

A Statement of Material Facts as to Which There Is No Genuine Issue and a Proposed Order are attached.

Dated: December 22, 2010

Respectfully submitted,

TONY WEST
Assistant Attorney General

RONALD C. MACHEN JR.
United States Attorney

ELIZABETH J. SHAPIRO
Deputy Branch Director

/s/ Judson O. Littleton
JUDSON O. LITTLETON

TX Bar No. 24065635

Trial Attorney

United States Department of Justice

Civil Division, Federal Programs Branch

20 Massachusetts Ave. NW

Washington, DC 20530

Tel. (202) 305-8714

Fax (202) 616-8470

Judson.O.Littleton@usdoj.gov

Attorneys for Defendant

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

ELECTRONIC PRIVACY INFORMATION CENTER,)	
)	
Plaintiff,)	
)	
v.)	Civil Action No. 10-1533 (RJL)
)	
NATIONAL SECURITY AGENCY,)	
)	
Defendant.)	

**MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT’S
MOTION FOR SUMMARY JUDGMENT**

STATEMENT

In this action under the Freedom of Information Act, plaintiff Electronic Privacy Information Center (“EPIC”) seeks the disclosure of records relating to an alleged cooperative research and development agreement reached between defendant National Security Agency (“NSA”) and Google in early 2010, as well as other alleged communications between NSA and Google regarding certain Google technologies. NSA informed EPIC that it could neither confirm nor deny the existence of any such records, pursuant to FOIA’s exemption from disclosure of records that are specifically exempted by other statutes, 5 U.S.C. § 552(b)(3). NSA’s response was valid as a matter of law. Accordingly, NSA is entitled to the entry of summary judgment in its favor.

1. Background

By letter dated February 4, 2010, plaintiff EPIC submitted a FOIA request to defendant NSA. *See* Letter from Matthew Phillips, Appellate Advocacy Counsel, EPIC, to FOIA/PA Officer, NSA (Janosek Decl. Ex. A). EPIC began its request by describing recent events concerning a cyber attack on Google's corporate infrastructure by hackers originating from China. EPIC then summarized media coverage in the immediate aftermath of the attack that reported that "Google and the NSA had entered into a 'partnership'" and a "collective research and development agreement." FOIA Request at 1-2; *see also* Complaint ¶¶ 5-7 (Dkt. No. 1). Against this background, EPIC requested records falling under the following categories:

1. All records concerning an agreement or similar basis for collaboration, final or draft, between the NSA and Google regarding cyber security;
2. All records of communication between NSA and Google concerning Gmail, including but not limited to Google's decision to fail to routinely encrypt Gmail messages prior to January 13, 2010; and
3. All records of communications regarding NSA's role in Google's decision regarding the failure to routinely deploy encryption for cloud-based computing service, such as Google Docs.

FOIA Request at 3; Complaint ¶ 12 (Dkt. No. 1).

NSA responded to EPIC's request by letter dated March 10, 2010. *See* Letter from Pamela N. Phillips, Chief, FOIA/PA Office, NSA to Matthews Phillips, Esq. (Janosek Decl. Ex. B) (the "NSA Response"). NSA explained that it "works with a broad range of commercial partners and research associates" in fulfilling its

“longstanding Information Assurance mission,” because such partnerships help “ensure the availability of secure tailored solutions for the Department of Defense and national security systems customers today and cutting-edge technologies that will secure the information systems of tomorrow.” *Id.* at 1. Noting, however, that it is “authorized by statute to protect information concerning its functions and activities,” NSA stated that it could “neither confirm nor deny whether the company has a relationship with the Agency related to the issues [EPIC] describe[d]” in its request. *Id.* NSA relied on FOIA Exemption 3, 5 U.S.C. § 552(b)(3), and Section 6 of the National Security Agency Act of 1959, Pub. L. No. 86-36, 73 Stat. 63 (codified at 50 U.S.C. § 402 note), as justification for its response.¹

EPIC filed an administrative appeal of this determination in a letter dated May 7, 2010. *See* Letter from Jared Kaprove, Domestic Surveillance Counsel, EPIC, and John Verdi, Director, Open Government Project, EPIC, to NSA/CSS FOIA Appeal Authority (Janosek Decl. Ex. C). EPIC argued that NSA’s response was unlawful because “NSA fail[ed] to provide any factual basis for the conclusion that any portion of the responsive documents is exempt under Section 6, much less all portions of all requested records.” *Id.* at 2. Accordingly, EPIC contended, “[w]ithout considerably more information about the number and nature of documents for

¹ The refusal to confirm or deny the existence or nonexistence of records responsive to a FOIA request is commonly referred to as a *Glomar* response, under terminology derived from the D.C. Circuit’s decision in *Phillippi v. CIA*, 546 F.2d 1009 (1976). There, CIA successfully defended its refusal to confirm or deny the existence of records concerning CIA’s reported contacts with the media regarding a ship named *Hughes Glomar Explorer*. *Id.* at 1011.

which the agency is claiming exemption from the FOIA, it is impossible for the NSA to support the validity of the asserted exemption.” *Id.* at 3.

NSA received the administrative appeal letter but had not finished processing it when EPIC filed the Complaint in this case on September 13, 2010. The filing of that Complaint terminated NSA’s processing of the appeal. Janosek Decl. ¶ 7.

2. FOIA and Summary Judgment Standard of Review

FOIA’s “basic purpose” reflects a “general philosophy of full agency disclosure unless information is exempted under clearly delineated statutory language.” *John Doe Agency v. John Doe Corp.*, 493 U.S. 146, 152 (1989) (internal quotation marks and citation omitted). “Congress recognized, however, that public disclosure is not always in the public interest.” *CIA v. Sims*, 471 U.S. 159, 166-167 (1985).

Accordingly, in passing FOIA, “Congress sought ‘to reach a workable balance between the right of the public to know and the need of the Government to keep information in confidence to the extent necessary without permitting indiscriminate secrecy.’” *John Doe Agency*, 493 U.S. at 152 (quoting H.R. Rep. No. 89-1497, at 6 (1966), reprinted in 1966 U.S.C.C.A.N. 2416, 2423); see also *Center for Nat’l Sec. Studies v. DOJ*, 331 F.3d 918, 925 (D.C. Cir. 2003) (“FOIA represents a balance struck by Congress between the public’s right to know and the government’s legitimate interest in keeping certain information confidential.”).

FOIA mandates disclosure of government records unless the requested information falls within one of nine enumerated exceptions. See 5 U.S.C. § 552(b).

“A district court only has *jurisdiction* to compel an agency to disclose *improperly withheld* agency records,” *i.e.*, records that do “not fall within an exemption.” *Minier v. CIA*, 88 F.3d 796, 803 (9th Cir. 1996); *see also* 5 U.S.C. § 552(a)(4)(B) (giving the district court jurisdiction only “to enjoin the agency from withholding agency records and to order the production of any agency records improperly withheld from the complainant”); *Kissinger v. Reporters Comm. for Freedom of the Press*, 445 U.S. 136, 150 (1980) (“Under 5 U.S.C. § 552(a)(4)(B)[,] federal jurisdiction is dependent upon a showing that an agency has (1) ‘improperly’; (2) ‘withheld’; (3) ‘agency records.’”). Although FOIA’s statutory exemptions are to be narrowly construed, *see Department of the Interior v. Klamath Water Users Protective Ass’n*, 532 U.S. 1, 8 (2001), courts must also give those exemptions “meaningful reach and application,” *John Doe Agency*, 493 U.S. at 152. “Requiring an agency to disclose exempt information is not authorized.” *Minier*, 88 F.3d at 803 (internal quotation marks and citation omitted).

Summary judgment is the procedural vehicle by which most FOIA actions are resolved. *Reliant Energy Power Generation, Inc. v. FERC*, 520 F. Supp. 2d 194, 200 (D.D.C. 2007). The government bears the burden of proving that the withheld information falls within the exemptions it invokes. *See* 5 U.S.C. § 552(a)(4)(B); *King v. U.S. Dep’t of Justice*, 830 F.2d 210, 217 (D.C. Cir. 1987). A court may grant summary judgment to the government entirely on the basis of information set forth in an agency’s affidavit or declaration if it “describe[s] the justifications for

nondisclosure with reasonably specific detail, demonstrate[s] that the information withheld logically falls within the claimed exemption, and [is] not controverted by either contrary evidence in the record nor by evidence of agency bad faith.” *Larson v. Dep’t of State*, 565 F.3d 857, 862 (D.C. Cir. 2009) (internal quotation marks and citation omitted). “Ultimately, an agency’s justification for invoking a FOIA exemption is sufficient if it appears logical or plausible.” *Wolf v. CIA*, 473 F.3d 370, 374-375 (D.C. Cir. 2007) (internal quotation marks and citations omitted).

ARGUMENT

PURSUANT TO EXEMPTION 3, NSA PROPERLY REFUSED TO CONFIRM OR DENY THE EXISTENCE OF RECORDS CRITICAL TO ITS MISSION

A. The National Security Agency Act Provides that the NSA Withhold Information that Would Reveal Any Function or Activities of the NSA

NSA’s response to EPIC’s FOIA request was lawful and well within the statutory exemptions Congress put in place to protect information vital to NSA’s mission. Due to the high sensitivity of NSA’s mission, Congress intentionally and reasonably provided the Agency with far-reaching authority to safeguard information relating to that mission.

Exemption 3 to FOIA’s disclosure requirements provides that an agency is not required to disclose records that are “specifically exempted from disclosure by statute,” if the 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 matters to be withheld.” 5

U.S.C. § 552(b)(3).² The “purpose of Exemption 3 [is] to assure that Congress, not the agency, makes the basic nondisclosure decision.” *Association of Retired R.R. Workers v. U.S. R.R. Retirement Bd.*, 830 F.2d 331, 336 (D.C. Cir. 1987). It was promulgated in recognition of other, agency-specific statutes limiting the disclosure of information held by the government and incorporates those statutes within the exemptions to FOIA. *See Balridge v. Shapiro*, 455 U.S. 345, 352-353 (1982); *Essential Info., Inc. v. U.S. Info. Agency*, 134 F.3d 1165, 1166 (D.C. Cir. 1998).

Courts apply a two-pronged inquiry when evaluating an agency’s invocation of Exemption 3. *See Sims*, 471 U.S. at 167-168. First, the court must determine whether the statute identified by the agency qualifies as an exempting statute under Exemption 3. Second, the court should consider whether the withheld material falls within the scope of the exempting statute. *See id.* As the D.C. Circuit has recognized, “Exemption 3 presents considerations distinct and apart from the other eight exemptions.” *Ass’n of Retired R.R. Workers*, 830 F.2d at 336. “[I]ts applicability depends less on the detailed factual contents of specific documents; the sole issue for decision is the existence of a relevant statute and the inclusion of withheld material within the statute’s coverage.” *Id.* (quoting *Goland v. CIA*, 607 F.2d 339, 350 (D.C. Cir. 1978)).

² The relevant section of FOIA setting forth Exemption 3 was amended in 2009 to specify that statutes “enacted after the date of the enactment of the OPEN FOIA Act of 2009” must expressly reference that section in order to qualify as Exemption 3 statutes. *See* 5 U.S.C. § 552(b)(3)(B) (added by OPEN FOIA Act of 2009, Pub. L. No. 111-83, tit. V, § 564, 123 Stat. 2184 (2009)). The statute invoked by NSA was enacted well before the date of that amendment.

NSA invoked Section 6 of the National Security Agency Act of 1959, Pub. L. No. 86-36, 73 Stat. 63 (codified at 50 U.S.C. § 402 note), as the relevant statute within the meaning of Exemption 3. Section 6 provides, in pertinent part, that “nothing 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.” *Id.* Section 6 qualifies as a exempting statute under Exemption 3. *Founding Church of Scientology of Washington, D.C. v. NSA*, 610 F.2d 824, 828 (D.C. Cir. 1979); *see Wilner v. NSA*, 592 F.3d 60, 72 (2d Cir. 2009). Further, Section 6’s protection is “absolute”; the court is not to consider a requesting party’s need for the information. *Linder v. NSA*, 94 F.3d 693, 698 (D.C. Cir. 1996). Section 6 is intentionally broad: The D.C. Circuit has recognized that “[i]n light of the peculiar NSA security needs . . . Congress certainly had rational grounds to enact for the NSA a protective statute broader than the CIA’s.” *See Hayden v. NSA/CSS*, 608 F.2d 1381, 1390 (D.C. Cir. 1979). Importantly, therefore, a “specific showing of potential harm to national security . . . is irrelevant to the language of [Section 6]. Congress has already, in enacting the statute, decided that disclosure of NSA activities is potentially harmful.” *Id.*

Exemption 3 covers “not only the content of protected government records but also the fact of their existence or nonexistence, if that fact itself properly falls within the exemption.” *Larson*, 565 F.3d at 861. “The *Glomar* doctrine is well

settled as a proper response to a FOIA request because it is the only way in which an agency may assert that a particular FOIA statutory exemption covers the ‘existence or nonexistence of the requested records’ in a case in which a plaintiff seeks such records.” *Wilner*, 592 F.3d at 68 (quoting *Phillippi*, 546 F.2d at 1012). A *Glomar* response is appropriate when “to confirm or deny the existence of records . . . would cause harm cognizable under a FOIA exception.” *Gardels v. CIA*, 689 F.2d 1100, 1103 (D.C. Cir. 1982). Agencies are not required to submit a *Vaughn* index when invoking a *Glomar* response, because listing responsive documents on that index would cause the very harm the applicable exemption is intended to prevent. *Linder*, 94 F.3d at 697.

Courts in this Circuit have consistently upheld *Glomar* responses by NSA where, as here, confirming or denying the existence of records would disclose information protected by Section 6 of the National Security Agency Act, in contravention of FOIA Exemption 3. *See Larson*, 565 F.3d at 868-869; *People for the Am. Way Found. v. NSA/CSS*, 462 F. Supp. 2d 21, 29-30 (D.D.C. 2006); *see also Wilner*, 592 F.3d at 71-72, 75; *Roman v. NSA*, 2009 WL 303686, at *5-6 (E.D.N.Y. 2009). NSA therefore is not required to disclose records that pertain to “any function” of NSA or that would reveal “any information with respect to the activities” of the Agency, including when even confirming or denying the existence of such records would reveal that protected information.

B. NSA Properly Declined, Pursuant to Its Broad Statutory Authority, to Confirm or Deny the Existence of Records Responsive to EPIC's Request

The attached declaration demonstrates that NSA properly determined that acknowledging the existence or nonexistence of records responsive to EPIC's FOIA request would reveal protected information about NSA's functions or activities. As explained by Diane M. Janosek, Deputy Associate Director for Policy and Records, one of NSA's primary cryptologic missions is its Information Assurance mission, under which NSA is tasked with protecting government information systems and providing support to other agencies that protect the nation's critical infrastructure and key resources. Janosek Decl. ¶ 4. NSA focuses primarily on discovering vulnerabilities in those information systems, monitoring malicious activity, and security testing, in its effort to ward off "ever-growing threats to [U.S. government] information systems." *Id.* ¶¶ 4-5. Because the "government is largely dependent on commercial technology for its information systems," NSA may discover security vulnerabilities in those commercial technologies purchased by the government from the private sector. *Id.* ¶ 6. If such vulnerabilities in a commercial technology or malicious attacks directed at such programs pose a threat to U.S. government information systems, NSA may take action against the threat in any number of ways. *Id.* ¶¶ 6, 12.

EPIC's request sought information directly related to this core function of NSA—its Information Assurance mission—and to NSA activities in fulfillment of that function. The request began by discussing Google's announcement in early

2010 that hackers originating from China had initiated a cyber attack against its corporate infrastructure. *See* FOIA Request (Janosek Decl. Ex. A) at 1. It then cited media reports alleging that NSA had entered into a partnership with Google in connection with that incident. *Id.* at 1-2. Its requests sought records that would constitute evidence of that alleged partnership, both in connection with the hacking incident and with respect to certain Google applications and the kinds of security technology employed on those applications. *Id.* at 3.

But as Ms. Janosek's declaration explains, even confirming or denying the existence of records EPIC sought would reveal whether NSA, as part of its Information Assurance mission, determined that vulnerabilities associated with Google applications "could make U.S. government information systems susceptible to exploitation or attack by adversaries" and accordingly collaborated with Google to secure those vulnerabilities. *See* Janosek Decl. ¶¶ 13-14. The decision whether or not to enter into such a partnership certainly qualifies as one of NSA's "activities" and furthers its Information Assurance mission. *Cf. Hayden*, 608 F.2d at 1389-1390 (concluding that documents relating to NSA's signals intelligence mission, "one of the Agency's primary functions," fell within the scope of Section 6 and were therefore properly withheld under Exemption 3); *People for the Am. Way Found.*, 462 F. Supp. 2d at 29-30 (upholding NSA's *Glomar* response with respect to its signals intelligence function because even the admission that no information existed pertaining to a particular individual would reveal information about NSA

activities). Accordingly, the fact of the existence or nonexistence of records concerning that decision falls comfortably within the scope of protection offered by Section 6 of the National Security Agency Act.

This conclusion applies to all three of EPIC's requests, and to any record that would be responsive to each. As for the first request, NSA would only enter into "an agreement or similar basis for collaboration" with Google if it determined that any security vulnerability revealed by the January 2010 cyber attack or otherwise poses potential harm to U.S. government information systems. *See* Janosek Decl. ¶ 13. As for the second and third requests, NSA would only communicate with Google regarding Gmail or its use of encryption for cloud-based computing services such as Google Docs if NSA discovered a vulnerability in those commercial systems that posed a threat to U.S. government information systems. *See id.* To disclose whether any such records exist would reveal protected information about NSA's functions and activities, and NSA therefore acted properly in issuing the *Glomar* response to EPIC's request.³

³ As Ms. Janosek states, the confirmation or denial of the existence of even one of these responsive records would suffice to reveal protected information about NSA's functions and activities with respect to Google. Janosek Decl. ¶ 14. Accordingly, she correctly determined that there is no reasonably segregable portion of nonexempt responsive records that can be released. *Id.*; *see also Moore v. Bush*, 601 F. Supp. 2d 6, 16 (D.D.C. 2009) ("[S]egregability is not an issue. . . . [when] NSA could not confirm or deny whether it had any responsive documents.").

CONCLUSION

For the foregoing reasons, NSA respectfully requests that this Court grant summary judgment in its favor.

Dated: December 22, 2010

Respectfully submitted,

TONY WEST
Assistant Attorney General

RONALD C. MACHEN JR.
United States Attorney

ELIZABETH J. SHAPIRO
Deputy Branch Director

/s/ Judson O. Littleton
JUDSON O. LITTLETON
TX Bar No. 24065635
Trial Attorney
United States Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave. NW
Washington, DC 20530
Tel. (202) 305-8714
Fax (202) 616-8470
Judson.O.Littleton@usdoj.gov

Attorneys for Defendant

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing Motion for Summary Judgment was served on December 22, 2010, by electronic filing to

Marc Rotenberg, Esquire
John Verdi, Esquire
Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
Tel. (202) 483-1140

/s/ Judson O. Littleton
JUDSON O. LITTLETON

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

ELECTRONIC PRIVACY INFORMATION CENTER,)	
)	
Plaintiff,)	
)	
v.)	Civil Action No. 10-1533 (RJL)
)	
NATIONAL SECURITY AGENCY,)	
)	
Defendant.)	

**STATEMENT OF MATERIAL FACTS
AS TO WHICH THERE IS NO GENUINE ISSUE**

As required by LCvR 7.1(h) and in support of its Motion for Summary Judgment, defendant National Security Agency hereby makes the following statement of material facts as to which there is no genuine issue.

EPIC’s FOIA Request

1. By letter dated February 4, 2010, EPIC submitted a Freedom of Information Act request to NSA. Compl. ¶ 12; Janosek Decl. ¶ 7.
2. EPIC requested the following agency records:
 - a. “All records concerning an agreement or similar basis for collaboration, final or draft, between the NSA and Google regarding cyber security”;
 - b. “All records of communication between NSA and Google concerning Gmail, including but not limited to Google’s decision to fail to routinely encrypt Gmail messages prior to January 13, 2010”;

- c. “All records of communications regarding NSA’s role in Google’s decision regarding the failure to routinely deploy encryption for cloud-based computing service, such as Google Docs.”

Compl. ¶ 12; Janosek Decl. ¶ 7.

3. By letter dated March 10, 2010, NSA issued a response to EPIC’s request, stating that it “is authorized by statute to protect information concerning its functions and activities,” and that it therefore could “neither confirm nor deny whether the company has a relationship with the Agency related to the issues” EPIC described. Janosek Decl. Ex. B.
4. By letter dated May 7, 2010, EPIC appealed NSA’s decision to deny the FOIA request. Janosek Decl. Ex. C.
5. NSA placed EPIC’s appeal in its queue for processing, but had not acted on that appeal before the instant Complaint was filed. Janosek Decl. ¶ 9.

NSA’s *Glomar* Determination

6. One of NSA’s core missions is its Information Assurance mission, in which it is charged with safeguarding Department of Defense and other national-security information systems and providing support to other agencies that help protect other government information systems and the nation’s critical infrastructure and key resources. Janosek Decl. ¶ 4.
7. The U.S. government is largely dependent on commercial technologies for its information systems and often purchases such technologies and applications from private vendors. Janosek Decl. ¶ 6.

8. If NSA discovers a security vulnerability in any of the commercial technologies used by U.S. government agencies and determines that the vulnerability might pose a threat to U.S. government information systems, it may choose to take action to combat the threat. Janosek Decl. ¶¶ 6, 12.
9. Action taken by NSA to combat a security threat discovered in commercial applications used in U.S. government information systems is an activity taken by NSA in furtherance of its Information Assurance function. Janosek Decl. ¶¶ 13, 14.
10. Determining whether to take action in response to a particular vulnerability is an activity taken by NSA in furtherance of its Information Assurance function. Janosek Decl. ¶¶ 13, 14.
11. NSA acknowledgment of the existence or nonexistence of records evidencing a relationship between it and Google would require NSA to disclose information about its activities in relation to its core Information Assurance function. Janosek Decl. ¶¶ 13, 14.

Dated: December 22, 2010

Respectfully submitted,

TONY WEST
Assistant Attorney General

RONALD C. MACHEN JR.
United States Attorney

ELIZABETH J. SHAPIRO
Deputy Branch Director

/s/ Judson O. Littleton
JUDSON O. LITTLETON
TX Bar No. 24065635

Trial Attorney
United States Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave. NW
Washington, DC 20530
Tel. (202) 305-8714
Fax (202) 616-8470
Judson.O.Littleton@usdoj.gov

Attorneys for Defendant