

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER,)	
)	
Plaintiff,)	Civil No. 06-00096 (HHK)
)	
v.)	
)	
DEPARTMENT OF JUSTICE,)	
)	
Defendant.)	
<hr/>		
AMERICAN CIVIL LIBERTIES UNION, et al.,)	
)	Civil No. 06-00214 (HHK)
Plaintiffs,)	
)	
v.)	
)	
DEPARTMENT OF JUSTICE,)	
)	
Defendant.)	
<hr/>		

DECLARATION OF LOUIS F. GILES

I, Louis F. Giles, hereby declare and state:

1. I am the Director of Policy for the National Security Agency (“NSA” or the “Agency”) and have served in this position since February 2002. I have served with NSA for 31 years, and prior to my current assignment, I held various senior and supervisory positions including Chief of the Information Assurance Directorate's (“IAD”) Customer Relations Office and Deputy Chief of the Special Programs Staff of NSA Signals Intelligence Directorate's Cryptanalysis Group. As the Director of Policy, I am a TOP SECRET classification authority, pursuant to Section 1.3 of Executive Order 12958, as amended March 25, 2003, and I am responsible for the processing of all requests made

pursuant to the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, for NSA records. It is also my responsibility to assert FOIA Exemptions in the course of litigation.

ORIGIN AND MISSION OF NSA

2. NSA was established by Presidential Directive in 1952 as a separately organized agency within the Department of Defense. See Executive Order 12333, Section 1.12(b). NSA's cryptologic mission has three functions: to collect, process, and disseminate SIGINT information for national foreign intelligence purposes; to conduct information security activities; and to conduct operations security training for the United States Government.

3. Signals intelligence is one of NSA's primary functions. NSA's SIGINT mission is to obtain information from foreign electromagnetic signals and to provide, frequently on a rapid response basis, reports derived from such information or data to national policy makers and the intelligence community of the United States Government. A primary SIGINT mission of NSA is to intercept communications in order to obtain foreign intelligence information necessary to the national defense, national security, or the conduct of the foreign affairs of the United States. The SIGINT collection mission of NSA provides national policy makers and the intelligence community with highly reliable foreign intelligence information.

4. The Agency's SIGINT role has been enhanced by superior intelligence sources and methods, which enable it to keep pace with challenging developments in virtually every area of technology. In the course of fulfilling these missions, NSA obtains information and reports it to customers within the United States Government. From a SIGINT mission standpoint, some of the information NSA gleans may not be significant;

however, it is frequently interwoven with information that reveals information concerning NSA's activities.

5. 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 external threats. The second reason is to obtain the information necessary to direct the foreign policy of the United States. Information produced by SIGINT is relevant to a wide range of important issues, including 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.

6. NSA has developed a sophisticated worldwide SIGINT collection network that acquires, among other things, foreign and international electronic communications. The technological infrastructure that supports NSA's foreign intelligence information collection network has taken years to develop at a substantial cost and untold human effort. It relies on sophisticated collection and processing technology.

7. NSA's ability to produce foreign intelligence information depends on its access to foreign and international electronic communications. Further, SIGINT technology is both expensive and fragile. Public disclosure of either the capability to collect specific communications or the substance of the information itself can easily alert targets to the vulnerability of their communications. Disclosure of even a single communication holds the potential of revealing the intelligence collection techniques that

are applied against targets around the world. Once alerted, SIGINT targets can easily frustrate SIGINT collection.

8. Information obtained from intercepted foreign communications is called communications intelligence ("COMINT"). NSA's COMINT efforts constitute only part of the functions and activities of the Agency. A fundamental tenet of the COMINT process is that the identity of specific communications (commonly referred to as "targets"), the degree of success in exploiting these targets, the vulnerability of particular foreign communications, and the extent of any cryptologic successes are all matters that must be maintained in strictest secrecy because of the fragility of the ability to exploit foreign communications. Disclosure of the identity of the targets, the degree of success or weakness in exploiting those targets, the vulnerability of particular foreign communications, and the extent of any cryptologic success would encourage countermeasures by the targets of NSA'S COMINT efforts. If a foreign power is successful in defeating an intercept operation, all of the intelligence from that source is lost unless and until NSA can establish new and equivalent exploitation of the foreign power's signals. If a source becomes unavailable, the military, national policymakers and intelligence community must operate without the information the signals provided. Such losses are extremely harmful to the national security of the United States.

PLAINTIFFS EPIC AND ACLU'S FOIA REQUESTS

9. The purpose of this declaration is to advise the Court of the Agency's processing of the referrals it received from the Department of Justice in response to Plaintiffs EPIC and ACLU's FOIA requests to that agency. Because of the highly

sensitive nature of the TSP, this declaration addresses the appropriateness of the Agency's invocation of FOIA Exemptions 1, 3 and 5 in withholding responsive records.

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, which establishes such criteria, is Executive Order 12958, as amended 25 March 2003.

11. Executive Order 12958 Section 1.4 provides that information may not be considered for classification unless it falls within seven specifically enumerated categories of information. The categories of classified information in the documents at issue here are those found in Section 1.4(b), foreign government information; 1.4 (c), intelligence activities (including special activities), intelligence sources and methods, or cryptology; Section 1.4(d), foreign relations or foreign activities of the United States, including confidential sources; and Section 1.4(g), vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism.

12. I have reviewed Joseph B.'s Declaration, which was submitted with this current litigation, since he is the Original Classification Authority at NSA for the Terrorist Surveillance Program (TSP). Based on my review of Joseph B.'s declaration, I have concluded that the records referred to NSA by the Department of Justice in response to Plaintiffs EPIC and ACLU's FOIA requests pertain to information that meets the

criteria for classification as set forth in Subparagraphs (c) and (g) of Section 1.4 of Executive Order 12958, as amended, which authorizes the classification of information concerning “intelligence activities (including special activities), intelligence sources or methods, or cryptology,” and “vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection systems relating to national security, which includes defense against transnational terrorism.”

13. Additionally, the documents are currently and properly classified TOP SECRET pursuant to Executive Order 12958, as amended 25 March 2003, sections 1.2.(1), because their disclosure reasonably could be expected to cause exceptionally grave damage to the national security. Further, the information is subject to Sensitive Compartmented Information (SCI) control systems, which requires special access and handling restrictions. Accordingly, since the responsive information was reviewed by Joseph B. for classification under the current classification Executive Order, Executive Order 12958, as amended, and determined to be currently and properly classified TOP SECRET-SCI and marked with proper classifications, the documents in question are properly exempt from disclosure pursuant to FOIA Exemption 1.

FOIA EXEMPTION THREE

14. Section 552(b)(3) of the FOIA provides that the FOIA does not require the release of matters that are specifically exempted from disclosure by statute, provided that the relevant statute requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or establishes particular criteria for withholding or refers to particular types of matter to be withheld. *See* 5 U.S.C. § 552(b)(3). Information about NSA’s COMINT efforts directly relates to the Agency’s most core functions and

activities. These functions and activities are protected from public disclosure by several statutes. Congress has passed these statutes to protect the fragile nature of NSA's COMINT efforts, including, but not limited to, the existence and depth of signal intelligence-related analytical successes, weaknesses and exploitation techniques. These statutes recognize the vulnerability of signals intelligence to countermeasures of a foreign power and the significance of the loss of valuable foreign intelligence information to national policymakers and the intelligence community.

15. The first of these statutes is a statutory privilege unique to NSA. NSA's statutory privilege is set forth in section 6 of the National Security Agency Act of 1959, Public Law 86-36 (50 U.S.C. § 402 note). Section 6 of the NSA Act provides that **“[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, of any information with respect to the activities thereof, . . .”** (emphasis added). By this language Congress expressed its finding that disclosure of any information relating to NSA activities is potentially harmful. The courts have held that the protection provided by this statutory privilege is, by its very terms, absolute. *See, e.g., Linder v. NSA*, 94 F.3d 693 (D.C. Cir. 1996). 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. *See Hayden v. NSA*, 608 F.2d 1381 (D.C. Cir. 1979). Further, while in this case the harm would be very serious, NSA 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. *Id.* To invoke this privilege, NSA must demonstrate only that the information sought to be protected falls within the scope of

section 6. NSA's functions and activities are therefore protected from disclosure regardless of whether or not the information is classified.

16. The second applicable 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 communication intelligence derived from the communications of any foreign government. The term "communications intelligence," as defined by Section 798, means that the procedures and methods used in the interception of communications and obtaining of information from such communications by other than the intended recipients.

17. The third applicable statute is Section 102A(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004, 50 U.S.C. § 403-1(i)(1), which states that the Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure." NSA, as one of the member agencies of the U.S. intelligence community, must also protect intelligence sources and methods. Like the protection afforded to core NSA activities by Section 6 of the NSA Act of 1959, the protection afforded to intelligence sources and methods is absolute. *See Central Intelligence Agency v. Sims*, 471 U.S. 159 (1985). Whether the sources and methods at issue are classified is irrelevant for purposes of the protection afforded by the National Security Act. *Id.*

18. Based on my review of Joseph B.'s declaration, I am confident that the information referred to NSA by the Department of Justice in response to Plaintiffs EPIC and ACLU's FOIA requests meet the criteria for protection based on all three statutes and

accordingly, this information is properly exempt from disclosure pursuant to FOIA Exemption 3.

FOIA EXEMPTION FIVE

19. Section 552(b)(5) of the FOIA protects inter-agency or intra-agency memoranda or letters which would not be available by law to a party in litigation with the agency. This exemption protects information that is normally privileged in the civil discovery context, such as information that is part of a predecisional deliberative process, and/or attorney-client privileged information, and/or attorney work product.


20. Again, based on my review of Joseph B.'s declaration information that is responsive to Plaintiffs' requests for information (including EPIC's Item 1, 2, 3, and 4 and ACLU's Items 2, 3, 5, 6, 7, 8, 9, 14, 15, and 16) would also be exempt under FOIA Exemption 5, in addition to being exempt under FOIA Exemptions 1 and 3, because the information is privileged and protected by the deliberative process privilege, attorney-client privilege and/or attorney work product.

21. In conclusion, I am satisfied that NSA has properly invoked Exemptions 1, 3 and 5 as the basis for withholding the information discussed therein. Moreover, I am confident that the responsive information cannot be segregated so as to release any non-exempt information. Finally, because of the highly sensitive nature of the information involved and the detailed information provided in this declaration and Mr. Joseph B.'s declaration, requiring NSA to produce an index of the particular documents withheld would be inappropriate because it would require a description of documents that would reveal information so highly classified that few Agency officials^(r1) have been provided with access to it; would require a description of potential documents the existence of

which NSA has neither confirmed nor denied; and would itself reveal information specifically protected by FOIA Exemptions 1 and 3.

22. I declare under penalty of perjury that the facts set forth above are true and correct.

Executed, this 8th day of September 2006, pursuant to 28 U.S.C. § 1746.



LOUIS F. GILES
Director of Policy
National Security Agency