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.	)	

DEFENDANT'S COMBINED REPLY AND OPPOSITION TO PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT

INTRODUCTION

Plaintiff EPIC seeks disclosure under FOIA of records of alleged communications between NSA and Google concerning certain Google technologies, including records related to an alleged cooperative research agreement between NSA and Google regarding cybersecurity. NSA has made clear that confirming or denying the existence of any such records would reveal information relating to its core functions and activities, and that information is protected from disclosure by 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). *See* Declaration of Diane M. Janosek, Deputy Associate Director for Policy and Records, NSA (Dkt. No. 9-1). NSA's response was appropriate and consistent with FOIA's requirements. *See Wolf v. CIA*, 473 F.3d 370, 374 (D.C. Cir. 2007) (explaining that a

Glomar response is "proper if the fact of the existence or nonexistence of agency records falls within a FOIA exemption").

Plaintiff's Opposition to Defendant's Motion for Summary Judgment and Cross-Motion for Summary Judgment reflects a fundamental misunderstanding of NSA's mission and the nature of a *Glomar* response. Further, it fails to appreciate the breadth of the authority Congress provided NSA to protect information about the agency's functions and activities. Because EPIC has therefore failed to create any dispute as to the lawfulness of NSA's response, NSA respectfully requests that the Court grant its motion for summary judgment and deny Plaintiff's cross-motion.

ARGUMENT

I. NSA Correctly Determined from the Face of EPIC's Request that a *Glomar* Response Was Appropriate

In its motion for summary judgment, NSA demonstrated that confirming or denying the existence of the records requested by EPIC would reveal information related to "any function" or "the activities" of NSA. Congress expressly provided NSA authority to protect such information from disclosure in Section 6 of the National Security Agency Act, see 50 U.S.C. § 402 note,[1] and Exemption 3 serves to ensure that that congressional judgment is not implicitly overridden by FOIA. *See Association of Retired R.R. Workers v. U.S. R.R. Retirement Bd.*, 830 F.2d 331, 336 (D.C. Cir. 1987) ("[T]he purpose of Exemption 3 [is] to assure that Congress, not the agency, makes the basic nondisclosure decision."); *Founding Church of Scientology*

[1] 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." 50 U.S.C. § 402 note.

of Washington, D.C. v. NSA, 610 F.2d 824, 828 (D.C. Cir. 1979) ("[Section 6] reflects . . . a congressional judgment that, in order to preserve national security, information elucidating the subjects specified ought to be safe from forced exposure. The basic policy choice was made by Congress, not entrusted to administrative discretion in the first instance."). Because NSA acted pursuant to clear statutory authority in issuing its *Glomar* response, that response was lawful and should be affirmed by this Court.

NSA refused to confirm or deny the existence of an alleged cooperative research agreement between NSA and Google, or of any communications between NSA and Google regarding Gmail or cloud-based computing services. That information undeniably relates to "any function of the National Security Agency," 50 U.S.C. § 402 note—indeed, it relates to one of NSA's primary functions. As explained in NSA's motion for summary judgment (at 10) and Ms. Janosek's declaration, one of NSA's primary cryptologic missions is its Information Assurance mission, under which it is charged with countering "ever-growing threats to [U.S. government] information systems." Janosek Decl. ¶¶ 4–6. Pursuant to that mission, NSA works to discover and repair security vulnerabilities in government information systems and monitors malicious activity with respect to those information systems. As Ms. Janosek explained, if NSA detects vulnerabilities in or malicious attacks on commercial technologies that could threaten the security of government information systems, it may take action to combat that threat. *See id.* ¶¶ 6, 12.

In the course of implementing its Information Assurance mission, NSA may choose to work with commercial partners to secure any discovered vulnerabilities. *See* Janosek Decl. ¶ 6. The decision whether to enter into such a relationship with a commercial partner depends in large part on NSA's assessment of a potential security threat. Consequently, the outcome of that decision could reveal much about NSA's security priorities and its estimation of vulnerabilities in government information systems—information that would certainly be valuable to our adversaries. *See id.* ¶ 13. Accordingly, confirming or denying the existence of records evidencing a partnership between NSA and a commercial entity like Google, particularly in response to a single cybersecurity incident or with respect to a certain commercial technology, would disclose "information with respect to [NSA's] activities" in furtherance of its Information Assurance mission. *See* 50 U.S.C. § 402 note.

For the most part, EPIC does not appear to seriously dispute that conclusion as a general matter. Instead, EPIC contends that NSA committed procedural errors in arriving at its decision to issue a *Glomar* response. First, EPIC asserts that NSA should have conducted a search for responsive records, and that the failure to do so "demonstrates that the agency lacks any factual foundation" for its response. *See* Plaintiff's Opp. at 4, 7. Further, EPIC contends that NSA's failure to conduct a search rendered NSA and this Court unable to determine whether any segregable portion of the requested documents should have been disclosed. *Id.* Both contentions

lack merit and demonstrate a misunderstanding of the purpose and consequence of the *Glomar* response in an Exemption 3 case like this one.

a. NSA had no need to conduct a search in response to EPIC's request.

When an agency issues a *Glomar* response, "the adequacy of a search is irrelevant . . . because the issue is whether the Agency has given sufficiently detailed and persuasive reasons for taking the position that it will neither confirm nor deny the existence of any responsive records." *Wheeler v. CIA*, 271 F. Supp. 2d 132, 141–42 (D.D.C. 2003) (affirming a *Glomar* response when the agency "did not identify whether or to what extent it had conducted a search"); *see Pipko v. CIA*, 312 F. Supp. 2d 669, 679–80 (D.N.J. 2004) (same); *Greenberg v. U.S. Dep't of Treasury*, 10 F. Supp. 2d 3, 24 (D.D.C. 1998). Indeed, particularly when a *Glomar* response is issued pursuant to Exemption 3, an agency may have no need to conduct a search at all to reach that determination. This is because when an agency invokes Exemption 3, "its 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." *Ass'n of Retired R.R. Workers*, 830 F.2d at 336 (quoting *Goland v. CIA*, 607 F.2d 339, 350 (D.C. Cir. 1978)).

It may often be apparent from the face of a request that the fact of the existence or nonexistence of any responsive records falls within the scope of a protective statute. That is certainly a likely scenario when the applicable statute is as broad as Section 6. "In light of . . . peculiar NSA security needs," the D.C. Circuit has

recognized that Congress purposefully enacted for NSA "a protective statute broader than the CIA's." *Hayden v. NSA/CSS*, 608 F.2d 1381, 1390 (D.C. Cir. 1979); *cf. Hunt v. CIA*, 981 F.2d 1116, 1120 (9th Cir. 1992) (noting that CIA's statutory authority to protect "intelligence sources and methods" is a "near-blanket FOIA exemption"). Conducting a search before refusing to disclose the results of that search would be a meaningless (and costly) exercise when it is apparent from the face of the request that the agency could not confirm or deny the existence of any responsive records due to its expansive statutory protective authority.

That is precisely the circumstance presented by this case. As explained above and in NSA's motion for summary judgment (at 10–12), it is apparent from the face of EPIC's request that to confirm or deny the existence of responsive records would disclose information protected by Section 6. Specifically, it might reveal whether NSA did or did not consider a particular cybersecurity incident or security settings in certain commercial technologies to potentially expose U.S. government information systems to an external threat. That threat assessment and ensuing action or inaction would go to the heart of a major NSA function, its Information Assurance mission. Janosek Decl. ¶¶ 13–14. That well-supported determination alone fulfills NSA's obligation with respect to EPIC's request. *See Hayden*, 608 F.2d at 1390 ("[T]he Agency stated in its affidavit[] that all requested documents concerned a specific NSA activity . . . . This is all that is necessary for the Agency to meet its burden under Public Law No. 86-36 and Exemption 3.").

b. It is apparent from the face of EPIC's request that there is no segregable portion of the requested information that can be disclosed by NSA.

EPIC also contends that NSA's decision not to conduct a search precluded it from making a proper segregability analysis and asserts, relying in large part on language from cases that did not involve a *Glomar* response, that that fact precludes this Court from upholding NSA's response in this case. Again, EPIC's argument fails.

As an initial matter, EPIC wrongly claims that "NSA failed to perform any segregability analysis." Plaintiff's Opp. at 7. Ms. Janosek expressly stated that "acknowledgment of the existence or nonexistence of even one record or communication satisfying Plaintiff's request would improperly disclose a function or activity of NSA and could have negative effects on NSA's Information Assurance mission." Janosek Decl. ¶ 14. Accordingly, she concluded that "there is no reasonably segregable, nonexempt portion of the requested records that can be released." *Id.*; *see also* NSA Motion for Summary Judgment at 12 n.3. As this conclusion was evident from the face of EPIC's request, NSA was not required to conduct a search in order to make that determination.

EPIC may instead have been referring to its contention that NSA was required to "'correlate the theories of exemptions with the particular textual segments which it desired exempted.'" Plaintiff's Opp. at 6, 9 (quoting *Schiller v. NLRB*, 964 F.2d 1205, 1209–10 (D.C. Cir. 1992)). This argument, relying on a case in which a *Glomar* response was not issued, once again misconstrues the nature of the *Glomar* response. *Schiller* was discussing the requirements of the document commonly

known as a *Vaughn* index, which agencies use to link specific exemptions to particular textual segments of withheld documents. *See* 964 F.2d at 1209–10. But it is well-established that a *Vaughn* index is not required when the agency issues a *Glomar* response, because that index would reveal the very information the agency seeks to protect—the fact of the existence or nonexistence of responsive records. *See Wolf*, 473 F.3d at 374 n.4; *Linder v. NSA*, 94 F.3d 693, 697 (D.C. Cir. 1996); *Phillippi v. CIA*, 546 F.2d 1009, 1013 n.7 (D.C. Cir. 1976). Relatedly, it is for the same reason that, in a case that EPIC itself cites in this section of its brief, Plaintiff's Opp. at 6, the court concluded that "segregability [was] not an issue" in the case because "NSA could not confirm or deny whether it had any responsive documents." *Moore v. Bush*, 601 F. Supp. 2d 6, 16 (D.D.C. 2009).

Accordingly, NSA correctly determined from the face of EPIC's request that confirming or denying the existence of even a single responsive record would reveal information relating to NSA functions and activities. Even confirming that one record exists that would evidence a relationship between NSA and Google might reveal whether NSA considered a particular cybersecurity incident to pose a security threat to U.S. government information systems. And denials of the existence of some records may give rise to the opposite inference with respect to other records in this case or in other cases in which the *Glomar* response is invoked by NSA. *See People for the Am. Way Found. v. NSA/CSS*, 462 F. Supp. 2d 21, 29–30 (D.D.C. 2006); *cf. Berman v. CIA*, 501 F.3d 1136, 1143 (9th Cir. 2007) (recognizing the "common sense premise that the impact of disclosing protected documents must

be evaluated . . . with regard to what secrets the document could divulge when viewed in light of other information available to interested observers").

EPIC's speculation that NSA might possess records that pertain only to Google's functions or activities, but not NSA's, similarly does not give rise to an obligation to search in this case. EPIC's understanding of NSA's mission is too narrow. Even if EPIC were correct that certain records or portions of records existed that revealed only information about Google and nothing about NSA, those records would still constitute evidence of a *relationship* between Google and NSA formed in response to a potential vulnerability exposed by a particular cybersecurity incident or commercial technology. As NSA has explained, it is the relationship, not just the content or number of alleged records, that would reveal protected information about NSA's implementation of its Information Assurance mission. *See* NSA Motion at 11–12.

Further, as Ms. Janosek explained, NSA takes a "pro-active defense approach" in its protection of U.S. government information systems. Janosek Decl. ¶ 5. "This approach is dependent on information from a number of intelligence and open sources in order to have early awareness of potential malicious activity or vulnerabilities." *Id.* The specific types and identities of sources that NSA may choose to rely on are certainly a key aspect of its mission, and any information shedding light on such sources is protected by Section 6. For instance, NSA may gather information about potential security threats from self-reporting of private entities. The decision whether or not to do so is a protected activity under NSA's

Information Assurance mission. Moreover, if NSA did choose to encourage and rely on self-reports of cybersecurity vulnerabilities from private entities, but those private entities knew that any such self-reports could be made public through a FOIA request, they might be hesitant to reach out to NSA, thereby hindering NSA's mission. These are precisely the considerations Congress authorized NSA to take into account when it gave the agency broad power to protect information relating to its "function[s]" and "activities," 50 U.S.C. § 402 note, and NSA acted properly in making that determination in this case.

II. The NSA Declaration Sufficiently Describes the Justifications for Its *Glomar* Response

EPIC mounts several other challenges to the NSA declaration in this case. *See* Plaintiff's Opp. at 9-14. None of these scattered contentions has merit. Ms. Janosek "describe[s] the justifications for nondisclosure with reasonably specific detail" and "demonstrate[s] that the information withheld logically falls within the claimed exemption," and EPIC has made no showing of "contrary evidence in the record" or "agency bad faith." *See Larson v. Dep't of State*, 565 F.3d 857, 862 (D.C. Cir. 2009). Accordingly, summary judgment is warranted in NSA's favor on the basis of the Janosek Declaration alone. *See id.*

To underscore the flaws in EPIC's arguments, it is worth reemphasizing the only issue facing the Court in this case. Because it is undisputed that Section 6 of the National Security Agency Act qualifies as an Exemption 3 statute, the only question here is whether, as a matter of law, the fact of the existence or nonexistence of responsive records "falls within the statute"—specifically, that it "relates to . . . any

function or activities of the agency." *Larson*, 565 F.3d at 868. And as explained above, Section 6 has an intentionally wide scope. Accordingly, any suggestion by EPIC that NSA was required to demonstrate harm to national security, *see* Plaintiff's Opp. at 13, is wrong. "A specific showing of potential harm to national security . . . is irrelevant to the language of Public Law No. 86-36. Congress has already, in enacting the statute, decided that disclosure of NSA activities is potentially harmful." *Hayden*, 608 F.2d at 1390.

Further, the determination whether the requested information falls within the scope of Section 6 is not affected by EPIC's assertion that "the relationship between the NSA and Google has already been 'well publicized.'" Plaintiff's Opp. at 9–10. NSA has never acknowledged such a relationship, and the "news media" is certainly incapable of waiving NSA's statutory authority to protect information related to its functions and activities. Only official acknowledgment from "the agency from which the information is being sought" can waive an agency's protective power over records sought under FOIA, *see Frugone v. CIA*, 169 F.3d 772, 774 (D.C. Cir. 1999); such waiver "cannot be based on mere public speculation, no matter how widespread." *Wolf*, 473 F.3d at 378; *see also ACLU v. DOD*, 628 F.3d 612, 621 (D.C. Cir. 2011) ("[W]e are hard pressed to understand the . . . contention that the release of a nongovernment document by a nonofficial source can constitute a disclosure affecting the applicability of the FOIA exemptions."); *Alfred A. Knopf, Inc. v. Colby*, 509 F.2d 1362, 1370 (4th Cir. 1975) ("It is one thing for a reporter or author to speculate or guess that a thing may be so or even, quoting undisclosed sources, to

say that it is so; it is quite another thing for one in a position to know of it officially to say that it is so."). NSA has steadfastly refused to confirm or deny the existence of any relationship with Google, and news media reports do not affect its statutory authority to maintain that position.

EPIC's remaining contentions that the Janosek Declaration is too vague or conclusory to support summary judgment, *see* Plaintiff's Opp. at 10–12, are similarly unavailing.[2] Ms. Janosek clearly explains the justification for the *Glomar* response in as much detail as possible without disclosing the protected information. After explaining the focus and goals of NSA's Information Assurance mission, Ms. Janosek demonstrates why confirming or denying the existence of records evidencing a relationship between NSA and Google regarding cybersecurity would reveal information relating to NSA activities in furtherance of that mission. Because that explanation is "logical" and "plausible," it is legally sufficient to dispose of this case. *See Wolf*, 473 F.3d at 375.

CONCLUSION

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

---

[2] EPIC appears to suggest that, in explaining why the protected information falls within the scope of a protective statute, the agency should not use the words of the statute too often. *See* Plaintiff's Opp. at 10-11. This is a somewhat puzzling assertion, particularly when the applicable statute uses such common terms with ordinary meanings as "function" and "activities." To be sure, a declaration may be insufficient if it "*merely* recit[es] statutory standards," *see People for the Am. Way*, 462 F. Supp. 2d at 28 (emphasis added), but the Janosek Declaration certainly does more than that—it explains why confirming or denying the existence of records EPIC seeks would reveal NSA activities in furtherance of its Information Assurance mission. Keying that explanation to the words of the protective statute is certainly the appropriate way to demonstrate that the requested information falls within that statute's scope.

Dated: February 18, 2011

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)
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 Combined Reply and Opposition to Plaintiff's Motion for Summary Judgment was served on February 18, 2011, 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.	)	

RESPONSE TO PLAINTIFF'S STATEMENT OF MATERIAL FACTS NOT IN GENUINE DISPUTE

As required by LCvR 7(h) and in support of its Motion for Summary Judgment, defendant NSA hereby responds to plaintiff EPIC's statement of material facts not in genuine dispute.

NSA does not dispute the facts submitted in EPIC's Statement of Material Facts Not in Genuine Dispute. NSA asserts, however, that none of those facts are significant to the resolution of the motions for summary judgment currently pending in this action.

Dated: February 18, 2011

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)
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