

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

)	
ELECTRONIC PRIVACY)	
INFORMATION CENTER)	
)	
Plaintiff,)	
)	
v.)	No. 1:10-cv-01533-RJL
)	
NATIONAL SECURITY AGENCY)	
)	
Defendant.)	
)	

PLAINTIFF'S OPPOSITION TO DEFENDANT'S MOTION FOR SUMMARY JUDGMENT, CROSS-MOTION FOR SUMMARY JUDGMENT, AND REQUEST FOR ORAL HEARING

Plaintiff the Electronic Privacy Information Center opposes Defendant's December 22, 2010 Motion for Summary Judgment, and cross-moves for summary judgment.

A statement of genuine issues regarding Defendant's statement of material facts, Plaintiff's statement of material facts not in dispute, a memorandum of points and authorities, and a proposed Order are filed herewith.

Pursuant to LCvR 7(f), Plaintiff requests an oral hearing on the parties' cross-motions.

Respectfully submitted,
/s/ John Verdi

 MARC ROTENBERG
 JOHN VERDI
 Electronic Privacy Information Center
 1718 Connecticut Ave. NW
 Suite 200
 Washington, DC 20009
 (202) 483-1140
Counsel for Plaintiff

Dated: January 28, 2011

CERTIFICATE OF SERVICE

I hereby certify that on the 28th day of January 2011, I served the foregoing PLAINTIFF'S OPPOSITION TO DEFENDANT'S MOTION FOR SUMMARY JUDGMENT, CROSS-MOTION FOR SUMMARY JUDGMENT, AND REQUEST FOR ORAL HEARING, including all exhibits and attachments, by electronic case filing upon:

JUDSON O. LITTLETON
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

/s/ John Verdi

John Verdi
Counsel for Plaintiff

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

ELECTRONIC PRIVACY INFORMATION CENTER)	
)	
Plaintiff,)	
)	
v.)	No. 1:10-cv-01533-RJL
)	
NATIONAL SECURITY AGENCY)	
)	
Defendant.)	

**PLAINTIFF’S MEMORANDUM OF POINTS AND AUTHORITIES IN OPPOSITION
TO DEFENDANT’S MOTION FOR SUMMARY JUDGMENT AND IN SUPPORT OF
PLAINTIFF’S CROSS-MOTION FOR SUMMARY JUDGMENT**

Plaintiff the Electronic Privacy Information Center (“EPIC”) opposes Defendant U.S. National Security Agency’s (the “NSA’s”) December 22, 2010 Motion for Summary Judgment, and cross-moves for summary judgment in favor of EPIC. Specifically, EPIC challenges the TSA’s “*Glomar* response” to EPIC’s Freedom of Information Act (“FOIA”) request seeking records concerning the agency’s communications with Google, Inc. regarding cybersecurity. The NSA’s improperly issued its *Glomar* response without performing any search for responsive records. Further, the sole affidavit supporting the agency’s response does not provide a sufficient factual basis.

The records requested by EPIC concern the privacy of millions of electronic mail users in the United States. These Internet users’ privacy interests may be adversely affected by the policies pursued by Google and the federal government.

FACTUAL BACKGROUND

On January 12, 2010, Google reported a major cyber attack from “highly sophisticated” hackers in China. On February 4, 2010, the Washington Post and the Wall Street Journal reported that Google contacted the NSA regarding the firm’s security practices, immediately following the attack. The Wall Street Journal reported that the NSA’s general counsel drafted a “cooperative research and development agreement” within twenty-four hours of Google’s January 12, 2010 announcement, authorizing the agency to “examine some of the data related to the intrusion into Google's systems.”

On January 13, 2010, Google changed a key setting, encrypting by default all subsequent traffic to and from its electronic mail servers. Prior to January 13, 2010, Google chose not to encrypt Gmail, the firm's electronic mail service, by default, despite two compelling warnings about the risk in 2009.

Google failed to provide Gmail users with this basic security functionality despite warnings from experts that the company’s failure to encrypt login transactions imperiled users’ data and exposed users to substantial security risks. On March 17, 2009, prior to the cyber attack in January 2010, Petitioner EPIC filed a Complaint before the Federal Trade Commission, urging the Commission to investigate Google’s reluctance to encrypt cloud-based user data (including Gmail data) by default. Following the EPIC complaint to the Federal Trade Commission, 37 experts in privacy and security wrote Google to highlight the “very real risk of data theft and snooping” posed by Google’s failure to employ encryption.

On February 4, 2010, EPIC filed a FOIA request with the NSA. EPIC’s request seeks:

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.

The NSA failed to disclose records. On March 10, 2010, the NSA denied EPIC's FOIA Request and issued a "*Glomar* response," writing to EPIC that the agency would neither confirm nor deny the existence of any agreement with Google concerning cybersecurity.

On May 7, 2010, EPIC transmitted a written administrative appeal to the NSA ("EPIC's Administrative Appeal") appealing the NSA's failure to disclose records responsive to EPIC's FOIA Request. The agency failed to present factual evidence that the requested documents fall within Section 6. Furthermore, EPIC noted that simple redactions can sufficiently conceal any protected information that does appear on original copies of the requested documents.

The NSA failed to respond to EPIC's Administrative Appeal within the deadlines set forth in the FOIA. EPIC filed this lawsuit, challenging the agency's *Glomar* response and failure to comply with statutory deadlines.

STANDARD OF REVIEW

Summary judgment is appropriate when there is no genuine issue as to the material facts, and the moving party demonstrates it is entitled to judgment as a matter of law. Fed. R. Civ. P. 56; *Diamond v. Atwood*, 43 F.3d 1538, 1540 (D.C. Cir. 1995). FOIA lawsuits are typically resolved on cross-motions for summary judgment. *Reliant Energy Power Generation v. FERC*, 520 F. Supp. 2d 194, 200 (D.D.C. 2007). A court reviews agency handling of a FOIA request *de novo*. 5 U.S.C. § 552(a)(4)(B); *Miller v. Casey*, 730 F.2d 773, 776 (D.C. Cir. 1984).

ARGUMENT

Although the D.C. Circuit has upheld the propriety of *Glomar* responses in some cases, the NSA's invocation of *Glomar* in this matter is unlawful.

The agency failed to conduct any search for records responsive to EPIC's FOIA request. This failure demonstrates that the agency lacks any factual foundation for its assertion that the relevant records are subject to FOIA Exemption 3 or appropriately subject to a *Glomar* response. Further, the failure deprives this Court of the ability to perform a segregability analysis. The D.C. Circuit requires that a District Court perform such an analysis before upholding an agency's withholding under FOIA.

The NSA supports its use of a *Glomar* response with a single affidavit, attested to by Diane M. Janosek, Deputy Associate Director for Policy and Records at the NSA (the "Janosek Affidavit"). The Janosek Affidavit is insufficient because it is vague and conclusory. In large part, it merely restates statutory and caselaw authority – such restatement is *per se* insufficient to support a FOIA withholding under the law of this Circuit.

I. The NSA Failed to Perform the Required Search and Segregability Analysis, and Some Documents Requested by EPIC are Not Exempt Under Exemption 3 Because they Relate to Google's Activities, Not the Agency's.

The U.S. Supreme Court "repeatedly has stressed the fundamental principle of public access to Government documents that animates the FOIA." *John Doe Agency v. John Doe Corp.*, 493 U.S. 146, 151-152 (1989). "The basic purpose of FOIA is to ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed." *NLRB v. Robbins Tire & Rubber Co.*, 437 U.S. 214, 242 (1978). The FOIA's "basic purpose reflect[s] a general philosophy of full agency disclosure unless information is exempted under clearly delineated statutory language." *Dept. of the Air*

Force v. Rose, 425 U.S. 352, 360-361 (1976), quoting S. Rep. No. 813, 89th Cong., 1st Sess., 3 (1965).

The FOIA includes exemptions from disclosure, “[b]ut these limited exemptions do not obscure the basic policy that disclosure, not secrecy, is the dominant objective of the Act.” *Rose*, 425 U.S. at 361. Therefore FOIA exemptions “must be narrowly construed.” *Id.* Furthermore, “the burden is on the agency to sustain its action.” 5 U.S.C. § 552(a)(4)(B); *Wolf v. C.I.A.*, 473 F.3d 370, 374 (D.C. Cir. 2007); *see also EPIC v. Dept. of Homeland Security*, 384 F. Supp. 2d 100, 106 (D.D.C. 2005).

An agency “may refuse to confirm or deny the existence of records where to answer the FOIA inquiry would cause harm cognizable under an FOIA exception.” *Gardels v. CIA*, 689 F.2d 1100, 1103 (D.C.Cir.1982); *see also Miller v. Casey*, 730 F.2d 773, 776-77 (D.C.Cir.1984); *Phillippi v. CIA*, 546 F.2d 1009, 1012 (D.C.Cir.1976). “Such an agency response is known as a *Glomar* response and is proper if the fact of the existence or nonexistence of agency records falls within a FOIA exemption.” *Wolf*, 473 F.3d at 374 (internal citations omitted).

“In determining whether the existence of agency records *vel non* fits a FOIA exemption, courts apply the general exemption review standards established in non-*Glomar* cases.” *Wolf v. C.I.A.*, 473 at 374; *Gardels v. C. I. A.*, 689 F.2d 1100, 1103-05 (D.C. Cir. 1982). Further, in cases challenging an agency’s *Glomar* response, the court should “attempt to create as complete a public record as is possible” and “the agency's arguments should then be subject to testing by [plaintiff], who should be allowed to seek appropriate discovery when necessary.” *Phillippi v. Central Intelligence Agency*, 546 F.2d 1009, 1013 (D.C. Cir. 1976).

Even if portions of agency records are exempt from disclosure under FOIA, the agency must segregate and disclose the non-exempt information. 5 U.S.C. § 552(b) (“Any reasonably

segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt under this subsection.”); *Mead Data Cent., Inc. v. United States Dep't of Air Force*, 566 F.2d 242, 260 (D.C.Cir.1977) (“Non-exempt portions of a document must be disclosed unless they are inextricably intertwined with exempt portions.”). An agency must “correlate the theories of exemptions with the particular textual segments which it desired exempted.” *Schiller v. NLRB*, 964 F.2d 1205, 1209-10 (D.C.Cir.1992) (reversing a grant of summary judgment to the government because the NLRB had failed to perform segregability analysis) “A district court clearly errs when it approves the government's withholding of information under the FOIA without making an express finding on segregability.” *PHE, Inc. v. Dep't of Justice*, 983 F.2d 248, 252 (D.C. Cir. 1993).

A segregability analysis is predicated on the agency performing an adequate search and identifying responsive documents – even in a case involving a *Glomar* response. Thus, before an agency “can obtain summary judgment in a FOIA case, [it] must show, viewing the facts in the light most favorable to the requester, that ... [it] has conducted a search reasonably calculated to uncover all relevant documents. *Moore v. Bush*, 601 F.Supp.2d 6, 8 (D.D.C. 2009), quoting *Steinberg v. Dep't of Justice*, 23 F.3d 548, 551 (D.C.Cir. 1994); see also *Founding Church of Scientology of Washington, D.C., Inc. v. NSA*, 610 F.2d 824 (D.C. Cir. 1979) (holding “an agency is not required to reorganize its files in response to a demand for information, but it does have a firm statutory duty to make reasonable efforts to satisfy it.” (internal citations omitted)); *EPIC v. DOJ*, 511 F.Supp.2d 56, 73-74 (D.D.C. 2007) (finding “the NSA declarations leave the court with no way to assess the appropriateness of the withholding decision, ... in particular ... whether the documents are protected by the claimed statutes” and ordering additional action by the agency).

The NSA bases its *Glomar* response in this case on FOIA Exemption 3. Exemption 3 permits an agency to withhold responsive records “specifically exempted from disclosure by statute,” if the statute

(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 criteria for withholding or refers to particular types of matters to be withheld.

5 U.S.C. § 552(b)(3).

The NSA relies on Section 6 of the National Security Agency Act of 1959, 50 U.S.C. § 402 note (the “NSA Act”), as the statute that allegedly justifies the agency’s Exemption 3 claim. NSA Mot. at 10. Section 6 states “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.

The NSA asserts Exemption 3 despite the fact that the agency failed to perform any search for responsive records, failed to identify a single record responsive to EPIC’s FOIA request, and therefore was wholly unable to determine whether the requested records would disclose “the organization . . . function . . . [or activities] of the National Security Agency.” 50 U.S.C. § 402 note. The NSA failed to perform any segregability analysis – a direct violation of this Circuit’s application of the FOIA.

The Janosek Affidavit states that “NSA did not conduct a search for responsive records” Janosek Aff. at ¶10. The agency alleges that “revealing the outcome of [a] search would reveal the very information that is exempted from disclosure under FOIA.” *Id.* The agency blithely, and incorrectly, assumes that EPIC’s FOIA request only seeks records concerning the NSA’s functions or activities. However, EPIC’s FOIA request seeks a variety of records. A search might reveal that some requested records relate to the NSA’s functions or activities. But it is virtually

certain that a search would reveal other records (or portions of records) that relate only to Google's corporate activities, but do not reveal information about NSA functions or activities.

For example, part 2 of EPIC's FOIA request seeks "[a]ll 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." Such records might include emails, letters, voicemails, or other communications from Google to the NSA concerning Gmail. And the content of such communications likely reveals much about Google, but little, if anything, about the NSA's functions and activities. Such records must be disclosed to EPIC under the FOIA. It is possible that portions of the communications reveal information about NSA activities, while other portions do not. Perhaps the non-exempt portions could be reasonably segregated from the exempt portions. Perhaps not. As The D.C. Circuit Court has observed, "the parties and the court, if sufficiently informed, may discern a means of liberating withheld documents without compromising the agency's legitimate interests." *Scientology*, 610 F.2d at 833. However, because the agency failed to perform any search, the parties and the Court are left to speculate as to what such records might contain.

The NSA's procedures in this case are the antithesis of the creation of "as complete a public record as is possible" required by *Phillippi*. *Phillippi*, 546 F.2d at 1013. Moreover, the agency's failure to search prevents "the agency's arguments" from being "subject to testing by [plaintiff], who should be allowed to seek appropriate discovery when necessary." *Id.* The agency cannot plausibly conclude, without reviewing a single word of a single record, that all documents requested by EPIC are properly exempt under Exemption 3. And the agency's *Glomar* response cannot be sustained when the agency's Exemption claim crumbles. A *Glomar* response is only proper if "the fact of the existence or nonexistence of agency records falls

within a FOIA exemption,” and is improper if the underlying FOIA Exemption claim fails. *Wolf*, 473 F.3d at 374 (internal citations omitted).

The NSA’s failure to search for responsive records prevents the agency from “correlat[ing] the theories of exemptions with the particular textual segments which it desire[s] exempted” – a correlation required by the D.C. Circuit Court. *Schiller* 964 F.2d at 1209-10. Further, the agency’s failure to search prevents this Court from “making an express finding on segregability,” a finding required by the D.C. Circuit. *PHE, Inc.*, 983 F.2d at 252.

II. The NSA Affidavit is Insufficient to Support the Agency's *Glomar* Response

“The Court may award summary judgment on the information provided in affidavits or declarations when they describe ‘the justifications for nondisclosure with reasonably specific detail, demonstrate that the information withheld logically falls within the claimed exemptions, and are not controverted by either contrary evidence in the record nor by evidence of agency bad faith.’” *People for the American Way Foundation v. NSA*, 462 F.Supp. 2d 21, 27 (D.D.C. 2006), quoting *Military Audit Project v. Casey*, 656 F.2d 724, 738 (D.C.Cir. 1981). “The burden is on the agency to sustain its action.” *Scientology*, 610 F.2d 824.

As discussed in Section I *supra*, The NSA relies on Section 6 of the NSA Act to support its *Glomar* response, noting that Section 6 bars disclosure of information concerning the “activities” or “functions” of the agency. 50 U.S.C. § 402 note. However, The D.C. Circuit Court has cautioned that “a term so elastic as ‘activities’ should be construed with sensitivity to the ‘hazard(s) that Congress foresaw’ [and] courts must be particularly careful when scrutinizing claims of exemptions based on such expansive terms. *Scientology*, 610 F.2d at 829. In addition, as EPIC has already emphasized in its FOIA request, the relationship between the NSA and Google has already been “well publicized.” *See Janosek Decl. Ex. A* at 2-4. When adjudicating

FOIA requests for information that has been widely disseminated in the news media, this court has recognized that “suppression of information of that sort would frustrate the pressing policies of the [FOIA] without even arguably advancing countervailing considerations.” *Scientology*, 610 F.2d at 831-2; *see also Janosek Decl. Ex. A* at 1-3.

The Janosek Affidavit fails to provide “sufficient detail to enable an informed determination as to whether disclosure ... would illuminate agency activities of which the public was not already aware.” *Scientology*, 610 F.2d at 826. The D.C. Circuit requires that affidavits supporting a *Glomar* response contain language that is more than “conclusory, merely reciting statutory standards, or ... too vague or sweeping.” *People for the American Way Foundation* 462 F.Supp. 2d at 28, quoting *King v. Dep’t of Justice*, 830 F.2d 210, 219 (D.C. Cir. 1987). Yet the Janosek Affidavit contains just this sort of conclusory, vague language.

The Janosek Affidavit “merely recite[s] statutory standards,” but fails to state the agency’s factual basis for its response in the required level of detail. *See Larson v. Department of State*, 565 F.3d 857, 868 (D.C. Cir. 2009). Section 6 of the NSA Act provides that “nothing in this Act or any other law ... shall be construed to require the disclosure of ... any function of the National Security Agency, or any information with respect to the activities thereof ...” 50 U.S.C. § 402 note. The Janosek Affidavit is seven pages long. Five pages are spent detailing the procedural history of this case and the origin and mission of the NSA. Neither the procedural recitation nor the general statements concerning the agency’s history are sufficiently specific to support the NSA’s *Glomar* response. The balance of the Janosek affidavit reiterates the Section 6 statutory standard no fewer than seven times:

1. “Such a positive or negative response would reveal a core function and activity of the NSA and is therefore protected from release by statute...” *Janosek Aff.* at ¶ 2.

2. “Such a response would reveal information about NSA’s functions and activities, which is protected from release by Exemption 3 statute, specifically Section 6 of the National Security Agency Act of 1959...” *Janosek Aff.* at ¶ 8.
3. “NSA provides such a *Glomar* response when to confirm or deny the existence of requested records would reveal a core function or activity of NSA – information expressly exempted from disclosure by statute.” *Janosek Aff.* at ¶ 10.
4. “NSA’s *Glomar* response in this case was proper because any positive or negative response to Plaintiff’s FOIA request would reveal a core function or activity of NSA.” *Janosek Aff.* at ¶ 10.
5. “To confirm or deny the existence of any such records would be to reveal whether NSA, in fulfilling one of its key missions, determined that vulnerabilities or cybersecurity issues pertaining to Google or certain of its commercial technologies could make the U.S. government information systems susceptible to exploitation or attack by adversaries and, if so, whether NS collaborated with Google to mitigate them.” *Janosek Aff.* at ¶ 13.
6. “Whether or not NSA has a relationship with Google or any other commercial entity in general or pertaining to a specific cybersecurity incident directly relates to one of the Agency’s core functions and activities.” *Janosek Aff.* at ¶ 14.
7. “[A]cknowledgment of the existence 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 Aff.* at ¶ 14.

Additional portions of the balance of the Janosek Affidavit merely recite language from caselaw. These recitations, like the seven restatements of statutory authority, are insufficient to support the agency’s *Glomar* response. Worse, these quotes lack the requisite level of specificity that the court typically requires of a satisfactory *Glomar* affidavit.

The court has found that sufficient affidavits (filed in other cases) assert that the “disclosure [of any information] would reveal information integrally related to [specific] NSA activity.” *Hayden v. NSA*, 608 F.2d 1381, 1390 (D.C. Cir. 1979). “Integral information” includes the identity of foreign electromagnetic channels monitored by the NSA (*See Hayden* 608 F.2d at 1383; *Iglesias v. CIA*, 525 F.Supp. 547, 554 (D.D.C. 1981)), classified CIA intelligence cables (*Larson* 565 F.3d at 863), and information related to the Terrorist Surveillance Program (TSP)

(*People for the American Way Foundation*, 462 F.Supp. 2d at 24). In this case, the Janosek Affidavit contends “acknowledgment by NSA of a relationship or agreement with Google related to a specific cybersecurity incident would reveal whether or not NSA considered the alleged attack to be of consequence for critical U.S. government information systems.” *Janosek Aff.* at ¶ 13. A “consideration” of the NSA does not rise to the level of importance that the court has previously accepted as sufficient, let alone a consideration related to a past occurrence.

The Janosek Affidavit also asserts that “in addition to revealing information about NSA functions and activities, such information falling in either category could alert our adversaries to NSA priorities, threat assessments, or countermeasures that may or may not be employed against future attacks.” *Janosek Aff.* at ¶ 13. Here the affidavit adopts language from a recent case before this court. *People for the American Way Foundation*, 462 F.Supp. 2d at 29 (stating that disclosure “would reveal information about NSA’s success or lack of success in implementing the TSP,” as well as “information about the U.S. intelligence community’s capabilities, priorities, and activities.”). However, in *People for the American Way*, the existence of the information the NSA sought to withhold, namely “briefing slides” that “detail[ed] information related to the number of individuals subject to surveillance, contain[ed] the identity of some individuals, and contain[ed] information related to the number of communications intercepted under the TSP,” had been identified and acknowledged by the Agency. *People for the American Way Foundation*, 462 F.Supp. 2d at 29. The Agency’s invocation of a *Glomar* response in the instant case prevents any independent analysis of the NSA’s broad assertion that any data related to EPIC’s FOIA request would “alert adversaries” to “priorities, threat assessments, or countermeasures.” *Janosek Aff.* at ¶ 13.

Notably, the Janosek Affidavit never claims that the information sought by EPIC's FOIA request would impact national security. Instead, the affidavit's sole assertion is that "whether or not NSA has a relationship with Google or any other commercial entity in general or pertaining to a specific cybersecurity incident directly relates to one of the Agency's core functions and activities: specifically, its Information Assurance mission, which entails assisting in the protection of U.S. government information systems." *Janosek Aff.* at ¶ 14. In support, the Affidavit lists a number of alleged justifications to support the NSA's response:

1. "To confirm or deny the existence of any such records would be to reveal whether NSA, in fulfilling one of its key missions, determined that vulnerabilities or cybersecurity issues pertaining to Google or certain of its commercial technologies could make U.S. government information systems susceptible to exploitation or attack by adversaries and, if so, whether NSA collaborated with Google to mitigate them." *Janosek Aff.* at ¶ 13.
2. "[A]ny acknowledgement by NSA of the existence or nonexistence of a relationship or agreement with Google related to a specific cybersecurity incident would reveal whether or not NSA considered the alleged attack to be of consequence for critical U.S. government information systems." *Janosek Aff.* at ¶ 13.
3. "[S]uch information falling in either category could alert our adversaries to NSA priorities, threat assessments, or countermeasures that may or may not be employed against future attacks." *Janosek Aff.* at ¶ 13.

The NSA charges that "because such information systems are necessarily dependent on commercial information technology, NSA's mission includes assessing purported malicious activity or security vulnerabilities in such commercial technologies and determining whether they present a serious threat to U.S. government information systems and, if so, how to combat that threat." *Janosek Aff.* at ¶ 12. The affidavit does not state how the confirmation or denial of the existence of such records could pose the threats listed. Nor does the Affidavit acknowledge how records concerning Google's corporate policies would reveal the NSA's activities or functions. As discussed in Section I *supra*, EPIC's FOIA request seeks such records concerning

Google, but the NSA failed to perform any search for the documents. Each of the justifications provided by the Janosek Affidavit are facially conclusory and find no support on the record.

CONCLUSION

As discussed above, Defendant's Motion for Summary Judgment should be denied, and the Court should order the NSA to perform a lawful search and disclose all responsive records. A proposed Order is attached.

Respectfully submitted,

/s/ John Verdi

MARC ROTENBERG
JOHN VERDI
Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
Counsel for Plaintiff

Dated: January 28, 2011

CERTIFICATE OF SERVICE

I hereby certify that on the 28th day of January 2011, I served the foregoing PLAINTIFF'S MEMORANDUM OF POINTS AND AUTHORITIES IN OPPOSITION TO DEFENDANT'S MOTION FOR SUMMARY JUDGMENT AND IN SUPPORT OF PLAINTIFF'S CROSS-MOTION FOR SUMMARY JUDGMENT, including all exhibits and attachments, by electronic case filing upon:

JUDSON O. LITTLETON
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

/s/ John Verdi

John Verdi
Counsel for Plaintiff

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

ELECTRONIC PRIVACY INFORMATION CENTER)	
)	
Plaintiff,)	
)	
v.)	No. 1:10-cv-01533-RJL
)	
NATIONAL SECURITY AGENCY)	
)	
Defendant.)	

**PLAINTIFF’S STATEMENT OF MATERIAL FACTS NOT IN GENUINE
DISPUTE**

In accordance with LCvR 7(h), Plaintiff the Electronic Privacy Information Center submits this statement of material facts not in genuine dispute in support of its cross motion for summary judgment.

1. On January 12, 2011, Google reported a major cyber attack from “highly sophisticated” hackers in China. *Memorandum of Law in Support of Defendant’s Motion for Summary Judgment* at 12; *Janosek Decl. Ex. A* at 1; *Complaint* at ¶ 5.
2. On February 4, 2010, the Washington Post and the Wall Street Journal reported that Google contacted the NSA regarding the firm’s security practices immediately following the attack. *Janosek Decl. Ex. A* at 2-4; *Complaint* at ¶ 6.
3. On February 4, 2010, EPIC transmitted, via certified mail, a written Freedom of Information Act (“FOIA”) request to NSA for agency records. (“EPIC’s FOIA Request”). EPIC requested the following agency records:
 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.

Janosek Decl. Ex. A; Complaint at ¶ 12.

4. By letter dated March 10, 2010, and postmarked March 15, 2010, the NSA denied EPIC's FOIA Request. The NSA invoked FOIA exemption b(3) and Section 6 of the National Security Agency Act and stated that they could "neither confirm nor deny whether the company has a relationship with the Agency related to the issues [EPIC described]." *Janosek Decl. Ex. B.*

5. EPIC transmitted, by certified mail, an administrative appeal (EPIC's FOIA Appeal) of the NSA's denial of EPIC's FOIA Request by letter dated May 7, 2010. *Janosek Decl. Ex. C.*

6. Through the date of the complaint, the NSA had failed to provide any response to EPIC's FOIA Appeal. *Complaint at ¶ 23.*

7. The NSA has not performed any search for agency records responsive to EPIC's FOIA Request. *Janosek Aff. at ¶ 10.*

Respectfully submitted,

/s/ John Verdi

MARC ROTENBERG
JOHN VERDI
Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140

Counsel for Plaintiff

Dated: January 28, 2011

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

ELECTRONIC PRIVACY INFORMATION CENTER)	
)	
Plaintiff,)	
)	
v.)	No. 1:10-cv-01533-RJL
)	
NATIONAL SECURITY AGENCY)	
)	
Defendant.)	
)	

**PLAINTIFF’S STATEMENT OF GENUINE ISSUES IN OPPOSITION TO
DEFENDANT’S STATEMENT OF MATERIAL FACTS**

In accordance with LCvR 7(h), Plaintiff the Electronic Privacy Information Center submits this statement of genuine issues in opposition to Defendant’s statement of material facts.

5. **Defendant’s alleged fact:** “NSA placed EPIC’s appeal in its queue for processing, but had not acted on that appeal before the instant Complaint was filed.”

Genuine issue: Plaintiff disputes that the NSA “placed [EPIC’s FOIA Appeal] in its queue for processing,” because EPIC received no response from the NSA in the more than three months between the submission of EPIC’s FOIA Appeal and the date the instant Complaint was filed.

6. **Defendant’s alleged fact:** “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.”

Genuine issue: Plaintiff disputes the description of the NSA's Information Assurance Mission to the extent the description is inconsistent with the underlying legal authority for the agency's program. See NSD 42, "National Policy for the Security of National Security Telecommunications and Information Systems," Jul. 5, 1990.

7. **Defendant's alleged fact:** "The U.S. government is largely dependent on commercial technologies for its information systems and often purchases such technologies and applications from private vendors."

Genuine issue: Plaintiff disputes the alleged "fact" on the grounds that: 1) there are insufficient facts in the record to support the statement; and 2) that the record fails to demonstrate Ms. Janosek's qualifications to opine as to the subject matter.

8. **Defendant's alleged fact:** "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."

Genuine issue: Plaintiff disputes the alleged "fact" on the grounds that Defendant's statement is wholly hypothetical.

9. **Defendant's alleged fact:** "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."

Genuine issue: Plaintiff disputes Defendant's "fact" insofar as the statement is a legal conclusion.

10. **Defendant's alleged fact:** "Determining whether to take action in response to a particular vulnerability is an activity taken by NSA in furtherance of its Information Assurance function."

Genuine issue: Plaintiff disputes Defendant's "fact" insofar as the statement is a legal conclusion.

11. **Defendant's alleged fact:** "NSA's 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."

Genuine issue: Plaintiff disputes Defendant's "fact" insofar as the statement is a legal conclusion.

Respectfully submitted,

/s/ John Verdi

MARC ROTENBERG
JOHN VERDI
Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
Counsel for Plaintiff

Dated: January 28, 2011