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.*

---

# OPENING BRIEF FOR APPELLANT ELECTRONIC PRIVACY INFORMATION CENTER

---

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.

## CERTIFICATE AS TO PARTIES, RULINGS AND RELATED CASES

Pursuant to F.R.A.P. 26.1 and D.C. Cir. Rules 27(a)(4) and 28(a)(1)(A), Appellant certifies as follows:

*A. Parties and Amici*

Appellant is the Electronic Privacy Information Center ("EPIC"). EPIC is a 501(c)(3) non-profit corporation. EPIC has no parent, subsidiary, nor affiliate. EPIC has never issued shares or debt securities to the public. EPIC is a public interest research center in Washington, D.C., which was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other Constitutional values.

Appellee is the National Security Agency ("NSA"). The NSA is a federal agency subject to the FOIA.

No amici appeared before the district court.

*B. Ruling Under Review*

Appellant seeks review of the July 13, 2011 Opinion and Order of Judge Richard J. Leon of the United States District Court for the District of Columbia in case number 1:10-cv-01533-RJL. The July 13, 2011 order grants the National Security Agency's motion for summary judgment and denies the Electronic Privacy Information Center's motion for summary judgment. The ruling under

review is published at *EPIC v. NSA*, 798 F.Supp.2d 26 (D.D.C. 2011). The ruling is located in the Joint Appendix at JA 106-15.

*C. Related Cases*

This case was appealed from case number 1:10-cv-01533-RJL in the United States District Court for the District of Columbia. The District Court closed case number 1:10-cv-01533-RJL on September 14, 2011. There are no related cases pending before this Court or any other Court in the United States.

*/s/ Marc Rotenberg*
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*

Dated: January 3, 2012

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

| | | |
|---|---|---|
| ELECTRONIC PRIVACY INFORMATION CENTER | ) | |
| Appellant, | ) | |
| v. | ) | No. 11-5233 |
| NATIONAL SECURITY AGENCY | ) | |
| Appellee. | ) | |

**F.R.A.P. 26.1 CORPORATE DISCLOSURE STATEMENT**

Petitioner the Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other Constitutional values. EPIC is a 501(c)(3) non-profit corporation. EPIC has no parent, subsidiary, or affiliate. EPIC has never issued shares or debt securities to the public.

Respectfully Submitted,

*/s/ Marc Rotenberg*

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*

Dated: January 3, 2012

## TABLE OF CONTENTS

**CERTIFICATE AS TO PARTIES, RULINGS AND RELATED CASES ..... i**

A. Parties and Amici ..... i

B. Ruling Under Review ..... i

C. Related Cases ..... ii

**F.R.A.P. 26.1 CORPORATE DISCLOSURE STATEMENT ..... iii**

**TABLE OF CONTENTS ..... v**

**TABLE OF AUTHORITIES ..... vii**

**GLOSSARY ..... ix**

**JURISDICTIONAL STATEMENT ..... x**

**STATEMENT OF ISSUE FOR REVIEW ..... xi**

**STATUTES AND REGULATIONS ..... xii**

**STATEMENT OF FACTS ..... 1**

1) Google and Gmail ..... 1

2) Gmail Security Practices ..... 2

3) The National Security Agency ..... 4

4) 2010 Attack on Google Servers and Subsequent Actions ..... 5

5) EPIC's Freedom of Information Act Request ..... 6

**ARGUMENT ..... 11**

I. The Purpose of the FOIA is to Promote Disclosure of Government Records 12

II. The *Glomar* Response is Limited and Narrowly Construed ..... 13

III. The NSA Must Search For Non-Exempt, Reasonably Segregable Records Responsive to EPIC's FOIA Request ..... 20

A. The NSA is Required to Search For Responsive Records When a FOIA Request Seeks Documents That Are Not Facially Exempt ..... 21
B. The NSA is Required to Provide "Any Reasonably Segregable Portion of a Record" That is Non-Exempt ..... 22
C. EPIC's FOIA Request Seeks Records that Are Not Exempt Under Exemption 3 and Section 6 of the NSA Act ..... 26

**CONCLUSION ..... 33**

**TYPE/VOLUME CERTIFICATE OF COMPLIANCE WITH RULE 32(a) ..... 34**

**CERTIFICATE OF SERVICE ..... 35**

## TABLE OF AUTHORITIES

**Cases**


*Armstrong v. Executive Office of the President*, 97 F.3d 575 (D.C. Cir. 1996).. 24
*Beltranena v. Clinton*, 770 F. Supp. 2d. 175 (D.D.C. 2011)..... 23
*CIA v. Sims*, 471 U.S. 159 (1985) ..... 28
* *Dept. of the Air Force v. Rose*, 425 U.S. 352 (1976) ..... 12
* *Founding Church of Scientology of Washington, D.C., Inc. v. NSA*, 610 F.2d 824 (D.C. Cir. 1979)..... 15, 16, 17, 22, 26, 28
* *Gardels v. CIA*, 689 F.2d 1100 (D.C. Cir. 1982) ..... 9, 14, 15
*Greenberg v. Dept. of Treasury*, 10 F. Supp. 2d 3 (D.D.C. 1998)..... 21
*Hidalgo v. Bureau of Prisons*, No. 01-5257 2002 WL 1997999 (D.C. Cir. 2002) ..... 24
*Jefferson v. Dept. of Justice, Office of Professional Responsibility*, 284 F.3d 172 (D.C. Cir. 2002)..... 24, 25
*John Doe Agency v. John Doe Corp.*, 493 U.S. 146 (1989)..... 12
*Johnson v. Executive Office for U.S. Attorneys*, 310 F.3d 771 (D.C. Cir. 2002) 24
*Juarez v. Dept. of Justice*, 518 F.3d 54 (D.C. Cir. 2008)..... 24
*Kimberlin v. Dept. of Justice*, 139 F.3d 944 (D.C. Cir. 1998) ..... 22
* *Larson v. Dept. of State*, 565 F.3d 857 (D.C. Cir. 2009) ..... 17, 18, 25
*Mead Data Cent., Inc. v. Dept. of Air Force*, 566 F.2d 242 (D.C. Cir.1977) ..... 23
*Miller v. Casey,* 730 F.2d 773 (D.C. Cir. 1984)..... 14
*Moore v. Bush*, 610 F. Supp. 2d 6 (D.D.C. 2009)..... 26
*Morley v. CIA*, 508 F.3d 1108 (D.C. Cir. 2007)..... 24
*Nation Magazine*, *Washington Bureau v. U.S. Customs Service*, 71 F.3d 885 (D.C. Cir. 1995)..... 21, 27
*NLRB v. Robbins Tire & Rubber Co.*, 437 U.S. 214 (1978) ..... 12
*People for the American Way Foundation v. NSA*, 462 F. Supp. 2d 21 (D.D.C. 2006)..... 21, 27
*PHE, Inc. v. Dept. of Justice*, 983 F.2d 248 (D.C. Cir. 1993)..... 23
*Phillippi v. CIA,* 546 F.2d 1009 (D.C. Cir. 1976) ..... 14, 31
*Safecard Services, Inc. v. SEC*, 926 F.2d 1197 (D.C. Cir. 1991)..... 22
*Schiller v. NLRB*, 964 F.2d 1205 (D.C. Cir. 1992) ..... 23
*Wolf v. CIA*, 473 F.3d 370 (D.C. Cir. 2007)..... 14, 15, 24, 30, 31


**Statutes**


15 U.S.C. § 45(a) (2011) ..... 3
5 U.S.C. § 552(a)(3) (2011) ..... 20
* 5 U.S.C. § 552(b) (2011)..... 21, 22
5 U.S.C. § 552(b)(3) (2011) ..... 7, 14


Authorities upon which the brief chiefly relies are marked by asterisks.

50 U.S.C. § 402 note (2011) ..... 7, 14, 15

**Other Authorities**

Ben Chestnut, *Major Email Provider Trends Update: Gmail Pretty Much Caught Up*, MAILCHIMP BLOG, Aug. 1, 2011 ..... 2
Google History, Google (last visited Dec. 9, 2011) ..... 1
High Assurance Platform Program, NSA/CSS ..... 19
Hitwise United States, Experian Hitwise (last visited Jan. 2, 2012) ..... 2
Information Assurance at NSA, NSA/CSS (May 23, 2011) ..... 4
Inline Media Encryptor, NSA/CSS ..... 19
John Markoff, *Google Asks Spy Agency for Help with Inquiry Into Cyberattacks*, N.Y. Times, Feb. 4, 2010, at A6. ..... 6
Melinda Plemel, *A Marketer's Field Guide to Gmail Inboxes*, RETURNPATH, July 28, 2011 ..... 1
Memorandum from President Barack Obama on Freedom of Information Act to Heads of Executive Departments and Agencies (Jan. 21, 2009) ..... 13
Mike McConnell, *Mike McConnell on How to Win the Cyber-War We're Losing*, WASH. POST, Feb. 28, 2010 at B01 ..... 6
Motion for Summary Judgment by National Security Agency, Attachment 3 at 5, *People for the American Way Foundation*, 462 F.Supp.2d 21 (D.C. Cir. May 5, 2006) (No. 06-00206) ..... 25
National Security Agency, *Best Practices for Keeping Your Home Network Secure* ..... 20
National Security Agency, *IAD's Latest Security Guide Helps Customers Protect Home Networks*, Nov. 8, 2010 ..... 19
NSA/CSS Mission, NSA/CSS, http://www.nsa.gov/about/mission/index.shtml (April 15, 2011) ..... 4
Stephanie A. DeVos, Note, *The Google-NSA Alliance: Developing Cybersecurity Policy at Internet Speed*, 21 Fordham Intell. Prop. Media & Ent. L.J. 173, 177 (2011) ..... 6
The White House, The Comprehensive National Cybersecurity Initiative, March 10, 2010 ..... 30
United States Department of Justice, Office of Information Policy, *FOIA Post: President's Obama's FOIA Memorandum and Attorney General Holder's FOIA Guidelines*, Apr. 17, 2009 ..... 13

## GLOSSARY

| | |
|---|---|
| AR | Administrative Record |
| APA | Administrative Procedure Act |
| CEO | Chief Executive Officer |
| CRADA | Cooperative Research and Development Agreement |
| EPIC | Electronic Privacy Information Center |
| FTC | Federal Trade Commission |
| Google | Google, Incorporated |
| HTTPS | Secure Hypertext Transfer Protocol |
| JA | Joint Appendix |
| NSA | U.S. National Security Agency |
| SIGINT | NSA Signals Intelligence Mission |

## JURISDICTIONAL STATEMENT

This Court has jurisdiction over this case pursuant to 28 U.S.C. § 1291 (2011), as an appeal from a final judgment rendered by the United States District Court for the District of Columbia. The District Court entered final judgment on July 8, 2011 and Appellant Electronic Privacy Information Center timely filed a Notice of Appeal on September 14, 2011. On November 16, 2011, this Court entered an Order setting the briefing schedule and setting the time for the filing of the Appellant's Opening Brief as January 3, 2012.

## STATEMENT OF ISSUE FOR REVIEW

Whether the NSA is required to conduct a search for responsive agency records and perform a segregability analysis prior to issuing a *Glomar* response to a request for records under the Freedom of Information Act ("FOIA") when the request encompasses both exempt and non-exempt records.

## STATUTES AND REGULATIONS

**Statutes**

15 U.S.C. § 45(a) (2011) ..... 3
5 U.S.C. § 552(a)(3) (2011) ..... 20
5 U.S.C. § 552(b) (2011) ..... 21, 22
5 U.S.C. § 552(b)(3) (2011) ..... 7, 14
50 U.S.C. § 402 note (2011) ..... 7, 14, 15

## STATEMENT OF FACTS

*1) Google and Gmail*

Google, Inc. ("Google") was incorporated in 1998 in Menlo Park, California by Larry Page and Sergey Brin. Google History, Google, http://www.google.com/intl/en/about/corporate/company/history.html (last visited Dec. 9, 2011). Google provides a wide array of essential Internet services, including an electronic mail program, "Gmail."

Gmail is "cloud-based" computing service. The data and applications of the user reside on remote computer servers, operated by Google. JA 0015 n. 13. This model of service delivery is in contrast to an architecture in which data and applications reside on servers or computers within the control of the user. *Id*. Google stores Gmail users' personal messages on its servers.

Gmail is the third-largest e-mail service in the world. *See* Melinda Plemel, *A Marketer's Field Guide to Gmail Inboxes*, RETURNPATH, July 28, 2011, http://www.returnpath.net/blog/intheknow/2011/07/marketers-field-guide-gmail-inboxes/. Google boasted roughly 146 million Gmail users in 2009, and closed 2010 with 193 Gmail million users. *Id.;* JA 0015 n. 13. Gmail users are among the most active e-mail users. *See* Ben Chestnut, *Major Email Provider Trends Update: Gmail Pretty Much Caught Up*, MAILCHIMP BLOG, Aug. 1, 2011, http://blog.mailchimp.com/major-email-provider-trends-update-gmail-pretty-

much-caught-up/. Both Google.com and Gmail.com are included in the top ten most-visited websites across the entire Internet. Hitwise United States, Experian Hitwise, http://www.hitwise.com/us/datacenter/main/dashboard-10133.html (last visited Jan. 2, 2012).

*2) Gmail Security Practices*

Prior to January 2010, Google did not routinely encrypt the personal information of Gmail users. JA-0015. Encryption technology, such as Secure Hypertext Transfer Protocol ("HTTPS"), protects information on the Internet from unauthorized access by hackers and other bad actors. JA 0016 n. 15. Between 2005 and 2008, security researchers uncovered at least three major security flaws in Gmail and other Google cloud-computing services. JA 0015 n. 13. In 2008, Google allowed Gmail users to encrypt the mail that passed through Google servers, but did not provide encryption by default. JA 0015 n. 10.

On March 17, 2009, the Electronic Privacy Information Center ("EPIC") filed a complaint with the Federal Trade Commission ("FTC"), urging an investigation into Google's cloud computing services, including Gmail, to determine "the adequacy of the privacy and security safeguards." JA 0015 n. 13. The complaint followed a breach of Google Docs, a Google product that stores users documents for online editing on Google's remote servers. *Id*. In the complaint to the FTC, EPIC stated that Google repeatedly assured consumers that

it stored user data securely, but had in fact not adopted basic security practices to safeguard the information in its possession. *Id*. EPIC charged that Google's business practices were unfair and deceptive under Section 5 of the FTC Act. 15 U.S.C. § 45(a) (2011). EPIC further stated, "the Google Docs Data Breach highlights the hazards of Google's inadequate security practices, as well as the risks of Cloud Computing Services generally." JA 0015 n. 13. EPIC specifically asked the FTC to require the adoption of privacy enhancing technologies, such as encryption, for Google Cloud Services. *Id*.

On June 16, 2009, 37 researchers and academics in the fields of computer science, information security, and privacy law sent a letter to Eric Schmidt, Google's Chief Executive Officer in support of EPIC's concerns. *See* JA 0016 n. 15. The technical experts pointed out that Google had employed HTTPS in Gmail to protect individuals' login information, but did not enable it by default to protect information transmitted across its servers. *Id*. In addition, the experts explained that it was difficult even for sophisticated users to locate the menu that would allow them to enable HTTPS. *Id*.

Despite these two warnings, through January 2010 Google continued to allow HTTPS only as an opt-in feature for Gmail users. *See* JA 0016 n. 17.

*3) The National Security Agency*

The National Security Agency ("NSA") was formed in 1952 "as a separately organized agency within the Department of Defense." JA 0048. The NSA has two identified missions: (1) the Signals Intelligence ("SIGINT") mission, to "collect, process, analyze, and disseminate SIGINT information for national foreign intelligence and counterintelligence purposes and to support military operations" and (2) the Information Assurance mission, to "confront the formidable challenge of preventing foreign adversaries from gaining access to sensitive or classified national security information." The NSA/CSS Mission, NSA/CSS, http://www.nsa.gov/about/mission/index.shtml (April 15, 2011).

The White House established the NSA's Information Assurance mission in 1990 with the publication of National Security Directive 42. Information Assurance at NSA, NSA/CSS, http://www.nsa.gov/ia/ia_at_nsa/index.shtml (May 23, 2011); *See also* JA-0076 – JA-0077 at ¶ 6. The NSA's Information Assurance mission includes protection of the "Department of Defense and other national-security information systems, as well as [provision of] direct support to other agencies that help protect other U.S. government information systems and the nation's critical infrastructure and key resources." JA 0048 at ¶ 4; JA 0044 at ¶ 6.

The cybersecurity authority of the NSA was further modified in January 2008 by National Security Presidential Directive ("NSPD-54"), signed by

President George W. Bush. *See* The White House, The Comprehensive National Cybersecurity Initiative, March 10, 2010, *available at* http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

*4) 2010 Attack on Google Servers and Subsequent Actions*

On January 12, 2010, Google reported that the company had suffered a "highly sophisticated and coordinated attack originating from China." JA 0073 at ¶ 1. According to Google, the primary goal of the attack was to access the Gmail accounts of Chinese human rights activists. JA 0014 n. 1. The attackers planted malicious code in Google's corporate networks, which also resulted in the theft of Google's intellectual property. *Id*. The attackers attempted to access the Gmail accounts of several Chinese human rights activists, but it is unclear to what extent they were able to succeed. *Id*. The following day, Google changed Gmail's settings, causing all subsequent traffic to and from its servers to be encrypted by default. *See* JA 0016 n. 17.

David Drummond, Senior Vice President for Corporate Development and Google's Chief Legal Officer, stated that the company was notifying other companies that may have been targeted and further stated "we are also working with the relevant U.S. authorities." JA 0014 n. 1.

On February 4, 2010, the Washington Post reported that Google had contacted the NSA immediately following the attack. *Id*. The New York Times article of the same day began "Google has turned to the National Security Agency for technical assistance to learn more about the computer network attackers who breached the company's cybersecurity defenses last year." John Markoff, *Google Asks Spy Agency for Help with Inquiry Into Cyberattacks*, N.Y. Times, Feb. 4, 2010, at A6. The Wall Street Journal reported that the NSA's general counsel finalized a "Cooperative Research and Development Agreement" ("CRADA") within 24 hours of Google's announcement of the attack, authorizing the NSA to "examine some of the data related to the intrusion in Google's systems." JA 0015 n. 9.

Former NSA director Mike McConnell wrote in the Washington Post a few weeks later that collaboration between the NSA and Google was "inevitable." Mike McConnell, *Mike McConnell on How to Win the Cyber-War We're Losing*, WASH. POST, Feb. 28, 2010 at B01. *See also*, Stephanie A. DeVos, Note, *The Google-NSA Alliance: Developing Cybersecurity Policy at Internet Speed*, 21 Fordham Intell. Prop. Media & Ent. L.J. 173, 177 (2011).

*5) EPIC's Freedom of Information Act Request*

On February 4, 2010, following the widely reported research agreement between Google and the NSA, EPIC filed a Freedom of Information Act ("FOIA")

request with the NSA ("EPIC's FOIA Request"). JA 0013-0018. EPIC specifically requested: (1) all records concerning an agreement or similar basis for collaboration, final or draft, between the NSA and Google regarding cybersecurity; (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. *Id*.

By letter dated March 10, 2010, the NSA acknowledged receipt of EPIC's FOIA Request and granted EPIC's request for a fee waiver. JA 0019-0021. The NSA invoked Exemption 3 of the Freedom of Information Act (5 U.S.C. § 552(b)(3) (2011)) and Section 6 of the National Security Agency Act (50 U.S.C. § 402 note (2011)) in order to issue a *Glomar* response, neither confirming nor denying the existence of NSA records responsive to EPIC's FOIA Request. *Id*.

On May 7, 2010, EPIC filed an administrative appeal stating that the NSA had failed to present factual evidence that the requested documents fell within Section 6 and that established FOIA exemptions could sufficiently conceal protected information. JA 0022-0026. The NSA never replied to EPIC's appeal or produced responsive documents. *See* JA 0044 at ¶ 5. EPIC filed a complaint in the

United States District Court for the District of Columbia on September 13, 2010. JA 0001-0007.

On cross motions for summary judgment, the District Court below held in favor of the NSA and found that the Janosek Declaration supported NSA's *Glomar* response to all three of EPIC's FOIA requests. JA 0106-0115.

## SUMMARY OF ARGUMENT

The *Glomar* response is appropriate where "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). The NSA has failed to meet this standard and has failed to perform the segregability analysis required by statute to determine whether non-exempt records may be released.

The NSA has also failed to show that all three categories of the EPIC FOIA Request refer to only exempt, non-segregable records. EPIC's FOIA Request includes, for example, requests for unsolicited communications sent by third parties ("All records of communication between NSA and Google concerning Gmail, including but not limited too Google's decision to fail to routinely encrypt Gmail messages prior to January 13, 2010."). While the agency may choose to assert several statutory exemptions if it wishes to withheld records in its possession, acknowledging the *existence* of unsolicited third-party e-mails sent to the NSA does not reveal any information about the NSA's functions and activities. Moreover, if records in possession of the agency reveal activities that fall outside of the agency's proper functions and activities, these too would be subject to disclosure under the FOIA.

The NSA cannot be entitled to summary judgment where it failed to search for records responsive to a FOIA request. Without first conducting the search, not even the agency can know whether there is a factual basis for its legal position.

The decision of the District Court should be reversed and the case remanded with an order requiring the agency to conduct the search for responsive records.

## ARGUMENT

In the District Court, the NSA contended that the agency may issue a *Glomar* response to a Freedom of Information Act ("FOIA") request without performing a search. JA 0081-0085. The NSA asserted *Glomar*, a narrow doctrine for a special category for records, without ever searching for any responsive records within the agency's possession, without ever attempting to identify materials that could be disclosed, without even creating a record that would allow appellant or the court to evaluate the agency's position on an agency activity that is widely report in the national media, acknowledged by the former director of the agency, and impacts the interests of millions of Internet users. The agency's position is contrary to FOIA and prevailing case law.

EPIC's FOIA Request implicates third-party communications that were neither generated nor solicited by the NSA. The communications are agency records that do not convey information concerning the NSA's functions and activities. Thus, the records are not exempt from disclosure under the FOIA. At a minimum, the NSA must search for these records before asserting a *Glomar* response.

In addition, EPIC's FOIA Request seeks agency records concerning NSA activities that may fall outside the agency's lawful mandate, as set out in Section 6 of the NSA Act, as modified by NSPD-54. The records may also not be exempt

from disclosure under the FOIA. The NSA must search for these records before asserting a *Glomar* response.

## I. The Purpose of the FOIA is to Promote Disclosure of Government Records

The FOIA is animated by the "fundamental principle of public access to Government documents." *John Doe Agency v. John Doe Corp.*, 493 U.S. 146, 151-52 (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, 360-61 (1976) (citing S. Rep. No. 813, 89th Cong., 1st Sess., 3 (1965)). In order to fulfill this purpose, the FOIA imposes a segregability requirement on every agency, to ensure disclosure of all non-exempt portions of records. *See* 5 U.S.C. § 552(b).

President Obama has underscored the importance of the Freedom of Information Act. On his first full day in office, January 21, 2009, President Obama issued a memorandum to the heads of all departments and agencies on the Freedom of Information Act (FOIA). The President directed that FOIA "should be

administered with a clear presumption: In the face of doubt, openness prevails." United States Department of Justice, Office of Information Policy, *FOIA Post: President's Obama's FOIA Memorandum and Attorney General Holder's FOIA Guidelines*, Apr. 17, 2009, http://www.justice.gov/oip/foiapost/2009foiapost8.htm; Memorandum from President Barack Obama on Freedom of Information Act to Heads of Executive Departments and Agencies (Jan. 21, 2009), http://www.whitehouse.gov/the_press_office/Freedom_of_Information_Act.

The President directed the Attorney General to issue FOIA Guidelines for the heads of executive departments and agencies "reaffirming the commitment to accountability and transparency." *Id.* On March 19, 2009, Attorney General Eric Holder issued those Guidelines. The Attorney General highlighted that the FOIA "reflects our nation's fundamental commitment to open government" and that his Guidelines are "meant to underscore that commitment and to ensure that it is realized in practice." *Id.*

## II. The *Glomar* Response is Limited and Narrowly Construed

The FOIA recognizes "limited exemptions," but exemptions "must be narrowly construed." *John Doe Agency*, 493 U.S. at 152. Furthermore, "the burden is on the agency to sustain its action." *Id.* If a record falls within one of the FOIA's limited exemptions, the agency may choose to withhold the document. But the agency must inform the requester of the withholding and cite the applicable

exemption. The requester is then provided the opportunity to challenge the agency's determination, and even in circumstances when requesters are not able to review documents directly, courts will conduct *in camera* review to assess the adequacy of the agency's claims.

In a unique category of FOIA cases, an agency may issue a "*Glomar* response" and refuse to confirm or deny the existence of records. *Gardels*, 689 F.2d at 1103; *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). Courts uphold *Glomar* responses when "to answer the FOIA inquiry would cause harm cognizable under" an applicable statutory exemption. *Gardels,* 689 F.2d at 1103. *Glomar* responses must be tethered to a specific exemption. The agency must demonstrate that acknowledging the mere existence of responsive records would disclose exempt information. *Wolf v. CIA,* 473 F.3d 370, 374 (D.C. Cir. 2007)

In the present case, the NSA issued a *Glomar* response, alleging that any records responsive to EPIC's FOIA Request would be exempt from disclosure under Exemption 3 of the FOIA (5 U.S.C. § 552(b)(3) ("Exemption 3")) and that acknowledgement of the existence of records would cause harm cognizable under the exemption. The NSA's Exemption 3 claim is based on Section 6 of the National Security Agency Act (50 U.S.C. § 402 note ("Section 6")), which provides 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 any information with respect to the activities thereof." 50 U.S.C. § 402 note (2011).

In *Glomar* cases, courts may grant summary judgment on the basis of agency affidavits that 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." *Gardels,* 689 F.2d at 1104-05 (citing *Halperin v, CIA*, 629 F.2d 144, 148 (D.C. Cir. 1980)). The supporting affidavit must give a "logical" justification for the *Glomar* response based on "general exemption review standards established in non-*Glomar* cases." *Wolf*, 473 F.3d at 375. "Very importantly, 'the burden is on the agency to sustain its action.'" *Founding Church of Scientology of Washington, D.C., Inc. v. NSA*, 610 F.2d 824, 830 (D.C. Cir. 1979). This Circuit has made clear that "'[c]onclusory and generalized allegations of exemptions' are unacceptable; if the court is unable to sustain nondivulgence on the basis of affidavits, in camera inspection may well be in order." *Wolf*, 473 F.3d at 375.

"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." *Id.* at 374; *Gardels*, 689 F.2d at 1103-05. When reviewing an agency rejection, "a court shall determine the matter de novo, and may examine the

contents of … agency records in camera to determine whether such records or any part thereof shall be withheld under any of the exemptions set forth….” *Founding Church of Scientology*, 610 F.2d at 830 (citing 5 U.S.C. § 552(a)(4)(B)).

In *Founding Church of Scientology*, this Circuit considered the NSA’s *Glomar* response in a FOIA matter. The court examined the sufficiency of the NSA’s supporting affidavit (the “Boardman affidavit”). *Id.* at 830-31. The Boardman affidavit stated that “[d]isclosure of specific information which may be related to a specific individual or organization … in the context of the agency’s singular mission would reveal certain functions and activities of the NSA….” *Id.* at 831. The court held that the Boardman affidavit was conclusory and thus insufficient to support NSA’s broad rejection. The court made clear that “[p]articipation of the information-requesters to the fullest extent feasible is essential to the efficacy of de novo re-examination of the agency’s action.” *Id.* at 833. But, as the court pointed out, the parties must rely on the public record and, “if sufficiently informed, may discern a means of liberating withheld documents without compromising the agency’s legitimate interests.” *Id.*

*Founding Church of Scientology*, “firmly reject[ed] the notion that an agency should advance just so much as it deems essential to establish the applicability of a claimed exemption when it is able, without endangering activity that should remain secret, to supply publicly further details that well might aid the

de novo determination on disclosability or non-disclosability of the desired documents." *Id.* at 832 n.72. The court stressed that, "every effort should be made to segregate for ultimate disclosure aspects of the records that would not implicate legitimate intelligence operations…." *Id.* at 829 n.49.

In *Larson v. Dept. of State*, 565 F.3d 857 (D.C. Cir. 2009), this Court's most recent case reviewing an NSA *Glomar* response, the agency first searched for responsive records and conducted a segregability analysis, and then asserted *Glomar* with respect to certain records it had in fact identified. The Court upheld the agency's Glomar claim, in light of "sufficiently specific" detail provided in the affidavit regarding the NSA's need to keep "targets and foreign communications vulnerabilities secret." *Id*. at 867. The specificity of the agency's assertion in *Larson,* as well as its willingness to pursue a search for responsive records, contrasts sharply with the matter now before this Court.

In *Larson*, the plaintiffs submitted requests under the FOIA for information about past violence in Guatemala. *Id.* at 861. These requests were sent to various federal agencies, including the NSA. *Id.* In response to these requests, the NSA released ten documents in full, it released thirty-eight in part, it withheld one hundred and thirty-eight, and it issued a *Glomar* response to one request. *Id.* at 861-62. The NSA offered to provide a supplemental classified declaration *ex parte in camera* regarding its *Glomar* response. *Id.* at 862. The Court held that the NSA

properly asserted a *Glomar* response to one request where the NSA demonstrated "that the withheld information is properly classified under Executive Order 12958 in the interest of national security and thus logically falls within Exemption 1." *Id.* at 867. The Court agreed with the NSA that it was necessary to withhold this information to keep "targets and foreign communications vulnerabilities secret." *Id.* In addition, the Court found that the information sought was exempt under Exemption 3 due to its classified nature, its connection to "intelligence sources and methods," and its relation to the NSA's activities under Section 6. *Id.* at 868-69.

This Court recognized the importance of the NSA's *Glomar* response in the "Signals Intelligence" context in *Larson*. However, in that case the NSA searched for responsive records, and the Court held that the *Glomar* response was appropriate because the request clearly implicated classified intelligence records. The NSA's *Glomar* response is not so easily justified in this case, where the request covers communications that may or may not relate to the NSA's "information assurance" activities. While this Court has given the NSA broad discretion to withhold information about the existence or nonexistence of intelligence records, the same cannot be said of the records requested here. The mere existence of a communication from Google, the leading provider of Internet services, would not obviously cause any harm to the NSA's information assurance mission, particularly after the communication and subsequent collaboration was

widely reported in the national media and acknowledged by the former director of the NSA.

Moreover, the NSA's information assurance mission is not shrouded in secrecy. Many of the agency's information assurance activities are publicly disclosed. Indeed, the agency itself makes information about its information assurance mission available online. *See, e.g.,* High Assurance Platform Program, NSA/CSS, http://www.nsa.gov/ia/programs/h_a_p/index.shtml (describing a "NSA initiative to define a framework for the development of the 'next generation' of secure computing platforms" using "commercial-off-the-shelf … technologies"); Inline Media Encryptor, NSA/CSS, http://www.nsa.gov/ia/programs/inline_media_encryptor/index.shtml (describing an NSA "media encryption device" sold to private entities and jointly marketed by a private corporation, ViaSat, Inc.).

The NSA's information assurance mission includes programs directed at consumers. The agency publishes "many guidance documents … to customers outlining practical tips for improving the security of all kinds of applications, operating systems, routers, databases and more." National Security Agency, *IAD's Latest Security Guide Helps Customers Protect Home Networks*, Nov. 8, 2010, http://www.nsa.gov/ia/news/2011/security_guide.shtml. The NSA "has been providing unclassified security guidance to customers for over ten years." *Id*. In

fact, the agency publishes a security guide that recommends the use of "application encryption (also called SSL or TLS) over the Internet," in conjunction with *Gmail* "by default." National Security Agency, *Best Practices for Keeping Your Home Network Secure* at 5, *available at* http://www.nsa.gov/ia/_files/factsheets/Best_Practices_Datasheets.pdf (emphasis added).

This issue – the implementation of SSL by default to protect Gmail consumers – is the core concern of EPIC's FOIA Request. The NSA provides detailed advice to the general public on this topic. It describes the Google email service by name on a publicly accessible website. Yet the agency refuses to even acknowledge the existence of any records related to this topic when it receives a request under the Freedom of Information Act.

This Court has never granted the broad authority that the NSA seeks in this case, to issue a *Glomar* response without conducting a search for responsive records, particularly when the agency itself has put so much information about the subject matter of the request in the public record.

## III. The NSA Must Search For Non-Exempt, Reasonably Segregable Records Responsive to EPIC's FOIA Request

Like all federal agencies, the NSA must disclose all documents that do not fall into a FOIA exemption. 5 U.S.C. § 552(a)(3) (2011). When a document is

determined to be exempt under one of the enumerated exemptions, the NSA still must disclose any reasonable segregable portion. 5 U.S.C. § 552(b) (2011). A lawful search for responsive records is a necessary predicate to any assertion of FOIA exemptions, assertion of a *Glomar* response, or the performance of a segregability analysis.

### A. The NSA is Required to Search For Responsive Records When a FOIA Request Seeks Documents That Are Not Facially Exempt

In response to a FOIA request, agencies "must make a good faith effort to conduct a search for the requested records, using methods which can be reasonably expected to produce the information requested." *Nation Magazine*, *Washington Bureau v. U.S. Customs Service*, 71 F.3d 885, 890 (D.C. Cir. 1995) ("Nation Magazine") (internal citations and quotation marks omitted). "Even if [the] agency establishes an exemption, it must nonetheless disclose all reasonably segregable, nonexempt portions of the requested record(s)." *Id*. (internal quotation marks omitted).

FOIA Requests often seek multiple categories of documents. *See, e.g.*, *Greenberg v. Dept. of Treasury*, 10 F. Supp. 2d 3, 10 (D.D.C. 1998) (listing 6 categories of records contained in a FOIA Request); *People for the American Way Foundation v. NSA*, 462 F.Supp.2d 21, 31 (D.D.C. 2006) ("Plaintiff's original FOIA request sought sixteen categories of documents."). While one category of records may be exempt, another may require the disclosure of documents.

"In order to discharge its FOIA obligations, the agency must demonstrate that 'each document that falls within the [category] requested either has been produced, is identifiable, or is wholly exempt from the Act's inspection requirements.'" *Founding Church of Scientology,* 610 F.2d at 836. In order to make this determination, an Agency must first conduct a search that is "reasonably calculated to uncover all relevant documents." *See Safecard Services, Inc. v. SEC*, 926 F.2d 1197, 1201 (D.C. Cir. 1991). There may be times when a requested category of documents falls unquestionably within the gambit of a FOIA exemption. *See, e.g.*, *Kimberlin v. Dept. of Justice*, 139 F.3d 944 (D.C. Cir. 1998) (DOJ provided a *Glomar* response pursuant to the exemption for law enforcement records when a request asked for "all papers, documents, and things pertaining to the OPR investigation," and therefore fell facially within the exemption.). However, this Court has never allowed that an Agency may claim that all potentially responsive documents fall within a FOIA exemption without first requiring the Agency to conduct a search for documents.

### B. The NSA is Required to Provide "Any Reasonably Segregable Portion of a Record" That is Non-Exempt

The FOIA makes clear that, 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. Dept. 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."); *Schiller v. NLRB*, 964 F.2d 1205, 1210 (D.C. Cir. 1992) ("It is error for a district court to simply approve the withholding of an entire document without entering a finding on segregability, or the lack thereof.").

An agency must "correlate the theories of exemptions with the particular textual segments which it desired exempted." *Id.*, 964 F.2d at 1209-10 (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. Dept. of Justice*, 983 F.2d 248, 252 (D.C. Cir. 1993).

Only after undertaking a search is an agency able to perform the segregability analysis to determine if documents may be disclosed or lawfully withheld. *E.g. Beltranena v. Clinton*, 770 F. Supp. 2d. 175, 182 (D.D.C. 2011) ("the Court will direct the agency to supplement its affidavits to do what it should have done in the first place: conduct adequate searches and demonstrate that it has done so, and provide detailed explanations, document-by-document, for its segregability determinations.") (internal citations and quotation marks omitted);

*Hidalgo v. Bureau of Prisons*, No. 01-5257 2002 WL 1997999 at *1 (D.C. Cir. 2002) ("the Bureau of Prisons sufficiently demonstrated that it performed an adequate search, properly withheld documents or portions of documents pursuant to exemption 7, and adequately supported the non-Segregability of the information withheld."); *Armstrong v. Executive Office of the President*, 97 F.3d 575 (D.C. Cir. 1996) (upholding an Agency's segregability analysis following a search); *Juarez v. Dept. of Justice*, 518 F.3d 54 (D.C. Cir. 2008) (requiring a segregability analysis to follow the Agency's search); *Morley v. CIA*, 508 F.3d 1108 (D.C. Cir. 2007) (Holding that the Agency's search was inadequate and that the District Court was required to make a segregability ruling); *Johnson v. Executive Office for U.S. Attorneys*, 310 F.3d 771 (D.C. Cir. 2002) (examining the District Court's finding that an appropriate search was conducted and followed by a segregability analysis.).

Agencies are not exempt from performing a segregability analysis, even in cases where they assert a *Glomar* response. *See, Wolf*, 473 F.3d at 374 ("In determining whether the existence of records *vel non* fits a FOIA exemption, courts apply the general exemption review standards established in non-*Glomar* cases."); *see also Jefferson v. Dept. of Justice, Office of Professional Responsibility*, 284 F.3d 172, 176 (D.C. Cir. 2002) ("The district court granted summary judgment following a declaration that "'all nonexempt information

contained in the 17 [redacted] documents was reasonably segregated for release' to Jefferson, and that pursuant to Exemption 7(C), 'OPR would neither confirm nor deny any other records that may or may not exist' on AUSA Downing.").

In order for a *Glomar* response to be proper, there must first be an evidentiary finding that every possible document encompassed by each category of a FOIA request falls within a named FOIA exemption and even then a court inquires into whether *Glomar* was properly asserted. *See, Jefferson*, 284 F.3d at 179 ("a *Glomar* response was inappropriate in the absence of an evidentiary record produced by OPR to support a finding that all OPR records regarding AUSA Downing are law enforcement records.").

This Court has routinely upheld *Glomar* responses only in cases where it is apparent from the record that the Agency first conducted a search and segregability analysis, and even disclosed or withheld specific responsive records. *See* Motion for Summary Judgment by National Security Agency, Attachment 3 at 5, *People for the American Way Foundation*, 462 F.Supp.2d 21 (D.C. Cir. May 5, 2006) (No. 06-00206) ("In response to plaintiff's FOIA request, NSA undertook a search for those categories of documents which were most likely to contain the information responsive to plaintiff's specific requests."); *Larson*, 565 F.3d at 861-62 (upholding a *Glomar* response after the agency demonstrated that a thorough search had been performed for the many categories of documents relating to the

lawsuit); *Founding Church of Scientology*, 610 F.2d at 825-26 (the NSA performed a search and identified certain records responsive to the request, but the court still held that the agency affidavit was insufficient to justify withholding them under Exemption 3 and Section 6); *Moore v. Bush*, 610 F. Supp. 2d 6, 15 (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.").

### C. EPIC's FOIA Request Seeks Records that Are Not Exempt Under Exemption 3 and Section 6 of the NSA Act

EPIC's FOIA Request seeks: (1) all records concerning an agreement or similar basis for collaboration, final or draft, between the NSA and Google regarding cybersecurity; (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. JA 0013-0018. Section 2 of EPIC's FOIA Request seeks communications between the NSA and Google concerning Gmail, Google's email product. Communications from Google to the NSA do not implicate the agency's functions and activities, and are therefore not exempt from disclosure. Further, some records responsive to EPIC's FOIA Request concern NSA activities that may fall outside

the scope of the agency's Section 6 authority. These records are not exempt from disclosure.

In response to EPIC's FOIA Request, the NSA asserted that it can "neither confirm nor deny" the existence of responsive records because "such a response would reveal information about NSA's functions and activities," which are protected from release by Section 6, and thus can be exempted pursuant to Exemption 3. In support of this assertion, the NSA submitted an affidavit of its Deputy Associate Director for Policy and Records, Diane M. Janosek (the "Janosek Declaration"). The NSA has not conducted "a search for responsive records" in this case. JA 0051; Janosek Decl. at ¶ 10. Yet, without searching or reviewing potentially responsive records, the agency claimed that, "there is no reasonably segregable, nonexempt portion of the requested records that can be released." JA 0081-0085; Janosek Decl. at ¶ 14.

Summary judgment in a FOIA case should only be granted to the Government if "the agency proves that it has fully discharged its obligations under the FOIA, after the underlying facts and the inferences to be drawn from them are construed in the light most favorable to the FOIA requester." *People for the American Way Foundation*, 462 F. Supp. 2d at 27. "An agency [has] a duty to construe a FOIA request liberally." *Nation Magazine*, 71 F.3d at 890 (citing *Truitt v. Dept. of State*, 897 F.2d 540, 544-45 (D.C. Cir. 1990)); *Founding Church of*

*Scientology*, 610 F.2d at 836-37. When reviewing an agency's invocation of Exemption 3, a court must first determine whether the agency has identified a proper statutory exemption, then it must determine whether the records requested fall within that statutory exemption. *CIA v. Sims*, 471 U.S. 159, 167 (1985). As this Circuit ruled in *Founding Church of Scientology*, Section 6, which was invoked in this case, "is a statute qualifying under Exemption 3." *Founding Church of Scientology*, 610 F.2d at 828. However, the court forewarned that Section 6 has "a potential for unduly broad construction," and stressed that "courts must be particularly careful when scrutinizing claims of exemptions based on such expansive terms." *Id.* (citing *Ray v. Turner*, 587 F.2d 1187, 1220 (D.C. Cir. 1978)).

The District Court below, presented with a broad, three-part FOIA request from EPIC, granted summary judgment on the basis of an agency affidavit that (1) admitted the agency did not conduct a search for responsive records and (2) concluded that "there is no reasonably segregable, nonexempt portion of the requested records that can be released." JA 0051, 0053; Janosek Decl. at ¶¶ 10, 14. If EPIC's FOIA request is construed liberally, as required by law, then it is broad enough to include any unsolicited, third-party communications sent from any

Google employee to any NSA contact "concerning Gmail."[1] JA 0016; Janosek Decl. at ¶ 7; *See also* JA 0003.

In order to survive summary judgment, the NSA's response must leave open no genuine issue of material fact. The agency's affidavit must justify the failure to acknowledge the existence of third-party communications that may or may not be related to NSA "functions and activities."

The agency affidavit argued that "[t]o 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 … 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." JA 0039; Janosek Decl. at ¶ 13. The affidavit does not attempt to explain, nor could it, how the mere existence, or nonexistence, of a communication created by a third-party could reveal information about NSA's "functions and activities."

Since responsive records might exist that (1) were not created by the NSA, and (2) do not relate to the NSA's "functions or activities" this conclusion requires a great deal more "specificity of detail" in order to be sufficient to support summary judgment. Not only does the affidavit's justification fail the "logical or

[1] For example, if any NSA e-mail account received a message with the term "Gmail" in it, even if that message was an advertisement, marked as SPAM, immediately deleted, or otherwise ignored by the agency, it would qualify as a responsive record.

plausible" test, *Wolf*, 473 F.3d at 375, but the NSA's refusal to conduct a search for reasonably segregable records borders on bad faith, and is a clear failure to comply with the FOIA.

In addition, EPIC's FOIA Request seeks records "concerning an agreement or similar basis for collaboration, final or draft, between NSA and Google regarding cyber security" and "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." JA 0003. Although the NSA has broad authority, the agency's authority to conduct cybersecurity activities is not unbounded. The NSA's cybersecurity authority was modified in January 2008 by NSPD-54. The White House, The Comprehensive National Cybersecurity Initiative, March 10, 2010, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative. NSPD 54 authorizes the NSA and other agencies to secure federal government computer networks, coordinate government research efforts concerning computer security and government data-sharing, and define the role for extending cybersecurity programs to critical infrastructure. *Id*. at 2-5. NSPD 54 does not authorize the NSA to enter into an "agreement or similar basis for collaboration" with "Google regarding cyber security" or play a "role in Google's decision regarding the failure to routinely deploy encryption for cloud-based

computing services, such as Google Docs." JA 0003. NSPD 54 primarily authorizes the NSA to secure government computer networks. EPIC's FOIA Request does not seek any records concerning this agency activity. NSPD 54 authorizes the NSA and/or other agencies to define a role for the government to help secure critical infrastructure. EPIC's FOIA Request does not seek any records concerning this agency activity – Google provides cloud-based services to consumers, not critical infrastructure services to the government.

As the case that created the *Glomar* response made clear, a court in a FOIA case must decide based on "as complete a public record as possible." *Phillippi*, 546 F.2d at 1013. The NSA has failed to meet that standard. 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 records responsive to EPIC's request are properly exempt under Exemption 3 and Section 6. 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 *Glomar* response is only justified if all three categories of records requested by EPIC, broadly construed, are facially exempt from FOIA

regardless of their content or context. The District Court's determination that "no genuine issue of material fact" existed as to this broad facial exemption claim is unsupported in the record because the NSA refused to conduct a search for records. There is simply no factual basis for the NSA to conclude that nonexempt records do not exist when the agency has not performed a search for records.

## CONCLUSION

For the foregoing reasons, this Court should overturn the District Court's decision and order that the NSA conduct a search for documents in response to EPIC's FOIA Request.

Respectfully submitted,

*/s/ Marc Rotenberg*
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*

Dated: January 3, 2012

**TYPE/VOLUME CERTIFICATE OF COMPLIANCE WITH RULE 32(A)**

I hereby certify that the foregoing brief complies with the typeface requirements of F.R.A.P. 32(a)(5) and the type-style requirements of Rule 32(a)(6). The brief is composed in a 14-point proportional typeface, Times New Roman, and complies with the word limit of Rule 32(a)(7)(B)(iii).

*/s/ Marc Rotenberg*
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*

## CERTIFICATE OF SERVICE

The undersigned counsel certifies that on this 3rd day of January 2012, he caused the foregoing brief to be served by ECF and two hard copies by first-class mail, postage prepaid, on the following:

Catherine Y. Hancock
U.S. Department of Justice
Office of the Attorney General
950 Pennsylvania Avenue, NW
Washington, DC 20530

Douglas N. Letter, Esquire, Attorney
U.S. Department of Justice
Civil Division, Appellate Staff
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

*/s/ Marc Rotenberg*
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*