060, 061, 062, 063, 064, 065, and 066.

¹ Document numbers listed in this Declaration correspond to those listed on the Vaughn index submitted by Defendants in this case. Plaintiff has previously indicated that it is not challenging DOJ's withholding in full of Document 043.

UNCLASSIFIED

FOIA EXEMPTION ONE

10. Section 552(b)(1) of the FOIA provides that the FOIA does not require the release of matters that are specifically authorized under criteria established by an Executive Order to be kept secret in the interest of the national defense or foreign policy, and are in fact properly classified pursuant to such Executive Order. The current Executive Order that establishes such criteria is E.O. 13526.

11. Section 1.1 of E.O. 13526 provides that information may be originally classified if: 1) an original classification authority is classifying the information; 2) the information is owned by, produced by or for, or is under the control of the Government; 3) the information falls within one or more of the categories of information listed in section 1.4 of the Executive Order; and 4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, and the original classification authority is able to identify or describe the damage.

12. Section 1.2(a) of E.O. 13526 provides that information shall be classified at one of three levels. Information shall be classified at the TOP SECRET level if its unauthorized disclosure reasonably could be expected to cause exceptionally grave damage to the national security. Information shall be classified at the SECRET level if its unauthorized disclosure reasonably could be expected to cause serious damage to the national security. Information shall be classified at the CONFIDENTIAL level if its unauthorized disclosure reasonably could be expected to cause damage to the national security.

UNCLASSIFIED

13. Section 1.4 of E.O. 13526 provides that information shall not be considered for classification unless it falls within one (or more) of eight specifically enumerated categories of information. The categories of classified information in the NSA documents at issue here are those found in Section 1.4(c), which includes intelligence activities (including covert action), intelligence sources and methods, or cryptology; Section 1.4(d), which includes foreign relations or foreign activities of the United States, including confidential sources; and Section 1.4(g), which includes vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security.

14. In my role as a TOP SECRET original classification authority ("OCA"), I reviewed the categories of information withheld pursuant to this FOIA request and determined that those categories are currently and properly classified in accordance with E.O. 13526. Based on that determination, I have determined that the responsive material at issue was properly withheld, as all of this information is currently and properly classified in accordance with E.O. 13526. Accordingly, the release of this intelligence information could reasonably be expected to cause damage to the national security. The damage to national security that reasonably could be expected to result from the unauthorized disclosure of this classified information is described below.

FOIA EXEMPTION 3

15. Exemption 3 provides that FOIA does not require the production of records that are:

“specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A)(i) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (ii) establishes particular

UNCLASSIFIED

criteria for withholding or refers to particular types of matters to be withheld; and (B) if enacted after the date of enactment of the OPEN FOIA Act of 2009, specifically cites to this paragraph.” 5 U.S.C. § 552(b)(3).²

16. The challenged information at issue here in this litigation falls squarely within the scope of three statutes. The first applicable statute is a statutory privilege unique to NSA. As set forth in section 6 of the NSA Act, Public Law 86-36 (50 U.S.C. § 3605), “[n]othing in this Act or any other law . . . shall be construed to require the disclosure of the organization or any function of the National Security Agency, [or] of any information with respect to the activities thereof. . . .” (emphasis added). Congress, in enacting the language in this statute, decided that disclosure of any information relating to NSA activities is potentially harmful. Federal courts have held that the protection provided by this statute is, by its very terms, absolute. Section 6 states unequivocally that, notwithstanding any other law, including the FOIA, NSA cannot be compelled to disclose any information with respect to its activities. To invoke this privilege, the U.S. Government must demonstrate only that the information it seeks to protect falls within the scope of Section 6. Further, while in this case the harm would be exceptionally grave or serious, the U.S. Government is not required to demonstrate specific harm to national security when invoking this statutory privilege, but only to show that the information relates to its activities. NSA’s functions and activities are therefore protected from disclosure regardless of whether or not the information is classified.

17. The second statute is Section 102A(i)(1) of the National Security Act of 1947, as amended, 50 U.S.C. § 3024(i)(1), which provides that “the Director of National

² The OPEN FOIA Act of 2009 was enacted on October 28, 2009, Pub. L. 111-83, 123 Stat. 2142, 2184; 5 U.S.C. § 552(b)(3)(B), after the applicable National Security Act provision was enacted, and therefore is not applicable to the analysis in this case.

UNCLASSIFIED

Intelligence shall protect intelligence sources and methods from unauthorized disclosure.” Like the protection afforded to core NSA activities by section 6 of the National Security Agency Act of 1959 (“NSA Act”), the protection afforded to intelligence sources and methods is absolute. Whether the sources and methods at issue are classified is irrelevant for purposes of the protection afforded by 50 U.S.C. § 3024(i)(1).

18. Finally, the third statute is 18 U.S.C. § 798. This statute prohibits the unauthorized disclosure of classified information: (i) concerning the communications intelligence activities of the United States, or (ii) obtained by the process of communications intelligence derived from the communications of any foreign government. The term “communications intelligence,” as defined by Section 798, means the “procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients.”

19. As described above, these statutes protect the fragile nature of the United States’ intelligence sources, methods, and activities, to include but not limited to, the existence and depth of signals intelligence-related successes, weaknesses, and exploitation techniques. These statutes recognize the vulnerability of intelligence sources and methods, including to countermeasures, and the significance of the loss of valuable intelligence information to national policymakers and the IC. Given that Congress specifically prohibited the disclosure of the sources and methods used by the IC, as well as any information related to NSA’s functions and activities, I have determined that the information was properly withheld under FOIA Exemption 3.

UNCLASSIFIED

CATEGORIES OF INFORMATION WITHHELD³

Categories of Internet Metadata Collected

20. The NSA withheld from disclosure information relating to the categories of electronic communications metadata collected under the PR/TT program. This information was redacted and withheld in the following documents: Documents 002, 003, 006, 011, 037, 041, 042, 046, 047, 048, 051, 054, 056, 059, 060, 061, 062, 063, 064, 065, and 066.

21. I have reviewed this information and determined that the categories of metadata collected under the PR/TT program are currently and properly classified at the TOP SECRET level in accordance with E.O. 13526, because the release of this information could reasonably be expected to cause exceptionally grave damage to the national security. Information regarding categories of internet metadata collected meets the criteria for classification set forth in Sections 1.4(c), 1.4(d), and 1.4(g) of E.O. 13526.

22. Disclosure of the details regarding the categories of electronic communications metadata that were collected pursuant to the PR/TT program would publicly reveal the still currently and properly classified scope of this program. The release of such information would reveal information concerning technological collection capabilities along with success (or lack of success) regarding the specific categories of electronic communications metadata that were collected pursuant to the PR/TT program. While the bulk PR/TT electronic communications metadata program is no longer

³ Throughout the documents containing NSA information, redactions were made pursuant to FOIA Exemption 6 to protect the names of U.S. Government employees, including employees of the FISC. FOIA Exemption 6 provides that FOIA does not require the production of records that are "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. 5 U.S.C. § 552(b)(6). In addition, NSA redacted information about its organization and structure from throughout the documents, pursuant to section 6 of the NSA Act, 50 U.S.C. § 3605, which protects the functions and activities of the NSA. As discussed above, 50 U.S.C. § 3605 has been recognized as an Exemption 3 statute under the FOIA.

UNCLASSIFIED

UNCLASSIFIED

operational, NSA is authorized to acquire and collect certain categories of electronic communications metadata under other authorities (such as Executive Order 12333, as amended, and Section 702 of the FISA Amendments Act of 2008). The continuing importance of the specific categories of Internet metadata that were collected under the bulk PR/TT program underscores the need to protect the still-classified operational details of this activity.

23. Additionally, disclosure of the categories of electronic communications metadata collected under the bulk PR/TT program could also be used by this Nation's foreign adversaries. Adversaries would be provided with a detailed roadmap into NSA's technological capabilities, which they could use to develop countermeasures to thwart NSA's current or future collection operations directed at specific targets. Public disclosure of NSA's capabilities to acquire specific categories of electronic communications metadata would alert targets to the vulnerabilities of their communications (and also, which of their communications are not vulnerable). Once alerted, targets can frustrate SIGINT collection by using different communication techniques. Adversaries could develop countermeasures that could be used to thwart not just email metadata collection, but also other types of communications collection. This may result in denial of access to targets' communications and therefore result in a loss of information crucial to the national security and defense of the United States. Furthermore, information that reveals NSA's technological capabilities could provide adversaries with unique insights that could assist such adversaries in developing their own bulk electronic communications metadata collection programs to target the United States and its interests both domestically and abroad.

UNCLASSIFIED

24. The categories of electronic communications metadata collected under the PR/TT program are also protected from release by statute and are likewise exempt from release based on FOIA Exemption 3, 5 U.S.C. § 552(b)(3). Specifically, there are three Exemption 3 statutes that protect this information from public release: section 6 of the NSA Act, 50 U.S.C. § 3605, 18 U.S.C. § 798, and Section 102A(i)(1) of the National Security Act, as amended, 50 U.S.C. § 3024(i)(1).

25. The categories of electronic communications metadata collected under this program relate to a "function of the National Security Agency," 50 U.S.C. § 3605. Indeed, this information relates to one of NSA's primary functions, its SIGINT mission. Further, any disclosure of the scope of this collection of electronic communications metadata, as stated above, would reveal NSA's capabilities. Thus, the categories and types of metadata collected, if revealed, would disclose "information with respect to [NSA's] activities" in furtherance of its SIGINT mission. 50 U.S.C. § 3605.

26. Likewise, the categories of electronic communications metadata collected under this program is protected from public release pursuant to Section 102A(i)(1) of the National Security Act, as amended, 50 U.S.C. § 3024(i)(1), which states that "[t]he Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure." Revealing the categories and types of metadata collected would provide our adversaries with information from which they could deduce the intelligence methods by which the electronic communications records were collected and the intelligence sources (the facilities) from which the records were collected, and thus, this information falls squarely within the protection of this statute and should be afforded absolute protection from release.

UNCLASSIFIED

27. Finally, the information is protected from release under 18 U.S.C. § 798, which protects from disclosure information concerning the communications intelligence activities of the United States, or obtained by communications intelligence processes. The categories and methods of metadata collected would reveal precisely the procedures and methods that the NSA uses to intercept communications of its targets, thereby falling within the scope of protection offered by this statute.

Types of Electronic Communications Acquired

28. The NSA withheld from disclosure information under the PR/TT program relating to the types of electronic communications from which metadata was acquired (e.g., electronic mail, etc.). This information was redacted and withheld in the following documents: Documents 002, 006, 009, 011, 037, 039, 040, 041, 042, 046, 047, 048, 051, 054, 056, 059, 060, 061, 062, 063, 064, 065, and 066.

29. I have reviewed this information and determined that information regarding the types of electronic communications under the PR/TT program from which metadata was acquired is currently and properly classified at the TOP SECRET level in accordance with E.O. 13526, because the release of this information could reasonably be expected to cause exceptionally grave damage to the national security. Information regarding the types of electronic communications acquired meets the criteria for classification set forth in Sections 1.4(c), 1.4(d), and 1.4(g) of E.O. 13526.

30. Disclosure of the type of electronic communications under the PR/TT program from which electronic communications metadata was acquired would again demonstrate the still-classified scope of the PR/TT program. The release of this information would reveal information concerning NSA's success (or lack of success) in

UNCLASSIFIED

UNCLASSIFIED

its acquisition efforts under the PR/TT program. As noted above, while the bulk PR/TT program is no longer operational, NSA's core mission continues to include the acquisition and collection of electronic communications under other authorities. Foreign targets have been known to analyze public disclosures of NSA's capabilities. Public disclosure of NSA's capabilities to acquire specific types of electronic communications would alert targets to the vulnerabilities of their communications (and also, which of their communications are not vulnerable). Once alerted, targets can frustrate SIGINT collection by using different communication techniques. Adversaries could develop countermeasures that could be used to thwart not just email metadata collection, but also other types of communications collection. This may result in denial of access to targets' communications and therefore result in a loss of information crucial to the national security and defense of the United States.

31. This same information is also protected from release by statute and is likewise exempt from release based on FOIA Exemption 3, 5 U.S.C. § 552(b)(3). Specifically, there are three Exemption 3 statutes that protect from public release the types of electronic communications acquired under the PR/TT program: section 6 of the NSA Act, 50 U.S.C. § 3605, 18 U.S.C. § 798, and Section 102A(i)(1) of the National Security Act, as amended, 50 U.S.C. § 3024(i)(1).

32. The types of communications acquired under this program relate to a "function of the National Security Agency," 50 U.S.C. § 3605. Indeed, it relates to one of NSA's primary functions, its SIGINT mission. Further, any disclosure of the scope of this collection of electronic communications metadata, as stated above, would reveal NSA's capabilities. Thus, the types of communications acquired, if revealed, would

UNCLASSIFIED

disclose "information with respect to [NSA's] activities" in furtherance of its SIGINT mission. 50 U.S.C. § 3605.

33. Likewise, the types of electronic communications acquired under this program are protected from public release pursuant to Section 102A(i)(1) of the National Security Act, as amended, 50 U.S.C. § 3024(i)(1), which states that "[t]he Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure." Revealing the types of communications acquired would provide our adversaries with information from which they could deduce the intelligence methods by which the electronic communications records were collected and the intelligence sources (the facilities) from which the records were collected, and thus, this information falls squarely within the protection of this statute and should be afforded absolute protection from release.

34. Finally, the information is protected from release under 18 U.S.C. § 798, which protects from disclosure information concerning the communications intelligence activities of the United States, or obtained by communications intelligence processes. The categories and methods of metadata collected would reveal precisely the procedures and methods that the NSA uses to intercept communications of its targets, thereby falling within the scope of protection offered by this statute.

Identities of the Providers

35. The NSA withheld from disclosure information relating to the identities of the providers that were compelled to participate in the PR/TT program. This information was redacted and withheld in the following documents: Documents 002, 009, 040, 041, 042, 046, 047, 048, 051, 054, 056, 059, and 060.

UNCLASSIFIED

36. I have reviewed this information and determined that the identities of the providers are currently and properly classified at the TOP SECRET level in accordance with E.O. 13526, because the release of this information could reasonably be expected to cause exceptionally grave damage to the national security. This information falls within Sections 1.4(c), 1.4(d), and 1.4(g) of E.O. 13526.

37. Releasing the identities of any telecommunication service provider subject to any PR/TT Primary Order would disclose currently and properly classified intelligence information. Confirmation or denial of a relationship between NSA and any other telecommunication service provider on a specific intelligence activity would cause exceptionally grave damage to the national security. Confirming or denying a relationship would reveal to foreign adversaries whether or not NSA utilizes particular intelligence sources and methods and, thus, would either compromise actual sources and methods or reveal that NSA does not utilize a particular source or method. Such facts would allow individuals, to include America's adversaries, to accumulate information and draw conclusions about how the U.S. Government collects communications, its technical capabilities, and its sources and methods. Any U.S. Government confirmation would replace speculation with certainty for hostile foreign adversaries who are balancing the risk that a particular channel of communication may not be secure against the need to communicate efficiently. Adversaries would then focus with a certainty on those particular channels they now believe are secure.

38. Moreover, the harm to national security is not reduced by the fact that the PR/TT program is no longer operational. If NSA were to disclose that a specific telecommunications service provider was compelled to participate in a recently-

UNCLASSIFIED

concluded intelligence collection program, such as the PR/TT program, then it logically follows that the same provider has been compelled to participate in other, ongoing intelligence collection programs. This is likely to cause NSA's foreign intelligence targets to switch to telecommunication services providers that have not been specifically identified as lawfully compelled to participate in a U.S. intelligence communication collection program. As a result, NSA may be denied access to valuable foreign intelligence information.

39. Finally, as described above, foreign intelligence targets are known to analyze public disclosures of the NSA's capabilities. Confirmation that specific providers participated in the PR/TT program would alert the targets to which email metadata records NSA did and did not collect, as well as the nature and scope of the PR/TT program. As such, the public disclosure that NSA possessed a specific capability over a specific period of time to acquire email metadata records from certain providers would easily alert targets to the vulnerability of their communications during the time period in which the PR/TT program was operational. Foreign intelligence targets know how they communicate, and therefore, would know, upon a disclosure of NSA's capabilities via the release of the identity of any particular telecommunications service provider, which of their electronic communications metadata records were potentially vulnerable to collection, querying, and analysis (and also, which of their communications may not have been vulnerable). Disclosure of this information would allow targets to know what information was collected at particular times, as well as gaps in coverage that would reveal that information from a particular period was "safe." In addition, once alerted, targets could potentially frustrate NSA collection under other programs by

UNCLASSIFIED

UNCLASSIFIED

switching to a provider that is not identified as having been subject to the FISC's Orders under this program. This may result in denial of access to targets' communications and therefore result in a loss of access to information crucial to the national security and defense of the United States.⁴

40. This same information is also protected from release by statute and is likewise exempt from release based on FOIA Exemption 3, 5 U.S.C. § 552(b)(3). Specifically, there are three Exemption 3 statutes that protect from public release the identities of the providers participating in the PR/TT program: section 6 of the NSA Act, 50 U.S.C. § 3605, 18 U.S.C. § 798, and Section 102A(i)(1) of the National Security Act, as amended, 50 U.S.C. § 3024(i)(1).

41. The identities of the providers participating in this program relate to a "function of the National Security Agency," 50 U.S.C. § 3605. Indeed, it relates to one of NSA's primary functions, its SIGINT mission. Further, any disclosure of the scope of this collection of electronic communications metadata, as stated above, would reveal NSA's capabilities, as well as the sources and methods used by the NSA in conducting its foreign intelligence mission. Thus, the identities of the providers, if revealed, would disclose "information with respect to [NSA's] activities" in furtherance of its SIGINT mission. 50 U.S.C. § 3605.

⁴ Congress recognized the need to protect the identities of telecommunication service providers alleged to provide certain assistance to the U.S. Government when it enacted provisions of the FISA Amendments Act of 2008. Those provisions barred lawsuits against telecommunication service providers providing assistance pursuant to an order of the FISC. In enacting this legislation, the Senate Select Committee on Intelligence (SSCI) found that "electronic surveillance for law enforcement and intelligence purposes depends in great part on the cooperation of private companies that operate the nation's telecommunications system. S. Rep. 110-209 (2007) at 9 (accompanying S. 2248, Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008). Notably, the SSCI expressly stated that, in connection with alleged post-9/11 assistance, "it would be inappropriate to disclose the names of the electronic communication service providers from which assistance was sought, the activities in which the Government engaged or in which the providers assisted, or the details regarding any such assistance." *Id.* The Committee added that the "identities of persons or entities who provide assistance to the intelligence community are properly protected as sources and methods of intelligence." *Id.*

UNCLASSIFIED

42. Likewise, the identities of the providers participating in this program are protected from public release pursuant to Section 102A(i)(1) of the National Security Act, as amended, 50 U.S.C. § 3024(i)(1), which states that “[t]he Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure.” It is without question that the identities of specified service providers in the PR/TT program are the intelligence sources for the electronic communications metadata records, and thus, they fall squarely within the protection of this statute and are afforded absolute protection from release.

43. Finally, the information is protected from release under 18 U.S.C. § 798, which protects from disclosure information concerning the communications intelligence activities of the United States, or obtained by communications intelligence processes. Disclosing the identities of the providers would reveal the scope of the PR/TT program and the methods by which the NSA intercepts communications of its targets, thereby falling within the scope of protection offered by this statute.

Docket Numbers and Dates

44. NSA has withheld certain operational details about the PR/TT program based on FOIA Exemptions 1 and 3. These details include the docket numbers and dates, which are found throughout all documents containing NSA information, with the exception of the date of the July 14, 2004 Opinion issued by Judge Kollar-Kottelly that initiated the PR/TT program.⁵

45. These operational details were protected so that our Nation’s adversaries could not deduce the specific gaps in coverage that occurred when the PR/TT program

⁵ In other litigation, NSA has publicly disclosed that, in December 2011, the Government decided not to seek reauthorization of the bulk collection of electronic communications metadata.

UNCLASSIFIED

was non-operational. The Director of National Intelligence has publicly acknowledged that the PR/TT program was reauthorized by the FISC approximately every 90 days from its inception until its termination in December 2011, except for a brief period. By revealing the docket numbers for this PR/TT program and dates, which comprise many of the withholdings in the documents, our adversaries could deduce or infer the time period for which the program was not operational, thereby determining which of their communications (email metadata) may have escaped NSA collection and querying.

46. Adversary knowledge that their communications escaped collection, querying, and analysis for an identified time provides them with certainty that any communications during that time period were safe. Foreign intelligence targets know how they communicate, and therefore, would know, upon a disclosure of a gap in NSA's capabilities, which of their electronic communications metadata records were potentially vulnerable to collection, querying, and analysis (and also, which of their communications may not have been vulnerable). For an adversary (particularly sophisticated adversaries who engage in advanced operational security techniques), such knowledge would be invaluable to determining communication security vulnerabilities (such as which email accounts may have been vulnerable to collection and which are safe). In a program such as the PR/TT program, which utilized electronic communications metadata in order to produce complex contact chaining results, an adversary would be confident that any account used during the disclosed timeframe could not be chained and thus was safe from collection. In essence, disclosure of the docket numbers and dates would allow targets to know what information the NSA possessed at particular times, as well as gaps in coverage that would reveal that information from a particular period was "safe."

UNCLASSIFIED

Similarly, if an adversary knew that a particular account was used only during the disclosed gap in coverage, that adversary could now revert to using that "safe" account in order to thwart future collection and detection.

47. After reviewing this information, I have determined that this information meets the criteria for classification in Sections 1.4(c), 1.4(d), and 1.4(g) of E.O. 13526 and is currently and properly classified at the SECRET level. As a result, it is exempt from disclosure under FOIA Exemption 1. Likewise, this information relates to a function or an activity of the NSA, specifically its SIGINT mission and the activities carried out in furtherance of this mission with this particular intelligence program, and is therefore protected under FOIA Exemption 3.

Details Regarding the Facilities from which Electronic Communications

Metadata was Collected

48. NSA has withheld information regarding the specific facilities from which electronic communications metadata was collected and operational details thereof based on FOIA Exemptions 1 and 3. This information was redacted and withheld in the following documents: Documents 002, 003, 009, 040, 041, 042, 046, 051, 054, 056, 059, 060, and 066.

49. Releasing the facilities subject to any of the PR/TT Primary Orders would disclose classified intelligence sources and methods. Releasing any information that would tend to reveal the specific facilities would reveal currently and properly classified information concerning NSA's methodology for identifying specific facilities for collection. While the NSA's FISC-authorized PR/TT metadata collection program is no longer operational, publicly producing information revealing which facilities were used

UNCLASSIFIED

for collection under that program would provide NSA's adversaries with unique insights into NSA's analytic process for identifying worldwide facilities for collection. Adversaries could extrapolate such information and apply these insights against other forms of communications used by said adversaries. Additionally, disclosure of the facilities from which metadata was collected pursuant to the PR/TT program would alert the targets to which email metadata records NSA did and did not collect, as well as the nature and scope of the PR/TT program. Disclosure of this information would allow targets to know what electronic communications metadata the NSA was collecting during the duration of the PR/TT program, as well as gaps in that collections that could reveal that information handled by a particular facility was "safe." Additionally, disclosing details regarding the PR/TT facilities would allow our adversaries insight into NSA's techniques and operational capabilities which could enable them to frustrate the government's collection of communications in other contexts. With this information, our adversaries would be able to undermine the IC's national security mission.

50. After reviewing this information, I have determined that this information meets the criteria for classification in Sections 1.4(c), 1.4(d), and 1.4(g) of E.O. 13526 and is currently and properly classified at the TOP SECRET level. As a result, it is exempt from disclosure under FOIA Exemption 1. Likewise, this information relates to a function or an activity of the NSA, specifically its SIGINT mission and the activities carried out in furtherance of this mission with this particular intelligence program, and is therefore protected under FOIA Exemption 3.

UNCLASSIFIED

Identities of the Targets of PR/IT Collection

51. The NSA withheld from disclosure information relating to the identities of the targets from which communications were collected under the PR/IT program. This information was redacted in the following documents:⁶ Documents 002, 003, 009, 031, 035, 036, 040, 041, 042, 046, 051, 054, 056, 059, 060, 061, 062, 063, and 066.

52. I have reviewed this information and determined that the identities of the targets of PR/IT collection are currently and properly classified at the TOP SECRET level in accordance with E.O. 13526, because the release of this information could reasonably be expected to cause exceptionally grave damage to the national security. This information falls within Sections 1.4(c), 1.4(d), and 1.4(g) of E.O. 13526.

53. The government has not publicly disclosed the specific targets of collection under the PR/IT program. Disclosing the specific targets would identify exactly which entities the government believes are engaged in terrorism and would reveal the full scope of the government's collection efforts under the PR/IT program, along with the limits of those efforts. This information would provide our adversaries detailed, damaging insight into the scope and timing of an important collection program. Knowing this scope and timing would enable our adversaries to gain insight into whether certain past communications are, or are not, likely to have been targeted and captured and cause those identified targets to take steps to circumvent future collection that might occur under other programs. Such evasion techniques may inhibit access to a target's communications, thereby denying the United States access to information crucial to the national security.

⁶ This information also appears in and was redacted from the case caption of every document filed with the FISC.

UNCLASSIFIED

54. This same information is also protected from release by statute and is likewise exempt from release based on FOIA Exemption 3, 5 U.S.C. § 552(b)(3). Specifically, there are three Exemption 3 statutes that protect from public release the identities of the providers participating in the PR/TT program: section 6 of the NSA Act, 50 U.S.C. § 3605, 18 U.S.C. § 798, and Section 102A(i)(1) of the National Security Act, as amended, 50 U.S.C. § 3024(i)(1).

55. The identities of the targets of the PR/TT program relate to a “function of the National Security Agency,” 50 U.S.C. § 3605. Indeed, it relates to one of NSA’s primary functions, its SIGINT mission. Further, any disclosure of the scope of this collection of electronic communications metadata, as stated above, would reveal NSA’s capabilities. Thus, the identities of the targets, if revealed, would disclose “information with respect to [NSA’s] activities” in furtherance of its SIGINT mission. 50 U.S.C. § 3605.

56. Likewise, the identities of the targets are protected from public release pursuant to Section 102A(i)(1) of the National Security Act, as amended, 50 U.S.C. § 3024(i)(1), which states that “[t]he Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure.” Revealing identities of the targets would provide our adversaries with information from which they could deduce the intelligence sources (the providers) from which the records were collected, and thus, this information falls squarely within the protection of this statute and should be afforded absolute protection from release.

57. Finally, the information is protected from release under 18 U.S.C. § 798, which protects from disclosure information concerning the communications intelligence

UNCLASSIFIED

activities of the United States, or obtained by communications intelligence processes. Disclosure of the identities of the targets of the PR/TT program would reveal key information about the communications intelligence activities of the United States, thereby falling within the scope of protection offered by this statute.

Adversary Threat and Tradecraft Information

58. The NSA withheld from disclosure information relating to the methods and techniques by which our adversaries attempt to conceal their communications to avoid detection and collection, otherwise known as their tradecraft. NSA also withheld information concerning the threats posed by particular adversaries. This information was redacted and withheld in the following documents: Documents 002, 041, 042, 054, 056, 060, 061, and 066.

59. I have reviewed this information and determined that this information is currently and properly classified at the TOP SECRET level in accordance with E.O. 13526, because the release of this information could reasonably be expected to cause exceptionally grave damage to the national security. This information falls within Sections 1.4(c), 1.4(d), and 1.4(g) of E.O. 13526.

60. Disclosure of this information could alert targets to the Intelligence Community's awareness of the ways in which adversaries attempt to conceal their communications and evade collection. It could also alert targets to the government's awareness of particular threats to or plots against the United States because adversaries know how they communicate and therefore, upon a disclosure of the government's awareness of specific examples of adversary tradecraft, targets would learn which of their communications may have been vulnerable to collection. This information could also

UNCLASSIFIED

UNCLASSIFIED

reveal the scope of the government's capabilities to detect and collect target communications because it reveals our ability to employ technology and analysis to recognize and defeat particular types of adversary tradecraft. If targets know that the government is aware of certain circumvention techniques and is able, nonetheless, to collect communications, our adversaries may attempt to evade collection of their communications through new or alternative methods. Similarly, if targets know that the government has difficulty detecting certain types of evasive tradecraft, targets may rely heavily on those techniques to prevent further detection. This knowledge may ultimately inhibit access to a target's communications, thereby denying the United States information crucial to the national security.

61. This same information is also protected from release by statute and is likewise exempt from release based on FOIA Exemption 3, 5 U.S.C. § 552(b)(3). Specifically, there are three Exemption 3 statutes that protect from public release the identities of the providers participating in the PR/TT program: section 6 of the NSA Act, 50 U.S.C. § 3605, 18 U.S.C. § 798, and Section 102A(i)(1) of the National Security Act, as amended, 50 U.S.C. § 3024(i)(1).

62. Information about adversary tradecraft relates to a "function of the National Security Agency," 50 U.S.C. § 3605. Indeed, it relates to one of NSA's primary functions, its SIGINT mission. Any disclosure regarding NSA's awareness of and ability to detect adversary tradecraft, as stated above, would reveal NSA's collection capabilities. Thus, this information, if revealed, would disclose "information with respect to [NSA's] activities" in furtherance of its SIGINT mission. 50 U.S.C. § 3605.

UNCLASSIFIED

63. Likewise, information about adversary tradecraft is protected from public release pursuant to Section 102A(i)(1) of the National Security Act, as amended, 50 U.S.C. § 3024(i)(1), which states that “[t]he Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure.” Revealing NSA’s awareness of adversary tradecraft would provide our adversaries with information from which they could deduce the intelligence methods by which this tradecraft was detected, and thus, this information falls squarely within the protection of this statute and should be afforded absolute protection from release.

64. Finally, the information is protected from release under 18 U.S.C. § 798, which protects from disclosure information concerning the communications intelligence activities of the United States, or obtained by communications intelligence processes. The disclosure of government knowledge regarding adversary tradecraft would reveal precisely the procedures and methods that the NSA uses to intercept communications of its targets, thereby falling within the scope of protection offered by this statute.

Operational Details About the PR/TT Program

65. The NSA withheld from disclosure information relating to the operational details regarding the PR/TT program. This information includes, generally: details about the PR/TT collection equipment; collection capabilities; analytical techniques that NSA applies to the data; and storage, database, and analytic tool names, capabilities, and functionality. This information was redacted and withheld in the following documents: Documents 002, 003, 004, 005, 006, 009, 011, 030, 031, 032, 033, 035, 036, 037, 040, 041, 042, 045, 046, 047, 048, 051, 054, 056, 059, 060, 061, 062, 063, 064, 065, and 066.

UNCLASSIFIED

UNCLASSIFIED

66. These withholdings did not include information similar to that which was recently declassified regarding the Section 215 telephony metadata collection program. Where declassified operational details about the Section 215 program were similar to those in the PR/TT program, that information was segregated and released in the PR/TT records to the extent possible. For example, operational information released in Document 062, the PR/TT NSA Review, was similar to that released previously regarding the Section 215 program, including but not limited to descriptions about the Reasonable Articulate Suspicion (RAS) Approval Process, the Activity Detection Alerting process, contact chaining, use of Station Table, and the use of a defeat list.

67. Disclosure of the remaining withheld operational details would reveal to our adversaries NSA's technical capabilities. With this information, our adversaries could attempt to develop countermeasures to frustrate NSA's SIGINT techniques and technologies. As a result, NSA's ability to maximize the utility of these techniques and technologies in other contexts may be significantly hampered. Its disclosure therefore could reasonably be expected to cause exceptionally grave damage to the national security of the United States and it is, accordingly, properly classified TOP SECRET pursuant to E.O. 13526.

68. Furthermore, any releases of additional operational details about the PR/TT program would reveal to our adversaries highly detailed facts about the nature of the NSA's uses of a specific intelligence source that could assist them in undermining the IC's national security mission. Again, foreign intelligence targets know how they communicate, and upon a disclosure of information that describes precisely how the PR/TT metadata was collected, analyzed, and used, these targets would know what type

UNCLASSIFIED

of information can be collected (and also, the type of information was not or cannot be collected). With this information, targets will attempt to frustrate collection of similar types of information.

69. Finally, release of operational information about NSA databases may provide a foreign intelligence service with information that would be useful should they attempt to penetrate NSA networks. Providing database names combined with details about the database would provide a roadmap for adversaries to identify and locate the most sensitive information on NSA's networks, thereby rendering NSA and its SIGINT mission vulnerable.

70. This same information is also protected from release by statute and is likewise exempt from release based on FOIA Exemption 3, 5 U.S.C. § 552(b)(3). Specifically, there are three Exemption 3 statutes that protect from public release the operations details of the PR/TT program: section 6 of the NSA Act, 50 U.S.C. § 3605, 18 U.S.C. § 798, and Section 102A(i)(1) of the National Security Act, as amended, 50 U.S.C. § 3024(i)(1).

71. Information about the operational details of the PR/TT program inherently relates to a "function of the National Security Agency," 50 U.S.C. § 3605. Indeed, it relates to one of NSA's primary functions, its SIGINT mission. Any disclosure regarding the operational details of the program, including database and analytic tool names, as stated above, would reveal NSA's capabilities and techniques. Thus, this information, if revealed, would disclose "information with respect to [NSA's] activities" in furtherance of its SIGINT mission. 50 U.S.C. § 3605.

UNCLASSIFIED

UNCLASSIFIED

72. Likewise, information about the operational details of the PR/TT program is protected from public release pursuant to Section 102A(i)(1) of the National Security Act, as amended, 50 U.S.C. § 3024(i)(1), which states that “[t]he Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure.” Revealing operational details about the program would provide our adversaries with a roadmap of the intelligence methods by which the PR/TT information was collected, and thus, this information falls squarely within the protection of this statute and should be afforded absolute protection from release.

73. Finally, the information is protected from release under 18 U.S.C. § 798, which protects from disclosure information concerning the communications intelligence activities of the United States, or obtained by communications intelligence processes. The disclosure of the operational details of the PR/TT program would reveal precisely the procedures and methods that the NSA uses to collect communications intelligence, thereby falling within the scope of protection offered by this statute.

Secondary Orders

74. NSA has also withheld in full all Secondary Orders issued during the PR/TT program. These Orders are described on the Vaughn index at entry number 10.

75. These Orders have been withheld in their entirety, as disclosing even the number of Secondary Orders would reveal the number of providers who were compelled to participate in the PR/TT program, a fact that has not been publicly disclosed and remains currently and properly classified. Revealing the number of providers that received orders under the PR/TT program would allow readers to deduce the identities of those providers. Additionally, any attempt to redact the identity of the service providers

UNCLASSIFIED

in these Secondary Orders would allow a reader to ascertain the identity of the provider simply by looking at the length of the redacted/blocked material, and comparing any redacted Secondary Order with other declassified documents.

76. Disclosure of this information, which would reveal the identities of the providers participating in the PR/TT program, could reasonably be expected to cause exceptionally grave damage to the national security for the reasons described in detail above. I have reviewed this information and determined that it is currently and properly classified as TOP SECRET and falls within Sections 1.4(c), 1.4(d), and 1.4(g) of E.O. 13526.

77. Foreign intelligence targets know how they communicate, and therefore, would know, upon a disclosure of NSA's capabilities via the release of the identity of any particular telecommunications service provider, which of their electronic communications metadata records were potentially vulnerable to NSA's collection and querying (and also, which of their communications may not have been vulnerable). Disclosure of this information would allow targets to know what information the NSA was collecting at particular times. In addition, once alerted, targets could potentially frustrate NSA collection under other programs by switching to a provider that is not identified as having been subject to the FISC's Orders or Secondary Orders under this program. This may result in denial of access to targets' communications and therefore result in a loss of access to information crucial to the national security and defense of the United States.

78. This same information is also protected from release by statute and is likewise exempt from release based on FOIA Exemption 3, 5 U.S.C. § 552(b)(3).

UNCLASSIFIED

Specifically, there are three Exemption 3 statutes that protect from public release the identities of the providers participating in the PR/TT program: section 6 of the NSA Act, 50 U.S.C. § 3605, 18 U.S.C. § 798, and Section 102A(i)(1) of the National Security Act, as amended, 50 U.S.C. § 3024(i)(1).

79. The Secondary Orders relate to a “function of the National Security Agency,” 50 U.S.C. § 3605. Indeed, they relate to one of NSA’s primary functions, its SIGINT mission. Further, any disclosure of the scope of this collection of electronic communications metadata as revealed in the Secondary Orders, as stated above, would reveal NSA’s capabilities, as well as the sources and methods used by the NSA in conducting its foreign intelligence mission. Thus, the Secondary Orders, if revealed, would disclose “information with respect to [NSA’s] activities” in furtherance of its SIGINT mission. 50 U.S.C. § 3605.

80. Likewise, the Secondary Orders are protected from public release pursuant to Section 102A(i)(1) of the National Security Act, as amended, 50 U.S.C. § 3024(i)(1), which states that “[t]he Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure.” It is without question that the Secondary Orders in the PR/TT program reveal both the intelligence sources and methods for the electronic communications metadata records, and thus, they fall squarely within the protection of this statute and are afforded absolute protection from release.

81. Finally, the information is protected from release under 18 U.S.C. § 798, which protects from disclosure information concerning the communications intelligence activities of the United States, or obtained by communications intelligence processes. Disclosing the Secondary Orders would reveal the scope of the PR/TT program and the

UNCLASSIFIED

methods by which the NSA intercepts communications of its targets, thereby falling within the scope of protection offered by this statute.

IV. SEGREGABILITY

82. All of these documents have been reviewed for purposes of complying with FOIA's segregability provision, which requires the U.S. Government to release "any reasonably segregable portion of a record" after proper application of the FOIA exemptions. 5 U.S.C. § 552(b). An intensive, line-by-line review of each one of these documents was performed by multiple agencies and all reasonably segregable, non-exempt information has been released.

83. Further, with respect to all of the redactions taken, it is my judgment that any information in those documents that, viewed in isolation, could be considered unclassified, is nonetheless classified in the context of this case because it can reasonably be expected to reveal (directly or by implication) classified national security information concerning the timing or nature of intelligence activities, sources, and methods when combined with other information that might be available to the public or adversaries of the United States. In these circumstances, the disclosure of even seemingly mundane portions of these documents, when considered in conjunction with other publicly available information, could reasonably be expected to assist a sophisticated adversary in deducing particular intelligence activities or sources and methods, and possibly lead to the use of countermeasures that may deprive the United States of critical intelligence collected under other, still-active programs.

84. For example, this pertains to even otherwise unclassified information that is contained in the withheld-in-full Secondary Orders. The withheld-in-full Secondary

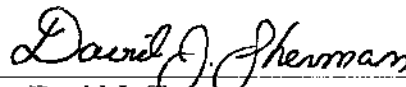
UNCLASSIFIED

Orders cannot reasonably be segregated and released without disclosing the number of Secondary Orders that accompanied each Primary Order issued under the PR/TT program, thereby risking disclosure of currently and properly classified information concerning the number and identities of the providers who were compelled to participate in the PR/TT program.

V. CONCLUSION

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Executed this 31st day of October, 2014, pursuant to 28 U.S.C. § 1746.



Dr. David J. Sherman
Associate Director for Policy and Records,
National Security Agency

UNCLASSIFIED