

No. 11-5233

ORAL ARGUMENT SCHEDULED FOR MARCH 20, 2012

**IN THE UNITED STATES COURT OF APPEALS
DISTRICT OF COLUMBIA CIRCUIT**

THE ELECTRONIC PRIVACY INFORMATION CENTER
Appellant,

v.

UNITED STATES NATIONAL SECURITY AGENCY
Appellee.

JOINT APPENDIX

MARC ROTENBERG
JOHN VERDI
AMIE STEPANOVICH*
ALAN BUTLER**
Electronic Privacy Information
Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
*Counsel for Appellant Electronic
Privacy Information Center*

* Ms. Stepanovich is admitted to practice in New York. Admission to the District of Columbia bar pending.

** Mr. Butler is admitted to practice in California.

JOINT APPENDIX

Electronic Privacy Information Center
v.
National Security Agency
(DC Cir No. 11-5233)

Document No.	Date	Document Title	Page(s)
1	09/13/10	Complaint for Injunctive Relief filed by Electronic Privacy Information Center	0001-0007
2	10/27/10	Answer to Complaint for Injunctive Relief Filed by National Security Agency	0008-0012
		Attachments: Tab A (EPIC FOIA Request) Tab B (NSA Response Letter) Tab C (EPIC Administrative Appeal)	0013-0018 0019-0021 0022-0026
3	12/22/10	Defendant’s Motion for Summary Judgment and Memorandum of Law in Support filed by National Security Agency	0027-0042
		Attachments: Tab A (Statement of Material Facts as to Which There is No Genuine Issue) Tab B (Declaration of Diane M. Janosek)	0043-0046 0047-0054
4	01/28/11	Plaintiff’s Opposition to Defendant’s Motion for Summary Judgment and Cross-Motion for Summary Judgment, and Memorandum of Law in Support filed by Electronic Privacy Information Center	0055-0072
		Attachments: Tab A (Plaintiff’s Statement of Material Facts Not in Genuine Dispute) Tab B (Plaintiff’s Statement of Genuine Issues in Opposition to Defendant’s Statement of Material Facts) Tab C Proposed Order	0073-0075 0076-0078 0079
5	02/18/11	Defendant’s Reply and Opposition to Plaintiff’s Motion for Summary Judgment filed by National Security Agency	0080-0093
		Attachments: Tab A (Response to Plaintiff’s Statement of Material Facts Not in Genuine Dispute)	0094-0095
6	03/04/11	Plaintiff’s Reply in Support of Plaintiff’s Motion for Summary Judgment filed by Electronic Privacy Information Center	0096-0105
7	07/13/11	Memorandum Opinion by Judge Richard J. Leon	0106-0115

JOINT APPENDIX

Document No.	Date	Document Title	Page(s)
8	07/13/11	Order of the United States District Court for the District of Columbia	0116
9	09/09/11	Civil Notice of Appeal filed by Electronic Privacy Information Center	0117

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

<hr/>)
ELECTRONIC PRIVACY INFORMATION CENTER)
1718 Connecticut Ave., N.W.)
Suite 200)
Washington, DC 20009)
)
Plaintiff,)
)
v.) Civil Action No. _____
)
NATIONAL SECURITY AGENCY)
9800 Savage Road,)
Suite 6248)
Washington, D.C. 20530)
)
Defendant.)
<hr/>)

COMPLAINT FOR INJUNCTIVE RELIEF

1. This is an action under the Freedom of Information Act (“FOIA”), 5 U.S.C. § 552 (2010), for injunctive and other appropriate relief, seeking the release of agency records sought by the Electronic Privacy Information Center from the National Security Agency.

Jurisdiction and Venue

2. This Court has subject matter jurisdiction over this action and personal jurisdiction over the parties pursuant to 5 U.S.C. § 552(a)(4)(B) (2010) and 5 U.S.C. § 552(a)(6)(C)(i) (2010). This Court also has jurisdiction over this action pursuant to 28 U.S.C. § 1331 (2010). Venue is proper in this district under 5 U.S.C. § 552(a)(4)(B) (2010).

Parties

3. Plaintiff Electronic Privacy Information Center (“EPIC”) is a public interest research

organization incorporated as a not-for-profit corporation in Washington, D.C. EPIC's activities include the review of federal policies and practices that impact the civil liberties and privacy interests of Internet users. EPIC routinely testifies before the United States Congress regarding emerging privacy and civil liberties issues. EPIC also publishes books, reports, a bi-weekly electronic newsletter, and maintains two of the most popular Internet sites on privacy – EPIC.ORG and PRIVACY.ORG.

4. Defendant the National Security Agency (“NSA”) is an agency established in the Executive Branch of the United States Government. The NSA is an agency within the meaning of 5 U.S.C. § 552(f)(1) (2010).

Facts

Defendant NSA and Google Entered Into a “Cooperative Research and Development Agreement” Following a Cyber Attack in January 2010

5. On January 12, 2010, Google reported a major cyber attack from “highly sophisticated” hackers in China.

6. 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.

7. 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."

8. On January 13, 2010, Google changed a key setting, encrypting by default all subsequent traffic to and from its electronic mail servers.

9. Previous to January 13, 2010, Google chose not encrypt Gmail, the firm's

electronic mail service, by default despite two compelling warnings about the risk in 2009.

10. 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 by default.

11. 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 non-encryption.

EPIC Submitted a FOIA Request to the NSA Regarding Its Collaboration With Google

12. On February 4, 2010, EPIC transmitted, via certified mail, a written FOIA request ("EPIC's NSA-Google FOIA Request") to the NSA for agency records. 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; and
- 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.

13. EPIC's NSA-Google FOIA Request followed immediately after news reports that appeared in the Wall Street Journal and Washington Post concerning a cyber attack on computer servers maintained by Google that contain the personal information of users of Google services.

14. EPIC urged the NSA to expedite processing for EPIC's NSA-Google FOIA Request on the bases that it pertains to a matter about which there is an urgency to inform the public relating to an actual or alleged federal government activity and that it was made by a person primarily engaged in disseminating information. 5 U.S.C. § 552(a)(6)(E) (2010). Petitioner cited the

widespread press reports of the arrangements as well as the privacy interests of hundreds of millions of Internet users who would be affected by the decisions.

15. EPIC also requested “News Media” fee status under the Freedom of Information Act, based on its status as a “representative of the news media” and previous determinations by other federal agencies.

The NSA Failed to Provide Records Responsive to EPIC’s FOIA Request

16. The NSA mailed a response to EPIC dated March 10, 2010 and postmarked March 15, 2010 (“The NSA’s Letter”).

17. The NSA’s Letter acknowledged the NSA’s receipt of EPIC’s NSA-Google FOIA Request, and acknowledged EPIC’s News Media status.

18. The NSA’s Letter cited FOIA exemption b(3) and Section 6 of the National Security Agency Act, neither confirming nor denying its relationship with Google.

19. The NSA’s Letter contained no records responsive to EPIC’s NSA-Google FOIA Request.

20. The NSA’s Letter failed to respond to the request for expedited processing in EPIC’s NSA-Google FOIA Request.

EPIC Filed an Administrative Appeal with the NSA

21. On May 7, 2010, more than twenty working days after the NSA received EPIC’s NSA-Google FOIA Request, EPIC transmitted a written administrative appeal to the NSA (“EPIC’s Administrative Appeal”).

22. EPIC’s Administrative Appeal appealed 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, 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

23. Through the date of this pleading, which is filed more than twenty working days after the NSA received EPIC's Administrative Appeal, the NSA has not responded to EPIC's Administrative Appeal.

24. Through the date of this pleading, the NSA has failed to produce any documents in response to EPIC's FOIA Request.

Count I

Violation of the FOIA: Failure to Comply With Statutory Deadlines

25. Paragraphs 1-25 above are hereby incorporated by reference as if set forth fully herein.

26. The NSA's response to EPIC's FOIA Request violated the statutory deadlines imposed by the FOIA, including the deadlines set forth in 5 U.S.C. § 552(a)(6)(A) (2010).

27. EPIC has exhausted the applicable administrative remedies with respect to EPIC's FOIA Request.

28. The NSA has wrongly withheld responsive agency records from EPIC.

29. EPIC is entitled to injunctive relief compelling the release and disclosure of the requested agency records.

Requested Relief

WHEREFORE, plaintiff prays that this Court:

- A. order defendant to conduct an adequate search for agency records responsive to EPIC's NSA-Google FOIA Request within five working days of the date of the Court's Order in this matter, with such searching including but not limited to all records concerning an agreement or similar basis for collaboration between the NSA and Google regarding

cyber security;

- B. order defendant to produce all responsive agency records within ten business days of the Court's Order in this matter;
- C. award plaintiff its costs and reasonable attorneys' fees incurred in this action pursuant to 5 U.S.C. § 552(a)(4)(E) (2010); and
- D. grant such other relief as the Court may deem just and proper.

Respectfully submitted,

By:



Marc Rotenberg, Esquire (DC Bar # 422825)
John Verdi, Esquire (DC Bar # 495764)
Ginger McCall, Esquire (Penn. Bar #307260)
Conor Kennedy, Esquire**
ELECTRONIC PRIVACY INFORMATION
CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009
(202) 483-1140 (telephone)
(202) 483-1248 (facsimile)

Dated:

* D.C. bar admission pending.
** N.Y. bar admission pending.

**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.)	

ANSWER TO COMPLAINT FOR INJUNCTIVE RELIEF

Defendant National Security Agency hereby answers plaintiff’s Complaint for Injunctive Relief (Docket No. 1) in the following numbered paragraphs, which correspond to the Complaint’s numbered paragraphs.

1. This paragraph is a characterization of plaintiff’s lawsuit to which no response is required. To the extent a response may be required, defendant admits that plaintiff’s lawsuit seeks injunctive and other appropriate relief pursuant to the Freedom of Information Act (“FOIA”), but denies that plaintiff is entitled to any such relief.

2. This paragraph sets forth conclusions of law to which no response is required.

3. Defendant is without knowledge or information sufficient to form a belief as to the truth of the allegations contained in this paragraph.

4. Admit.

5-7. These paragraphs contain plaintiff’s characterization of newspaper articles cited in its FOIA request dated February 4, 2010, to which no response is required. Defendant respectfully refers the Court to the cited articles for full and accurate statements of their contents.

8-11. Defendant is without knowledge or information sufficient to form a belief as to the truth of the allegations contained in these paragraphs.

12. Defendant admits that it received plaintiff's FOIA request dated February 4, 2010. Defendant respectfully refers the Court to that request, attached as Ex. 1, for a full and accurate statement of its contents.

13. Defendant is without knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph.

14-15. These paragraphs contain characterizations of the contents of plaintiff's FOIA request, to which no response is required. Defendant respectfully refers the Court to that request, attached as Ex. 1, for a full and accurate statement of its contents.

16. Defendant admits that its response letter was dated March 10, 2010, but is without knowledge or information sufficient to form a belief as to the truth of the allegation concerning the postmark date of that response.

17-20. These paragraphs contain characterizations of defendant's response letter dated March 10, 2010, to which no response is required. Defendant respectfully refers the Court to that response letter, attached as Ex. 2, for a full and accurate statement of its contents.

21. Defendant acknowledges receiving plaintiff's letter of administrative appeal dated May 7, 2010, and respectfully refers the Court to that letter, attached as Ex. 3, for a full and accurate statement of its contents.

22. This paragraph contains a characterization of the contents of plaintiff's letter of administrative appeal dated May 7, 2010, to which no response is required. Defendant

respectfully refers the Court to that letter, attached as Ex. 3, for a full and accurate statement of its contents. To the extent that a response may be required, defendant denies.

23. Defendant admits that it has not responded to plaintiff's letter of administrative appeal. Defendant further avers that plaintiff's filing of this civil action terminated the administrative processing of that appeal.

24. Defendant admits that it has not produced any documents in response to plaintiff's FOIA request. Defendant further avers that, based on Exemption 3 of FOIA, it did not acknowledge the existence or nonexistence of information responsive to plaintiff's FOIA request.

25. Defendant re-alleges its answers to paragraphs 1 through 24.

26-29. These paragraphs contain conclusions of law to which no response is required.

The remaining allegations in the Complaint constitute a prayer for relief to which no response is required. If a response were required, the allegations are denied. Defendant further denies that plaintiff is entitled to any relief demanded in the Complaint, or any relief whatsoever.

Defendant denies all allegations contained in the Complaint that it has not expressly admitted.

DEFENSES

1. The fact of the existence or nonexistence of any records responsive to plaintiff's FOIA request is exempt from disclosure under FOIA.

2. The Court lacks jurisdiction to grant relief to plaintiff because no records have been improperly withheld.

WHEREFORE, defendant prays that the Court dismiss plaintiff's suit with prejudice, render judgment that plaintiff take nothing by this action, and award defendant all other relief to which it is entitled.

Dated: October 27, 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)
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 Answer to Complaint for Injunctive Relief was served on October 27, 2010, by electronic filing to

Marc Rotenberg, 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

Ex. 1

Electronic Privacy Information Center v. National Security Agency
Civil Action No. 10-1533 (RJL)

24 Feb 2010

epic.org

February 4, 2010

BY CERTIFIED MAIL

National Security Agency
 Attn: FOIA/PA Office (DJP4)
 9800 Savage Road, Suite 6248
 Ft. George G. Meade, MD 20755-6248

1718 Connecticut Ave NW

Suite 200

Washington DC 20009

USA

+1 202 483 1140 [tel]

+1 202 483 1248 [fax]

www.epic.org

RE: Freedom of Information Act Request and Request for Expedited Processing

Dear FOIA/PA Officer:

This letter constitutes a request under the Freedom of Information Act ("FOIA"), 5 U.S.C § 552, and is submitted on behalf of the Electronic Privacy Information Center ("EPIC"). EPIC seeks records in the possession of the National Security Agency ("NSA") regarding the agency's arrangements with Google on cyber security, as well as records regarding the agency's role in setting security standards for Gmail and other web-based applications.

Background

On January 12, 2010, Google announced that hackers originating from China had attacked Google's corporate infrastructure.¹ According to Google, evidence suggested "that a primary goal of the attackers was accessing the Gmail accounts of Chinese human rights activists."² In response, Google made infrastructure and architectural changes and decided to stop censoring search results on the Chinese version of Google.³

On February 4, 2010, the press reported that Google and the NSA had entered into a "partnership" to help analyze the attack by permitting them to "share critical information."⁴ The Washington Post reported that "Google and the NSA declined to comment on the partnership."⁵ However, the NSA acknowledged that it has worked with the private sector on cyber security in the past: NSA spokeswoman Judi Emmel stated that "as part of its information-assurance mission, NSA works with a broad range of commercial partners and research associates to ensure the availability of secure tailored solutions for Department of Defense and national security systems customers."⁶

¹ David Drummond, *A new approach to China*, The Official Google Blog, Jan. 12, 2010, <http://googleblog.blogspot.com/2010/01/new-approach-to-china.html>.

² *Id.*

³ *Id.*

⁴ Ellen Nakashima, *Google to enlist NSA to help it ward off cyberattacks*, Feb. 4, 2010, <http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR2010020304057.html?hpid=topnews>.

⁵ *Id.*

⁶ *Id.*

Moreover, sources told the Post that “Google approached the NSA shortly after the attacks,” and that “the NSA is reaching out to other government agencies that play key roles in the U.S. effort to defend cyberspace and might be able to help in the Google investigation.”⁷ According to sources, “the focus of the partnership is “building a better defense of Google's networks, or what its technicians call ‘information assurance.’”⁸

The Wall Street Journal has also reported on the relationship between Google and the NSA:

The NSA's general counsel began drafting what's known as a cooperative research and development agreement the day Google announced the [hacker attack], according to a person familiar with the investigation. The agreement was finalized within 24 hours, but the flow of information was still limited, according to a person familiar with the investigation. It allowed the NSA to examine some of the data related to the intrusion into Google's systems.

Both the FBI and NSA dispatched officials to work directly with Google. Most of the information shared with NSA officials has been about the nature of the data that was stolen from Google, a person familiar with the investigation said.⁹

In a related cyber security matter, on January 13, 2010 Google set as a default the encryption of all traffic to and from its Gmail email servers.¹⁰ In the announcement, Google stated that it had not previously made encryption the default because it “can make your mail slower since encrypted data doesn't travel across the web as quickly as unencrypted data.”¹¹

Complete traffic encryption was available to users beginning in 2008, but was not enabled by default.¹² Due in part to the lack of encryption in Google's cloud computing services, EPIC filed a Complaint before the Federal Trade Commission on March 17, 2009, petitioning the Commission to investigate the adequacy of Google's privacy and security safeguards.¹³ The Commission is reviewing EPIC's Complaint.¹⁴ Similarly, 37 security and privacy experts wrote

⁷ *Id.*

⁸ *Id.*

⁹ Siobhan Gorman & Jessica E. Vascellaro, *Google Working With NSA to Investigate Cyber Attack*, Wall St. J., Feb. 4, 2010,

http://online.wsj.com/article/SB10001424052748704041504575044920905689954.html?mod=WSJ_latestheadlines.

¹⁰ Sam Schillace, *Default https access for Gmail*, The Official Gmail Blog, Jan. 13, 2010,

<http://gmailblog.blogspot.com/2010/01/default-https-access-for-gmail.html>; see Ryan Singel, *Google Turns on Gmail Encryption to Protect Wi-Fi Users*, Wired, Jan. 13, 2010, <http://www.wired.com/threatlevel/2010/01/google-turns-on-gmail-encryption-to-protect-wi-fi-users>.

¹¹ *Id.*; see also Alma Whitten, *HTTPS security for web applications*, Google Online Security Blog, June 16, 2009, <http://googleonlinesecurity.blogspot.com/2009/06/https-security-for-web-applications.html> (discussing Google's failure to encrypt all email traffic).

¹² *Id.*

¹³ EPIC, *In re: Google, Inc. and Cloud Computing Services*, March 17, 2009, available at <http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf>.

¹⁴ Letter from Eileen Harrington, Acting Director, Bureau of Consumer Protection, to Marc Rotenberg, John Verdi, and Anirban Sen (Mar. 18, 2009), http://epic.org/privacy/cloudcomputing/google/031809_ftc_ltr.pdf.

to Google, observing that the lack of encryption exposed Google users to “a very real risk of data theft and snooping, even by unsophisticated attackers.”¹⁵

As of 2009, Gmail had roughly 146 million monthly users.¹⁶ Despite the cyber security risk to the millions of Gmail users, Google did not enable complete encryption until after the hacker attack originating from China.¹⁷ The Washington Post reported that “Google approached the NSA shortly after the attacks.”¹⁸ The timing of Google’s decision to enable traffic encryption suggests a connection between that decision and Google’s relationship with the NSA regarding the hacker attacks.

Documents Requested

EPIC requests copies of 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.

Request for Expedited Processing

This request warrants expedited processing because it is made by “a person primarily engaged in disseminating information . . .” and it pertains to a matter about which there is an “urgency to inform the public about an actual or alleged federal government activity.” 5 U.S.C. § 552(a)(6)(E)(v)(II).

EPIC is “primarily engaged in disseminating information.” *American Civil Liberties Union v. Department of Justice*, 321 F. Supp. 2d 24, 29 n.5 (D.D.C. 2004).

Moreover, there is particular urgency for the public to obtain information about the relationship between the NSA and Google. As of 2009, Gmail had roughly 146 million monthly users, all of whom would be affected by any relationship between the NSA and Google. In less

¹⁵ Letter from 37 experts to Eric Schmidt, CEO of Google (June 16, 2009), http://www.wired.com/images_blogs/threatlevel/2009/06/google-letter-final2.pdf.

¹⁶ Michael Arrington, *Bing Comes To Hotmail*, TechCrunch, July 9, 2009, <http://www.techcrunch.com/2009/07/09/bing-comes-to-hotmail>.

¹⁷ See Sam Schillace, *Default https access for Gmail*, The Official Gmail Blog, Jan. 13, 2010, <http://gmailblog.blogspot.com/2010/01/default-https-access-for-gmail.html>.

¹⁸ Ellen Nakashima, *Google to enlist NSA to help it ward off cyberattacks*, Feb. 4, 2010, <http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR2010020304057.html?hpid=topnews>.

than one day, the relationship has received widespread coverage in the media.¹⁹ In order for the public to make meaningful decisions regarding their personal data and email, it must be aware of the details of that relationship. Neither Google nor the NSA has provided information regarding their relationship. The public should be informed.

Request for "News Media" Status

EPIC is a non-profit, educational organization that routinely and systematically disseminates information to the public. EPIC is a representative of the news media. *Epic v. Dep't of Defense*, 241, F.Supp. 2d 5 (D.D.C. 2003).

Based on our status as a "news media" requester, we are entitled to receive the requested records with only duplication fees assessed. Further, because disclosure of this information will "contribute significantly to public understanding of the operations or activities of the government," as described above, any duplication fees should be waived.

Thank you for your consideration of this request. As provided in 5 U.S.C. § 552(a)(6)(E)(ii)(I). I will anticipate your determination on our request for expedited processing within ten (10) calendar days.

Sincerely,



Matthew Phillips
Appellate Advocacy Counsel, EPIC

¹⁹ See, e.g., *Id.*; Siobhan Gorman & Jessica E. Vascellaro, *Google Working With NSA to Investigate Cyber Attack*, Wall St. J., Feb. 4, 2010, http://online.wsj.com/article/SB10001424052748704041504575044920905689954.html?mod=WSJ_latestheadlines; David Alexander, *Google, NSA may team up over cyberattacks: report*, Reuters, Feb. 4, 2010, <http://www.reuters.com/article/idUSTRE6130M120100204>.

DOCID: 3664481

REF ID:A3664481

U.S. POSTAGE
PAID
WASHINGTON, DC
20009
FEB 04 10
AMOUNT
\$3.85
00015345-05

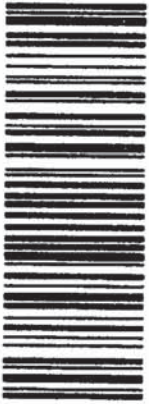


20755



1000

OPEN BY CGSI
FEB 18 2010
INSPECTED BY CGSI



7006 2J50 0001 7646 2211

ELECTRONIC PRIVACY INFORMATION CENTER

epic.org

1718 Connecticut Ave NW
Suite 200
Washington DC 20009
USA

National Security Agency
Attn: FOIA/PA Office (DJP4)
9800 Savage Road, Suite 6248
Ft. George G. Meade, MD 20755-6248

Ex. 2

Electronic Privacy Information Center v. National Security Agency
Civil Action No. 10-1533 (RJL)



NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 60923
10 March 2010

Matthew Phillips, Esquire
Electronic Privacy Information Center
1718 Connecticut Ave., NW, Suite 200
Washington, DC 20009

Dear Mr. Phillips:

This responds to your Freedom of Information Act (FOIA) request of 4 February 2010, which was received by this office on 24 February 2010, for:

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.

Your request has been assigned Case Number 60923. For purposes of this request and based on the information you provided in your letter, you are considered a representative of the media. There are no assessable fees for your request. Your request has been processed under the provisions of the FOIA.

As part of its longstanding Information Assurance mission, NSA works with a broad range of commercial partners and research associates to 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.

Please be advised that this Agency is authorized by statute to protect information concerning its functions and activities. The third exemption of the FOIA provides for the denial of information specifically protected from disclosure by statute. Therefore, we can neither confirm nor deny whether the company has a relationship with the Agency related to the issues you describe. The specific statute applicable in this case is the National Security Agency Act

FOIA Case: 60923

[Section 6, Public Law 86-36 (50 U.S.C. 402 note)]. Thus, your request is denied pursuant to the third exemption of the FOIA.

The Initial Denial Authority for NSA information is the Deputy Associate Director for Policy and Records, Diane M. Janosek. As your request is being denied, you are hereby advised of this Agency's appeal procedures. Any person denied access to information may file an appeal to the NSA/CSS Freedom of Information Act Appeal Authority. The appeal must be postmarked no later than 60 calendar days of the date of the initial denial letter. The appeal shall be in writing addressed to the NSA/CSS FOIA Appeal Authority (DJP4), National Security Agency, 9800 Savage Road STE 6248, Fort George G. Meade, MD 20755-6248. The appeal shall reference the adverse determination and shall contain, in sufficient detail and particularity, the grounds upon which the requester believes that the determination is unwarranted. The NSA/CSS FOIA Appeal Authority will endeavor to respond to the appeal within 20 working days after receipt, absent any unusual circumstances.

Sincerely,

A handwritten signature in cursive script, enclosed in a rectangular box. The signature appears to read "Pamela N. Phillips".

PAMELA N. PHILLIPS
Chief
FOIA/PA Office

Ex. 3

Electronic Privacy Information Center v. National Security Agency
Civil Action No. 10-1533 (RJL)

13 May 2010



May 7, 2010

BY CERTIFIED MAIL
NSA/CSS FOIA Appeal Authority (DJP4)
National Security Agency
9800 Savage Road STE 6248
Ft. George G. Meade, MD 20755-6248

1718 Connecticut Ave NW
Suite 200
Washington DC 20009
USA
+1 202 483 1140 [tel]
+1 202 483 1248 [fax]
www.epic.org

RE: Freedom of Information Act Appeal (FOIA Case 60923)

Dear FOIA Appeals Officer:

This letter constitutes an appeal under the Freedom of Information Act ("FOIA"), 5 USC § 552, and is submitted to the National Security Agency ("NSA") by the Electronic Privacy information Center ("EPIC").

On February 4, 2010, EPIC requested, via certified mail, documents regarding the agency's arrangements with Google on cyber security, as well as records regarding the agency's role in setting security standards for Gmail and other web-based applications. Specifically, EPIC requested the following:

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.

Procedural Background

On February 4, 2010, EPIC transmitted EPIC's FOIA Request to the NSA, requesting the above records as well as news media status and expedited processing.

In a letter dated March 10, 2010 and postmarked March 15, 2010, the NSA responded. In its letter, the NSA FOIA Office acknowledged EPIC's status as a member of the news media, and made no determination as to expedited processing. The March 10 letter also contained a substantive determination as to EPIC's FOIA Request. Specifically, the letter stated that the Agency would "neither confirm nor deny whether the company has a relationship with the Agency related to the issues [EPIC] describe[s]." The agency cited FOIA exemption b(3) and Section 6 of the National Security Agency Act as grounds for denying EPIC's request and withholding responsive agency records.

EPIC Appeals the NSA's Failure to Disclose Records

EPIC hereby appeals the NSA's failure to disclose records responsive to EPIC's FOIA Request. The denial is without sufficient grounds, because the claimed statutory exemption does not justify withholding.

The third exemption to the FOIA, cited by the NSA in its denial of EPIC's FOIA Request, states that the FOIA does not apply to matters that are

specifically exempted from disclosure by statute (other than section 552b of this title), if that statute—

- (A)
 - (i) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue; or
 - (ii) establishes particular criteria for withholding or refers to particular types of matters to be withheld; and
- (B) if enacted after the date of enactment of the OPEN FOIA Act of 2009, specifically cites to this paragraph.

5 U.S.C. 552(b)(3). Section 6 of the National Security Agency Act states relevantly, "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 any information with respect to the activities thereof, or of the names, titles, salaries, or number of the persons employed by such agency." National Security Agency Act of 1959, Pub. L. No. 86-36, § 6, 73 Stat. 63, 64, codified at 50 U.S.C. § 402 *note*.

By citing this statute as the basis for its exemption, the NSA claims that all portions of all documents requested by EPIC fall within Section 6, *i.e.* "the organization or any function of the [NSA]" or information concerning the NSA's activities or employees. However, the agency has presented no evidence for this assertion. EPIC's FOIA Request does not explicitly specify any organizational or functional information, nor does it request any "names, titles, salaries, or number of the persons employed by [the NSA]." Such information could easily be redacted from any disclosed documents if it appears. The NSA fails 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.

While courts have found that records described in Section 6 are exempt under section 552(b)(3), those same courts still required that the National Security Agency provide some factual basis for asserting the exemption. *see, e.g. Electronic Privacy Information Center v. Dep't of Justice*, 511 F. Supp. 2d 56, 67 (D.C.D. 2007); *Id.* at 73 ("Unsurprisingly, the declarations submitted by officials from NSA fail to identify at any level the documents withheld. . . . Accordingly, the court will require further submissions from NSA regarding these documents.").

Even when courts have not required a *Vaughn* index, see *Vaughn v. Rosen*, 484 F.2d 820, 826 (D.C. Cir. 1978), they have, at the very least, required affidavits and information regarding a sample search satisfying the criteria of *Northrop Corp. v. McDonnell Douglas Corp.*, 751 F.2d 395, 405–06 (D.C. Cir. 1984). See *Linder v. NSA*, 94 F.3d 693, 696–97 (D.C. Cir. 1996) (quashing subpoena and holding that a *Vaughn* index was not required where defendant agency had provided extensive affidavits regarding a sample search).

The NSA has provided no information regarding the agency records that are responsive to EPIC's request, nor has it even asserted that it performed a search for responsive documents. Without considerably more information about the number and nature of documents for which the agency is claiming exemption from the FOIA, it is impossible for the NSA to support the validity of the asserted exemption.

Conclusion

By improperly denying a request without providing sufficient grounds for its decision, the NSA has failed to comply with the FOIA. EPIC appeals the NSA's failure to disclose responsive documents and its failure to perform an adequate, reasonable search for the agency records described in EPIC's FOIA Request. As provided in 32 C.F.R. § 299.5(o)(6) and the NSA's letter dated March 10, 2010, I will anticipate your response to this appeal within 20 working days.

Sincerely,



Jared Kaprove
Domestic Surveillance Counsel, EPIC



John Verdi
Director, Open Government Project, EPIC

DOCID: 3694710REF ID:A3694710

1718 Connecticut Ave NW

Suite 208

Washington DC 20009

USA

epic.org

ELECTRONIC PRIVACY INFORMA

CERTIFIED MAIL

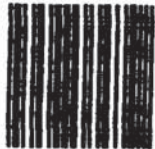


7006 2150 0001 7646 7349

OPEN BY CGSI
MAY 10 2010
INSPECTED BY CGSI

NSA/CSS FOIA Appeal Authority (DJP4)
National Security Agency
9800 Savage Road STE 6248
Ft. George G. Meade, MD 20755-6248

1006



20755

0003-1055-06
\$3.24

U.S. POSTAGE
PAID
WASHINGTON, DC
MAY 07, 10
PM/AM

**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 MOTION FOR SUMMARY JUDGMENT

Defendant National Security Agency respectfully moves for summary judgment under Rule 56 of the Federal Rules of Civil Procedure. This case involves a request for information plaintiff submitted to defendant pursuant to the Freedom of Information Act, 5 U.S.C. § 552. Defendant has refused to confirm or deny the existence of any records responsive to plaintiff’s request. That response is justified under the exemption to FOIA set forth at 5 U.S.C. § 552(b)(3). Accordingly, because defendant has appropriately responded to plaintiff’s request, and because there are no genuine issues in dispute, defendant is entitled to judgment in its favor as a matter of law. The accompanying Memorandum of Law in Support of Defendant’s Motion for Summary Judgment sets forth the reasons the Court should grant this motion.

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**

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

**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 an 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

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.)
_____)

DECLARATION OF DIANE M. JANOSEK

I, DIANE M. JANOSEK, hereby declare and state:

1. I am the current Deputy Associate Director for Policy and Records for the National Security Agency (hereinafter, "NSA" or "Agency"). I have served with NSA for over eleven (11) years, and prior to my current assignment, I held various leadership positions throughout the Agency. As the Deputy Associate Director for Policy and Records, I am responsible for processing all requests made pursuant to the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552 (2006), as amended by the OPEN Government Act of 2007, Pub. L. No. 110-175. I am also a TOP SECRET classification authority pursuant to section 1.3 of Executive Order 13526. It is my responsibility to invoke FOIA exemptions in the course of litigation.

2. Through the exercise of my official duties as Deputy Associate Director for Policy and Records, I have become familiar with the current litigation arising out of the request for records filed by Plaintiff, the Electronic Privacy Information Center, under the

Freedom of Information Act. The purpose of this declaration is to explain why NSA cannot acknowledge the existence or nonexistence of a relationship between NSA and Google regarding cybersecurity. Such a positive or negative response would reveal a core function and activity of NSA and is therefore protected from release by statute, specifically FOIA Exemption 3, 5 U.S.C. § 552(b)(3), and Section 6 of the National Security Agency Act of 1959, 50 U.S.C. § 402 note (Pub. L. No. 86-36). In order to provide the necessary context for the discussion that follows, I will first describe NSA's origin and mission.

I. ORIGIN AND MISSION OF NSA

3. NSA was established by Presidential Directive in October 1952 as a separately organized agency within the Department of Defense. NSA's cryptologic duties have two primary missions: (1) to collect, process, analyze, and disseminate Signals Intelligence (SIGINT) information for national foreign intelligence and counterintelligence purposes; and (2) to conduct information security activities.

4. Under this second mission, NSA's Information Assurance mission, NSA is charged with protecting Department of Defense and other national-security information systems, as well as providing direct support to other agencies that help protect other U.S. government information systems and the nation's critical infrastructure and key resources. For example, NSA provides support for important management systems for the U.S. government, including support for electronic key development and management and guidance on key distribution. NSA must maintain its formidable global advantage in information-system security to ensure that the United States and its allies can thwart our adversaries who seek to disrupt and exploit our networks and systems. To that end, NSA

has an unrivaled awareness of threats to national-security systems and how to mitigate them; indeed, NSA is simply the standard-bearer of government vulnerability discovery and security testing. NSA also provides or oversees cryptography for national-security systems. Additionally, NSA participates in public-private initiatives for technology certification, trust engineering, cross-domain solutions, security-automation standards, best security practices, information-assurance education, and operations security. NSA has worked with commercial vendors to develop and produce cryptographic products for use by the U.S. government, and NSA has worked with a number of organizations in developing and implementing standards for information-technology security.

5. In order for NSA to best help protect the U.S. government from ever-growing threats to its information systems, the Agency has developed a pro-active defense approach that includes monitoring malicious activity and, where possible, malicious actors. 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. NSA relies on information from vulnerability studies, security testing and evaluation, lessons learned, and forensic investigations to provide the best possible defense of U.S. government information systems.

6. The U.S. government is largely dependent on commercial technology for its information systems—for example, items such as word processing programs, operating systems, and e-mail software, among many others, are purchased commercially by the U.S. government from the private sector. NSA may discover vulnerabilities in commercial information technology or commercial security products used by NSA, the

Department of Defense, or other U.S. government agencies. Depending on the nature or severity of the discovered vulnerability, NSA may choose to take measures to secure it.

II. Processing of Plaintiff's FOIA Request

7. Plaintiff filed a FOIA request (attached as Exhibit A) on 4 February 2010, which was received by NSA on 24 February 2010, seeking information on the following: (1) All records concerning an agreement or similar basis for collaboration, final or draft, between 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 services, such as Google Docs.

8. By letter dated 10 March 2010 (attached as Exhibit B), the Chief, FOIA/PA Office, NSA/CSS, responded to Plaintiff's FOIA request. In this response, NSA informed Plaintiff about NSA's Information Assurance mission. Further, NSA informed Plaintiff that it could not confirm or deny the existence or nonexistence of the records responsive to Plaintiff's request—commonly known as a *Glomar* response—because such a response would reveal information about NSA's functions and activities, which is protected from release by an Exemption 3 statute, specifically, Section 6 of the National Security Agency Act of 1959, Pub. L. No. 86-36 (50 U.S.C. § 402 note). NSA also notified Plaintiff of its right to appeal this denial of the requested information.

9. By letter dated 7 May 2010 (attached as Exhibit C), Plaintiff appealed the NSA's decision to deny Plaintiff's FOIA request, as set forth in the 10 March 2010 letter

from the Chief, FOIA/PA Office. NSA placed Plaintiff's appeal in its appeal queue for processing. On 13 September 2010, before NSA had processed Plaintiff's appeal, Plaintiff filed a civil action regarding its FOIA request to NSA. At that time, NSA ceased processing Plaintiff's appeal.

10. I have submitted this declaration to explain to the Court why NSA cannot acknowledge the existence or nonexistence of the records sought by the Plaintiff, which in essence would constitute evidence of an alleged relationship or collaboration between NSA and Google regarding cybersecurity. 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. Accordingly, in such circumstances, NSA does not conduct a search for responsive records. A search is unnecessary because revealing the outcome of that search would reveal the very information that is exempted from disclosure under FOIA. As explained further below, 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.

III. NSA'S Invocation of Exemption 3 in Providing a *Glomar* Response to Plaintiff's FOIA Request

11. The fact of the existence or nonexistence of information responsive to Plaintiff's FOIA request is exempt from disclosure pursuant to Exemption 3 of the FOIA. *See* 5 U.S.C. §552(b)(3). This section provides that the FOIA does not require the release of "matters that are specifically exempted from disclosure by statute," provided that such 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.” One such statute is Section 6 of the National Security Agency Act of 1959, which provides in pertinent part: “[N]othing in this Act or any other law . . . shall be construed to require the disclosure of the organization or any function of the National Security Agency, [or] of any information with respect to the activities thereof” Accordingly, when a FOIA requester seeks records that would reveal information about an NSA “function” or its “activities,” the release of those records is not required under FOIA.

12. As stated above, one of NSA’s core missions is to assist in the effort to ensure the continued security of critical U.S. government information systems, a mission vital to U.S. national security in present times. And 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.

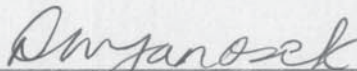
13. In its FOIA request, Plaintiff pointed out that Google acknowledged that it had been attacked by hackers originating from China. Plaintiff then requested records that would demonstrate a relationship between NSA and Google both before and related to that specific cybersecurity incident. Plaintiff also requested records of communications between NSA and Google regarding the encryption technology employed by Google in two of its principal technologies, Gmail and cloud-based computing services. 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. Further, any 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. 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.

14. 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. Such information would reveal what has or has not been done to fulfill that critical mission. Accordingly, I have determined that NSA's *Glomar* response was proper under FOIA Exemption 3 and the National Security Agency Act of 1959. Further, because 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, I have determined that there is no reasonably segregable, nonexempt portion of the requested records that can be released.

I hereby declare under penalty of perjury that the foregoing is true and correct.

Executed this 20th day of December, 2010.



DIANE M. JANOSEK
Deputy Associate Director for Policy and Records
National Security Agency

**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.)
)
NATIONAL SECURITY AGENCY)
)
Defendant.)

No. 1:10-cv-01533-RJL

**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

**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.)	

[PROPOSED] ORDER

Upon consideration of Defendant’s Motion for Summary Judgment, Plaintiff’s Opposition and Cross-motion for Summary Judgment, and any opposition and replies thereto, it is hereby

ORDERED that Defendant’s Motion is DENIED, and it is further

ORDERED that Plaintiff’s Motion is GRANTED, and it is further

ORDERED that Defendant perform an adequate search for records responsive to EPIC’s February 4, 2010 FOIA Request and disclose all responsive records to EPIC within thirty (30) days of the date of this order.

So ordered on this ____ day of _____, 2011

ROYCE C. LAMBERTH
United States District Judge

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

ELECTRONIC PRIVACY)
 INFORMATION CENTER,)
)
 Plaintiff,)
)
 v.)
)
 NATIONAL SECURITY AGENCY,)
)
 Defendant.)

Civil Action No. 10-1533 (RJL)

**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.)
)
NATIONAL SECURITY AGENCY,)
)
Defendant.)

Civil Action No. 10-1533 (RJL)

**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

**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 REPLY IN SUPPORT OF ITS
CROSS-MOTION FOR SUMMARY JUDGMENT**

Plaintiff the Electronic Privacy Information Center (“EPIC”) submits the following reply in support of its motion for summary judgment against Defendant the U.S. National Security Administration (“NSA”). EPIC challenges the NSA’s “*Glomar* response” to EPIC’s Freedom of Information Act (“FOIA”) request seeking records concerning the agency’s communications with Google, Inc. regarding cybersecurity.

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 February 4, 2010, EPIC filed a FOIA request with the NSA (“EPIC’s FOIA Request”). EPIC’s request sought:

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.

EPIC’s reply supports its cross-motion for summary judgment, Dkt. No. 10 (“EPIC’s Motion”) and responds to the NSA’s Reply and Opposition to Plaintiff’s Motion for Summary Judgment, Dkt. Nos. 12-13 (“NSA’s Reply”).

ARGUMENT

The NSA’s Reply reiterates the Agency’s contention that “confirming or denying the existence of the records requested by EPIC would reveal information related to ‘any function’ or ‘the activities’ of NSA.” NSA’s Reply at 2.

However, the Agency fails to rebut EPIC’s argument that the NSA is required to perform a search and segregability analysis prior to issuing a response to EPIC’s FOIA Request. Indeed, none of the cases cited in the NSA’s Reply support the proposition that an agency may issue a

Glomar response before searching for responsive documents. It is apparent that some records or portions of records demanded in EPIC's FOIA Request will fall outside the scope of the Section 6. The NSA must identify those records, perform a segregability analysis, and disclose the non-exempt records or portions of records.

Further, the NSA's assertion that the Janosek Declaration sufficiently supports the Agency's *Glomar* response is not persuasive in light of binding case law.

I. The NSA Must Perform a Search and Segregability Analysis Before the Agency May Issue a Lawful *Glomar* Response

The FOIA permits an agency to withhold documents that are specifically exempt from disclosure by statute. 5 U.S.C. § 552 (b)(3). The National Security Agency Act is such a statute, barring disclosure of any document that relates to "the organization or any function of the National Security Agency, or any information with respect to the activities thereof..." 50 U.S.C. § 402 note. In addition, this court has held that the National Security Agency may "refuse to confirm or deny the existence of certain records ... if [a] FOIA exemption would itself preclude the acknowledgement of such documents. *Wilner v. NSA*, 592 F.3d 60, 65 (2d Cir. 2009), quoting *Milner v. CIA*, 88 F.3d 796, 800 (9th Cir. 1996).

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 v. CIA*, 473 F.3d 370, 374 (D.C. Cir. 2007) (internal citations omitted).

However, an agency's *Glomar* response must be grounded on a factual determination that the requested records are exempt from disclosure under FOIA. *Phillipi v. Central Intelligence Agency*, 546 F.2d 1009, 1013 (D.D.C. 1976) (holding that an agency is required to "provide a public affidavit explaining in as much detail as possible the basis for its claim that it can be required neither to confirm nor to deny the existence of the requested records."). The requisite factual basis cannot be formulated absent a lawful agency search for records and subsequent segregability analysis.

In this case, the NSA admits that the agency has not spent a single minute searching for documents that are responsive to EPIC's FOIA Request. Janosek Decl. at ¶ 10. The agency has not identified a single record responsive to EPIC's FOIA Request. *Id.* And the NSA has failed to perform any segregability analysis. Janosek Decl. at ¶ 14. The NSA may not lawfully issue a *Glomar* response to EPIC's FOIA Request without developing a factual basis for its assertion of Exemption 3.

To be sure, an Exemption 3 determination turns "less on the detailed factual contents of specific documents" than on "the existence of a relevant statute and the inclusion of withheld material within the statute's coverage." NSA's Reply at 5, quoting *Ass'n of Retired R.R. Workers v. U.S. R.R. Retirement Bd.*, 830 F.2d 331, 336 (D.C. Cir. 1987) (internal citations omitted). However, *Ass'n of Retired R.R. Workers* assumes that the agency has identified the "specific documents" and analyzed the relevant statute's application to the "withheld material." In this case, the NSA has done neither. The authorities cited in the NSA's Reply do not support the agency's failure to search for responsive records in this case. *Ass'n of Retired R.R. Workers* upheld U.S. Railroad Retirement Board's Exemption 3 assertion, but only after the agency searched for and identified documents in response to the request. *Id.* at 335 (noting that the

agency determined that “the particular matter sought (*i.e.*, the mailing list)” was exempt under Exemption 3.) The NSA’s Reply also cites *Hunt v. CIA*, *Larson v. Department of State*, *People for the American Way Foundation v. NSA*, and *Moore v. Bush*. These cases uphold *Glomar* responses, but only after the agency searched for responsive records and determined that the records, if any, were properly the subject of a *Glomar* response. *See Hunt v. CIA*, 981 F.2d 1116, 1119 (9th Cir. 1992) (holding that records had been identified that contained information on “foreign nationals who are CIA intelligence sources, or who are suspected foreign intelligence operatives, or, who are CIA intelligence targets.”); *Larson v. Department of State*, 565 F.3d 857, 861-2 (D.C. Cir. 2009) (finding that records were ““derived from the most sensitive and fragile’ signals intelligence targets and identifies targets whose communications the NSA has exploited or pertains to intelligence collection assignments and the technical details of collection.”) (internal citations omitted); *People for the American Way Foundation v. NSA*, 462 F.Supp.2d 21, 31 (D.D.C. 2006) (finding that “the defendant’s declarations describe the information withheld and the ‘justifications for nondisclosure with reasonably specific detail.’”) (internal citations omitted); *Moore v. Bush*, 601 F.Supp.2d 6, 20 (D.D.C. 2009) (“NSA has shown that it too conducted a search reasonably calculated to uncover all relevant documents in response to Mr. Moore’s requests.”).

As a practical matter, the NSA is simply not able to determine that all documents responsive to EPIC’s FOIA Request are subject to Section 6 without any knowledge of what those documents may consist of or what information they might contain. The NSA’s reply fundamentally misconstrues the scope of EPIC’s FOIA Request by limiting it to only those matters that reflect a judgment call by the Agency. The NSA alleges that it is “apparent from the face of EPIC’s request that to confirm or deny the existence of responsive records would ...

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.” NSA’s Reply at 6. However, EPIC’s FOIA Request is much more broad. EPIC’s FOIA Request concerns a wide range of documents that do not reflect on the NSA’s activities in any way. For example, as EPIC has previously stated, documents that are responsive to EPIC’s FOIA Request might include emails, letters, voicemails, or other communications from Google to the NSA that are likely to reveal much about Google, but little, if anything, about the NSA’s functions and activities. EPIC’s Motion at 8.

By failing to even conduct a search for documents, it is impossible for the NSA to claim that all hypothetical responsive documents would necessarily reveal the activities of the Agency. In addition, the Agency’s response creates an incomplete record that prevents this Court from conducting an adequate review of the Agency’s action, which would stand unchecked – a result that is contrary to the D.C. Circuit’s direction to trial courts. *See Phillippi v. Central Intelligence Agency*, 546 F.2d 1009, 1013 (D.C. Cir. 1976) (“it is clear that the FOIA contemplates that the courts will resolve fundamental issues in contested cases on the basis on in camera examinations of the relevant documents.” Also stating that “The Agency’s arguments should then be subject to testing by appellate, who should be allowed to seek appropriate discovery when necessary to clarify the Agency’s position or to identify the procedures by which that position was established.”).

II. The Janosek Declaration is Not Sufficient to Support the NSA’s *Glomar* Response

The NSA re-asserts that the Janosek Declaration is “reasonably specific” to demonstrate that “the information withheld logically falls within the claimed exemption.” NSA Reply at 10

(internal citations omitted). However, the Declaration fails to state the agency's factual basis for its response in the required level of detail.

Although Congress drafted Section 6 with an "exceptionally wide scope," courts have emphasized that care must be used when "scrutinizing claims of exemptions based on such expansive terms." *Founding Church of Scientology of Wash., D.C., Inc. v. NSA*, 610 F.2d 824, 829 (D.C. Cir. 1979). EPIC does not suggest, as the NSA believes, 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." NSA Reply at 12, note 2. However, the NSA cannot use mere repetition of statutory language as a crutch for a lack of substantive reasoning to support the use of a *Glomar* response. "Barren assertions that an exempting statute has been met cannot suffice to establish that fact." *Scientology*, 610 F.2d at 831. As EPIC indicates, in the two pages (double-spaced) that the Janosek Declaration devotes to justifying the Agency's response, the statutory standard is reiterated no less than seven separate times. The Janosek Declaration then states three substantive, though conclusory, rationales for withholding a response to EPIC's FOIA Request:

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 Decl. 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 Decl. 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 Decl. at ¶ 13.

Though these assertions contain plenty of "doomsday" language about prevention of future cybersecurity attacks, the Janosek Declaration fails to provide any factual support for why all

responsive documents in the Agency’s possession would reveal the “vulnerabilities or cybersecurity issues” to which the Declaration alludes. For example, the Janosek Declaration states that “any acknowledgement...of the existence or nonexistence of a relationship with Google related to a specific cybersecurity incident would reveal whether or not the NSA considered the alleged attack to be of consequence for critical U.S. government information systems. Janosek Decl. at ¶ 13. However, EPIC’s FOIA Request is explicitly not limited to communications related to a specific cybersecurity attack, and is likely to include documents that have no relation at all to the January 12, 2010 cyber-attack.¹

CONCLUSION

For the foregoing reasons, EPIC asks the Court to deny Defendant’s Motion for Summary Judgment and grant EPIC’s Cross-motion for Summary Judgment as to the NSA’s invocation of a *Glomar* response to EPIC’s FOIA Request.

Respectfully submitted,

/s/ John Verdi

MARC ROTENBERG

JOHN VERDI

Electronic Privacy Information Center

¹ Compare this to the specificity of the affidavits in other cases that describe specific cause and effect reasoning to show that a *Glomar* response is appropriate to prevent disclosure of the Agency’s activities or functions. *See People for the American Way Foundation v. NSA*, 462 F.Supp.2d at 29 (“The NSA’s declarations explain that ‘confirmation by NSA that a person’s activities are not of foreign intelligence interest or that NSA is unsuccessful in collecting foreign intelligence information on their activities on a case-by-case basis would allow our adversaries to accumulate information and draw conclusions about NSA’s technical capabilities, sources, and methods.’”); *Larson v. Department of State*, 565 F.3d at 866-7 (“The agency similarly determined that confirming the existence or nonexistence of records responsive to Portillo-Bartow’s request would reveal vulnerabilities of communications systems, the success or lack of success in collecting information, and projects or plans relating to national security.”); *Hunt v. CIA*, 981 F.2d 1116 at 1119 (“[the affidavits] describe the scope of CIA record-keeping on foreign nationals. The CIA possesses records on foreign nationals who are CIA intelligence operatives, or, who are CIA intelligence targets. To confirm or deny the existence of records on Eslaminia could therefore reveal intelligence sources or targets... According to CIA affidavits, barring a *Glomar* response, CIA intelligence gathering would be impaired by its own disclosures in response to FOIA requests. CIA sources could find themselves under suspicion and in grave danger. The CIA avers that potential future sources would be reluctant to come forward; targets of intelligence security would be alerted and could take additional precautions; and foreign operatives could learn whether or not the CIA was aware of their activities.”).

1718 Connecticut Ave., NW
Suite 200
Washington, D.C. 20009
(202) 483-1140
Counsel for Plaintiff

CERTIFICATE OF SERVICE

I hereby certify that on the 4th day of March 2011, I served the foregoing PLAINTIFF'S REPLY IN SUPPORT OF ITS 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

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

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


MEMORANDUM OPINION
(July 8, 2011) [#9, #11]

Plaintiff Electronic Privacy Information Center (“EPIC” or “plaintiff”) brings this action against the National Security Agency (“NSA” or “defendant”) for failure to disclose information pursuant to the Freedom of Information Act (“FOIA”). Plaintiff seeks material relating to NSA’s possible relationship with Google following news of an alleged cyber attack by hackers in China and of a subsequent cooperation agreement between Google and NSA. Before this Court is defendant’s Motion for Summary Judgment and plaintiff’s Cross-Motion for Summary Judgment. After due consideration of the parties’ pleadings, the relevant law, and the entire record herein, defendant’s motion is GRANTED and plaintiff’s motion is DENIED.

BACKGROUND

On February 4, 2010, following media coverage of a possible partnership between the NSA and Google relating to an alleged cyber attack by hackers in China, EPIC submitted a FOIA request to NSA seeking:

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 the 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 the 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.

NSA denied EPIC's request. Letter from Pamela N. Phillips, NSA, FOIA/PA Office, Mar. 10, 2010 [#9-3]. While it acknowledged working "with a broad range of commercial partners and research associates," the Agency refused to "confirm [or] deny" whether it even had a relationship with Google. *Id.* In support of its response, NSA cited Exemption 3 of FOIA and Section 6 of the National Security Agency Act of 1959 ("NSA Act"), explaining that any response would improperly reveal information about NSA's functions and activities. *Id.* Such a response – neither confirming nor denying the existence of requested documents – is known as a *Glomar* response.¹

On May 7, 2010, EPIC appealed through the agency's internal appeal process. Compl. ¶ 21. However, after NSA failed to respond to EPIC's appeal within the statutory deadline, EPIC filed the complaint initiating this lawsuit. Pl.'s Opp'n to Mot. For Summ.

¹ The term "*Glomar* response" is derived from the ship the *Glomar Explorer*, and refers to the C.I.A.'s refusal to acknowledge the existence or non-existence of any records pertaining to the ship. *Phillippi v. C.I.A.*, 546 F.2d 1009, 1011 (D.C. Cir. 1976).

J. at 3 (Pl.’s Opp’n).² On December 22, 2010, NSA filed its Motion for Summary Judgment, contending that the use of a *Glomar* response was appropriate under the circumstances and that the requested information was protected from release by FOIA Exemption 3, 5 U.S.C. § 552 (b)3, and Section 6 of the NSA Act, Sec. 6, Pub. L. No. 86-36, 73 Stat. 63, 50 U.S.C. § 402 note. Def.’s Mem. in Supp. of Mot. Summ. J. (“Def.’s Mot.”) at 3.

In support of its motion, NSA submitted a declaration by Diane M. Janosek, the Deputy Associate Director for Policy and Records for the NSA (“Janosek Declaration” or “Declaration”). Decl. of Diane M. Janosek, Dec. 20, 2010 (“Janosek Decl.”) [#9-1]. Specifically, the Declaration states that, as part of its Information Assurance mission, NSA is responsible for “protecting Department of Defense and other national-security information systems, as well as providing direct support to other agencies that help protect other U.S. government information systems and the nation’s critical infrastructure and key resources.” *Id.* ¶ 4. The NSA also performs government vulnerability discovery and security testing, and participates in public-private security initiatives relating to the commercial technology that the U.S. Government uses for its information systems. *Id.* ¶¶ 5-6.

With respect to EPIC’s specific request, the Declaration states that “[t]o confirm or deny the existence of any such records would be to reveal whether the NSA . . . determined that vulnerabilities or cybersecurity issues pertaining to Google or certain of

² Once the suit was filed, NSA stopped processing EPIC’s appeal and filed an answer on October 27, 2010 to EPIC’s complaint. Def.’s Mot. at 4.

its commercial technologies could make U.S. government information systems susceptible to exploitation or attack.” *Id.* ¶ 13. The Declaration further clarifies that even an acknowledgement of a relationship between the NSA and a commercial entity could potentially alert “adversaries to NSA priorities, threat assessment, or countermeasures,” and that, as such, the information relates to the Agency’s core functions and activities under its Information Assurance mission. *Id.* ¶¶ 13-14.

In response to NSA’s Motion, EPIC filed a cross-motion on January 28, 2011. EPIC asserts two arguments: first, that NSA was required under FOIA to search for relevant records and segregate and disclose non-exempt information prior to issuing a *Glomar* response; and second, that the Janosek Declaration was “vague and conclusory,” and, therefore, insufficient under the law of this Circuit. Pl.’s Opp’n at 4. For the following reasons, I disagree.

ANALYSIS

Summary judgment is appropriate when the record demonstrates that there is no genuine issue of material fact in dispute and that the moving party is entitled to judgment as a matter of law. Fed. R. Civ. P. 56(a). The moving party bears the burden, and the court will draw “all justifiable inferences” in favor of the non-moving party. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 255 (1986). Nevertheless, the non-moving party “may not rest upon the mere allegations or denials of his pleading, but . . . must set forth specific facts showing that there is a genuine issue for trial.” *Id.* at 248 (internal quotations omitted). Factual assertions in the moving party’s affidavits may be accepted

as true unless the opposing party submits its own affidavits, declarations or documentary evidence to the contrary. *Neal v. Kelly*, 963 F.2d 453, 456 (D.C. Cir. 1992).

“When assessing a motion for summary judgment under FOIA, the Court shall determine the matter *de novo*.” *Judicial Watch, Inc. v. U.S. Dep’t of Homeland Sec.*, 598 F. Supp. 2d 93, 95 (D.D.C. 2009) (citing 5 U.S.C. § 552(a)(4)(B)). While the “burden is on the agency to sustain its action,” 5 U.S.C § 552 (a)(4)(B), courts must give substantial weight to an agency’s affidavits, *Hayden v. NSA/CSS*, 608 F.2d 1381, 1387 (D.C. Cir. 1979), *see Military Audit Project v. Casey*, 656 F.2d 724, 745 (D.C. Cir. 1981). The court may rely on the agency’s affidavits or declarations if they contain reasonable specificity of detail rather than merely conclusory statements, and if they are not called into question by contradictory evidence in the record or by evidence of agency bad faith. *See Halperin v C.I.A.*, 629 F.2d 144, 150 (D.C. Cir. 1980). “Ultimately, an agency’s justification for invoking a FOIA exemption is sufficient if it appears logical or plausible.” *Larson v. U.S. Dep’t of State*, 565 F.3d 857, 862 (D.C. Cir. 2009) (internal quotations omitted).

When an agency issues a *Glomar* response – refusing to confirm or deny the existence of documents – it must establish that the requested information is protected by one of the nine recognized FOIA exemptions. 5 U.S.C. § 552(b)(3); *see Wolf v. C.I.A.*, 473 F.3d 370, 375 (D.C. Cir. 2007). Exemption 3 permits an agency to prevent the release of records that are “specifically exempted from disclosure by statute.” 5 U.S.C. § 552(b)(3). Although FOIA requests are traditionally “narrowly construed,” *Dep’t of the Air Force v. Rose*, 425 U.S. 352, 361 (1976), Exemption 3 “differs from other FOIA

exemptions in that its applicability depends less on the detailed factual contents of specific documents,” *Goland v. C.I.A.*, 607 F.2d 339, 350 (D.C. Cir. 1978). Instead, “the sole issue for decision is the existence of a relevant statute and the inclusion of withheld material within that statute’s coverage.” *Id.*; see *Ass’n of Retired R.R. Workers v. U.S. R.R. Ret. Bd.*, 830 F.2d 331, 336 (D.C. Cir. 1987).

It is well established that Section 6 of the NSA Act is a statutory exemption under Exemption 3. See *Hayden*, 608 F.2d at 1389; *Founding Church of Scientology of Washington, D. C., Inc. v. N.S.A.*, 610 F.2d 824, 826 (D.C. Cir. 1979). Section 6 of the NSA Act broadly prohibits the disclosure of information pertaining to the organization, function, or activities of the NSA. National Security Agency Act of 1959, Sec. 6, Pub. L. No. 86-36, 73 Stat. 63, 50 U.S.C. § 402 note. Specifically, the NSA need not disclose “the organization or any function of the National Security Agency, [or] any information with respect to the activities thereof.” *Id.* While our Circuit has admonished that “courts must be particularly careful when scrutinizing claims of exemptions based on such expansive terms,” as those included in Section 6, *Scientology*, 610 F.2d at 829, this heightened scrutiny must be tempered by the recognition of the substantial challenges posed to the NSA in maintaining operational security, see *Hayden*, 608 F.2d at 1390 (interpreting the NSA Act to reflect congressional recognition of the agency’s “peculiar security needs”).

Thus, once the agency, through affidavits, has created “as complete a public record as is possible” and explained “in as much detail as is possible the basis for its claim,” *Phillippi*, 546 F.2d at 1013, the “court is not to conduct a detailed inquiry to

decide whether it agrees with the agency’s opinions,” *Halperin*, 629 F.2d at 148. Further, “NSA is not required to show harm to national security under Section 6.” *Larson*, 565 F.3d at 868; *see also Hayden*, 608 F.2d at 1390. As the Supreme Court explained in *C.I.A. v. Sims*, “bits and pieces of data ‘may aid in piecing together bits of other information even when the individual piece is not of obvious importance in itself.’” 471 U.S. 159, 178 (1985) (quoting *Halperin v. C.I.A.*, 629 F.2d 144, 150 (D.C. Cir. 1980)).

Here, NSA’s supporting affidavits satisfy the criteria for non-disclosure under Section 6.³ The Janosek Declaration contains sufficient detail, pursuant to Section 6, to support NSA’s claim that the protected information pertains to “the organization or any function of the National Security Agency, [or] . . . to the activities thereof.” 50 U.S.C. § 402 note; *see Hayden*, 608 F.2d at 1388 (granting summary judgment based on affidavits that describe “the activity involved, the need for maintaining secrecy, and the reason for believing that disclosure of any of the requested material could compromise legitimate secrecy needs”); *Miller v. Casey*, 730 F.2d 773, 776 (D.C. Cir. 1984) (describing as ample an affidavit which “demonstrates that the information withheld logically falls

³ Plaintiff’s argument regarding the public dissemination of information relating to a purported Google/NSA agreement is misleading. The agency has not waived its FOIA protections by official disclosure of the requested information. *See Wolf v. C.I.A.*, 473 F.3d 370, 378 (D.C. Cir. 2007). Nor does plaintiff ever contest this point. Rather, plaintiff incorrectly argues that information, which is widely reported in the media, is stripped of its FOIA protections. Pl.’s Opp’n at 9-10. Indeed, while *Glomar* responses are deemed inappropriate when the specific information has already been officially and publicly disclosed by the solicited agency, such disclosure “cannot be based on mere speculation, no matter how widespread.” *Id.* The agency, itself, must waive FOIA protections through an official disclosure. *Id.*

within the claimed exemption, and [is] not controverted by either contrary evidence in the record nor by evidence of agency bad faith” (internal quotations omitted)).

Indeed, as the Janosek Declaration makes clear, the requested information relates to the NSA’s cryptologic Information Assurance mission, which is designed to protect national security information systems and critical infrastructure resources. Janosek Decl. ¶ 5. Because of the reliance by the U.S. government on commercial systems, this mission includes the assessment of commercial technologies and the Agency’s participation in public-private security initiatives. *Id.* ¶¶ 5-6, 12.

Thus, with respect to plaintiff’s first request – all records concerning an agreement between NSA and Google regarding cyber-security – the Janosek Declaration explains that “any acknowledgement by NSA of the existence or nonexistence of a relationship or agreement with Google... would reveal whether or not NSA considered the alleged attack to be of consequence for critical U.S. government information systems.” *Id.* ¶ 13.

Further, with respect to plaintiff’s second and third requests – NSA/Google communications regarding encryption of Gmail and cloud-based computing service, such as Google Docs – the Janosek Declaration clarifies that “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 vulnerability or cyber security issues pertaining to Google or certain of its commercial technologies could make U.S. government information systems susceptible to exploitation or attack by adversaries . . .” *Id.* ¶ 13. The Declaration then adds, “[i]n 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.” *Id.*

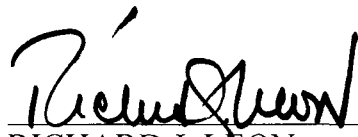
This Declaration provides more than cursory details concerning the relationship between the withheld material and NSA’s organization and function. *See Scientology*, 610 F.2d at 831. To the contrary, it explains the relevance of the Information Assurance mission to national security, the clear tie between the requested information and the Information Assurance mission, and the cognizable harm posed by acknowledging the existence/non-existence of the information.⁴ Thus, because NSA’s answer is both logical and plausible,⁵ the Declaration satisfies all the requirements set forth by our Circuit. *See Larson*, 565 F.3d at 862; *Halperin*, 629 F.2d at 148; *Hayden*, 608 F.2d at 1388.

⁴ EPIC argues that the NSA’s single supporting declaration is conclusory and fails to demonstrate that the requested information pertains to the NSA’s Information Assurance mission and is protected by the NSA Act exemption. Pl.’s Opp’n at 7-8. EPIC also challenges that its requests are broad enough to include documents that “do not reflect on the NSA’s activities in any way.” Pl.’s Opp’n at 6. These claims understate the Janosek Declaration’s depiction of the NSA’s Information Assurance mission, as well as the explanation of how the requested records would reveal information relating to NSA activities. Simply put, it is the relationship between Google and the NSA not just the content of records that warrants protections. *See Goland*, 607 F. 2d at 350.

⁵ NSA also argues that revealing a relationship with Google could dissuade other companies from working with the agency in the future or self-reporting on problems. Def.’s Reply at 10. This is a serious concern which also warrants finding for the NSA. *See Sims*, 471 U.S. at 175.

CONCLUSION

For all of the foregoing reasons, the Court GRANTS defendant's Motion for Summary Judgment [#9] and DENIES plaintiff's Cross-Motion for Summary Judgment [#11]. An Order consistent with this decision accompanies this Memorandum Opinion.



RICHARD J. LEON
United States District Judge

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

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

ORDER


For the reasons set forth in the Memorandum Opinion entered this 8th day of July, 2011, it is hereby

ORDERED that defendant’s Motion for Summary Judgment [#9] is **GRANTED**; and it is further

ORDERED that the plaintiff’s Cross-Motion for Summary Judgment [#11] is **DENIED**; and it is further

ORDERED that final judgment be entered for the defendant on all counts in the Complaint.

SO ORDERED.



 RICHARD L. LEON
 United States District Judge

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

333 Constitution Avenue, NW
Washington, DC 20001-2866
Phone: 202-216-7000 | Facsimile: 202-219-8530

Plaintiff: Electronic Privacy Information Ctr

vs.

Civil Action No. 1:10-cv-01533-RJL

Defendant: National Security Agency

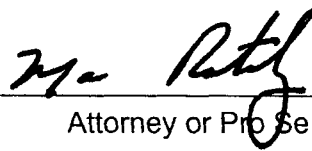
CIVIL NOTICE OF APPEAL

Notice is hereby given this 9 day of September 2011, that
the Electronic Privacy Information Center

hereby appeals to the United States Court of Appeals for the District of Columbia Circuit from the
judgement of this court entered on the 13 day of July, 2011, in

favor of the United States National Security Agency

against said Electronic Privacy Information Center



Attorney or Pro Se Litigant

(Pursuant to Rule 4(a) of the Federal Rules of Appellate Procedure a notice of appeal in a civil action must be filed within 30 days after the date of entry of judgment or 60 days if the United States or officer or agency is a party)

USCA Form 13
August 2009 (REVISED)

RECEIVED

SEP 09 2011

Clerk, U.S. District and
Bankruptcy Courts

JA-0117