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.*

# REPLY 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 the State of New York. Her application for admission to the District of Columbia bar is pending.
[**] Mr. Butler is admitted to practice in the State of California.

# TABLE OF CONTENTS

## TABLE OF AUTHORITIES

*Authorities chiefly relied upon are marked with an asterisk.

## SUMMARY OF THE REPLY ARGUMENT

The NSA concedes that EPIC's request under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, seeks certain agency records that might "reveal information only about Google (and nothing about NSA)." Appellee's Brief ("Br. of Appellee") at *22. Yet, the NSA argues, "those records, if maintained by the Agency, would still constitute evidence of some kind of relationship between Google and the NSA." *Id.* The NSA fails to rebut EPIC's contentions that unsolicited communications from Google, and other similar records, are not exempt under Section 6 of the National Security Agency Act of 1959 ("Section 6"), Pub. L. No. 86-36, 73 Stat. 63, 64 (codified at 50 U.S.C. § 402 note), and that information about the *mere existence or nonexistence* of these records would not reveal any NSA *functions or activities*. Thus, these records are subject to release under the FOIA and the NSA's *Glomar* response is unlawful.

The NSA also does not dispute that a *Glomar* response must be tethered to a FOIA exemption as applied to a specific record or category of records. Yet the NSA has not tied its *Glomar* response to a record or category of records in this case. Moreover, the NSA relies on prior cases concerning "classified intelligence gathering," and not the Agency's Information Assurance mission, which is a public-facing program involving commercial products, at issue in this case.[1]

It is impossible for the Agency to determine whether documents requested are exempt under FOIA prior to a search. Moreover, the NSA's novel interpretation of Section 6 would place a new category of records beyond judicial review. For all of these reasons, the decision of the lower court should be reversed.

[1] For example, the NSA currently provides, on a publicly accessible website, "Best Practices for Securing a Home Network." BEST PRACTICES FOR KEEPING YOUR HOME NETWORK SECURE (National Security Agency 2011), *available at* http://www.nsa.gov/ia/_files/factsheets/Best_Practices_Datasheets.pdf.

# ARGUMENT

## I. EPIC's FOIA Request Includes Documents That are Not Facially Exempt Under the FOIA

The NSA's invocation of FOIA Exemption 3, 5 U.S.C. § 552(b)(3), must be analyzed according to the two-prong test established by the Supreme Court in *CIA v. Sims*: (1) whether the statute in question qualifies under Exemption 3, and (2) whether the withheld material meets the statutory criteria. 471 U.S. 159, 167 (1985). It is clearly established that Section 6 of the NSA Act is a qualifying statute under Exemption 3. *See Founding Church of Scientology v. NSA*, 610 F.2d 824, 828 (D.C. Cir. 1979). The only question that remains is whether the materials requested by EPIC satisfy the statutory criteria necessary to support the NSA's blanket *Glomar* response and refusal to search. Because the NSA has failed to provide a factual or legal basis to refute EPIC's contention that non-exempt records exist and must be disclosed, EPIC's FOIA Request can not be considered facially exempt under Section 6 of the NSA Act. Indeed, courts routinely require agencies to search for records, rejecting the notion that a FOIA request can be facially exempt.

### A. The NSA Has Asserted No Factual or Logical Arguments to Contest EPIC's Contention That Non-Exempt Records Exist and Must Be Disclosed

The NSA's response and affidavit is implausible and unreasonable given the records described in EPIC's FOIA Request. EPIC sought: (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. The second category of documents would include unsolicited communications from Google to the NSA, and the NSA has not contradicted EPIC's construction of the request.

In fact, the NSA acknowledged that EPIC's request included records that might "reveal information only about Google (and nothing about NSA)," and yet it maintains that the mere existence or nonexistence of those records would satisfy the criteria of Section 6 of the NSA Act. Br. of Appellee at *22. The NSA's justification for this conclusion was that "those records, if maintained by the Agency, would still constitute evidence of some kind of relationship between Google and the NSA." *Id.* The NSA has failed to explain how the *mere existence or nonexistence* of an e-mail communication from a third party Government vendor would reveal any protected *function* or *activity* of the Agency itself. Indeed, under the Agency's theory, the government could make the same assertion with respect to the current shipping rates for FedEx or UPS, assuming such records were in possession of the Agency and sought under the FOIA.

While the NSA may or may not communicate with Google as part of its Information Assurance mission, EPIC's FOIA Request clearly includes documents not relevant to that mission, as well as documents that could only reveal information that the NSA has already publicly disclosed. The NSA mischaracterizes EPIC's FOIA Request by stating that responsive documents would reveal "information about a potential Google-NSA relationship." Br. of Appellee at *10. While one category of documents sought by EPIC related specifically to a Google-NSA relationship ("records concerning an agreement or similar basis for collaboration…between the NSA and Google"), EPIC's FOIA Request includes requests for records that do not.[2]

The NSA's argument, that disclosure of the mere existence or nonexistence of requested communications would *reveal functions or activities of the NSA* as defined under Section 6, fails as to the most obvious responsive document to

[2] EPIC requested "records of communication between NSA and Google concerning Gmail." JA 0016. The NSA's argument rests on an unsupported construction of the phrase "communications between." Depending on the nature of the conversation, the NSA may have contacted Google and both sides may have responded. However, the NSA fails to consider that Google may have communicated with the NSA in an unsolicited manner that reveals nothing about the NSA's functions and activities. *See* Br. of Appellee at *21 ("NSA explained that it would only communicate with Google…if NSA discovered a vulnerability…that posed a threat to U.S. government information systems.").

EPIC's FOIA Request: an e-mail message from Google regarding the China Gmail hack.[3] The Request describes the circumstances surrounding the attack on Google's "corporate infrastructure, [including Gmail]" from China. *See* JA 0014. The second category of documents requested includes "all records of communication … concerning Gmail, including but not limited to Google's decision to fail to routinely encrypt Gmail messages…." *Id.* Thus, any e-mail sent from Google to the NSA containing the terms "Gmail" and "encrypt" would clearly be responsive to the EPIC FOIA Request, though the *mere existence or nonexistence of* such records would not reveal the Agency's functions or activities.[4] The existence of an e-mail does not reveal any information about (1) the

[3] The factual basis for the existence of this (and other) responsive, non-exempt documents is set out in EPIC's FOIA Request: "sources told the Post that 'Google approached the NSA shortly after the attacks.'" JA 0015 (citing Ellen Nakashima, *Google to Enlist NSA to Help It Ward Off Cyberattacks*, Washington Post, Feb. 4, 2010, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR2010020304057.html). As the Request indicated, several major news articles were published around the time that Google was hacked. JA 0015 (citing Siobhan Gorman & Jessica E. Vascellaro*, Google Working With NSA to Investigate Cyber Attack*, Wall St. J., Feb. 4, 2010).

[4] The NSA challenges EPIC's argument that information about the *mere existence or nonexistence* of an unsolicited communication from Google cannot be exempt under Section 6 and FOIA Exemption 3 because such information would not cause any harm to the NSA's Information Assurance mission. The NSA argues, "any suggestion that NSA is required to demonstrate harm to national security is mistaken." Br. of Appellee at *24. However, the Agency goes on to justify EPIC's claim, citing this Court, "Congress has already, in enacting the statute, decided that disclosure of NSA activities is potentially harmful." *Id.* (citing *Hayden v. NSA*, 608 F.2d 1381, 1390 (D.C. Cir. 1979)). Since EPIC's key assertion is that information about the *existence of* documents responsive to EPIC's FOIA Request would not

NSA's response or (2) the NSA's relationship with that entity. It only reveals that some communication, responsive to EPIC's FOIA request, is in possession of the Agency and subject to disclosure under the FOIA.

If Section 6 is interpreted so broadly as to prevent acknowledgement of the *mere existence or nonexistence* of such an e-mail, then the kind of "unduly broad construction" that this Circuit warned of in *Founding Church of Scientology*, 610 F.2d at 827, will have been realized. Even the NSA has not previously taken such a broad view of Section 6; the NSA regularly responds to FOIA requests with documents, redacted documents, and lists of withheld documents. *See, e.g., Larson v. Dep't of State*, 565 F.3d 857, 860 (D.C. Cir. 2009); *Students Against Genocide v. Dep't of State*, 257 F.3d 828, 837 (D.C. Cir. 2001), *Hayden v. NSA*, 608 F.2d 1381, 1383 (D.C. Cir. 1980); *Founding Church of Scientology*, 610 F.2d at 834. In *Larson,* the Agency withheld documents pursuant to FOIA Exemptions 1 and 3, and asserted *Glomar* in response to a single category of documents. 565 F.3d at 865-66.

### B. The Disclosure of Responsive, Non-Exempt Records Would Not Reveal Information About the NSA's Functions or Activities

There are four potential outcomes that would follow from the NSA's search for documents responsive to EPIC's FOIA Request: (1) the NSA would not

reveal any NSA functions or activities, that information does not implicate the "harm" contemplated by Congress. Thus, the NSA has no basis to assert *Glomar* as to that category of innocuous documents.

uncover any responsive documents, (2) the NSA would uncover documents responsive to EPIC's FOIA Request, all of which implicate the NSA's functions and activities, (3) the NSA would uncover documents that are responsive to EPIC's FOIA Request and none of the documents implicate the NSA's functions or activities, or (4) the NSA would uncover documents responsive to EPIC's FOIA Request, some of which implicate the NSA's functions and activities and some that do not.

In scenario (1), the Agency could simply respond that no responsive documents were located. In scenario (2), the Agency could assert the *Glomar* response, as the acknowledgement of the existence or non-existence of these records would *necessarily* implicate the functions and activities of the Agency, and could be exempt (if the Agency chooses to assert the exemption, which is permissive as per the statute) under Section 6 of the NSA Act. In scenario (3), the Agency could simply provide the documents requested.

It is scenario (4) that is now before this Court. The Agency is in possession of records responsive to the EPIC's FOIA Request, some of which implicate the functions and activities of the Agency, others of which do not. The Agency's declaration is conclusory to the extent that it seeks to shoehorn all of the records sought into category 2, thereby assuming the outcome it desires: that all of the records sought would *necessarily* reveal functions and activities of the Agency.

### C. The District Court Considered Only the Government's Activities, Failing to Consider the Activities of Companies and the Impact on Internet Users

In relying on the Janosek Declaration, the District Court placed disproportionate weight on the Agency's assertion that the Information Assurance mission pertains solely to safeguarding the security interests of the federal government. In so doing, the Court failed to acknowledge that EPIC's FOIA Request concerned the interests of private users of Google services, completely unrelated to the activities of the federal government.

As a consequence, the District Court cast the blanket of matters that the NSA may have "considered to be of consequence for critical U.S. government information systems," JA 0113, over records that may have had nothing whatsoever to do with government information systems. Such records would not reveal the NSA's functions and activities and would not be properly subject to Exemption 3 and Section 6 of the NSA Act. Of course, such a determination could have been made if the Agency first located records and undertook a segregability analysis, as urged by EPIC, before asserting a *Glomar* response.

The government in its opposition argues that the NSA's Information Assurance mission tasks the Agency with "protecting national security information systems," Br. of Appellee at *11. Yet the Agency through the Information Assurance mission also currently provides, on a publicly accessible website, "Best

Practices for Securing a Home Network." BEST PRACTICES FOR KEEPING YOUR HOME NETWORK SECURE (National Security Agency 2011), *available at* http://www.nsa.gov/ia/_files/factsheets/Best_Practices_Datasheets.pdf. There is nothing in law to suggest that a home computer network is considered a "national security information system" nor should the Agency be permitted to extend its legitimate assertion of a statutory exemption to activities that clearly fall outside the Agency mission.

The fact that such records could have been disclosed by the Agency is further evidence that the Janosek Declaration was insufficient to resolve the matter before the court.

## II. Because EPIC's FOIA Request Seeks Records That Are Non-Exempt, the NSA Must Perform a Search

### A. The NSA Cannot Justify the Agency's Refusal to Conduct a Search for Records Concerning its Information Assurance Mission by Relying on Precedent Concerning the Agency's Intelligence Gathering Activities

The NSA contends that EPIC's FOIA Request is facially exempt from FOIA because it covers *only* materials that satisfy the criteria of Section 6 of the NSA Act, and that "acknowledging whether or not responsive records exist in this case would disclose information protected by that statutory provision." Br. of Appellee at *19. In support of this contention, the NSA relies on the deference granted by Congress in Section 6, but this argument does not speak to EPIC's core point, that some of the materials requested relate to third party activities, the existence of which could not possibly reveal NSA *functions* or *activities*. The NSA also argues that its own judgment as to the application of Section 6 is owed "substantial weight," citing *Students Against Genocide*, 257 F.3d 840, but the NSA still bears the burden of demonstrating that "the information withheld logically falls within the claimed exemption," *Larson*, 565 F.3d at 865, and the NSA has failed to do so.

The NSA's reliance on *Wilner* and *Larson* for the proposition that "Section 6's coverage is quite broad," Br. of Appellee at *19, is misplaced in this case. Both of those cases involved requests for records relating to the NSA's "classified intelligence gathering" activities and sources, *id*. at 868-69. As the court in *Larson* made clear, "it is logical to conclude that the need to assure confidentiality of a foreign source includes neither confirming nor denying the existence of records…." *Larson*, 565 F.3d at 864 (citing *Wolf v. CIA*, 473 F.3d 370, 377 (D.C. Cir. 2007). The need for secrecy in intelligence gathering is well established. *See CIA v. Sims*, 471 U.S. 159 (1985) (discussing passage of the National Security Act of 1947). This Circuit has said, "[t]here can be no doubt that the disclosure of [Signals Intelligence ("SIGINT")] reports would reveal information concerning the activities of the agency." *Linder v. NSA*, 94 F.3d 693, 696 (D.C. Cir. 1996). However, the same logic does not apply to the NSA's Information Assurance mission, as described in the NSA's affidavit, and no court has upheld such a broad assertion of Section 6 with respect to that mission. The mere existence or nonexistence of communications with information systems providers does not implicate any specific NSA activities or functions that have not already been disclosed in the NSA's affidavit.

The *Glomar* doctrine is clearly applicable in the foreign intelligence-gathering context. The NSA is charged with "collecting, processing, and disseminating [SIGINT] information for national foreign intelligence purposes." *Wilner v. NSA*, 592 F.3d 60, 65 (2nd Cir. 2009). Information about the mere existence or nonexistence of records relating to the NSA's SIGINT activities can act "much like a piece of [a] jigsaw puzzle, each detail may aid in piecing together other bits of information even when the individual piece is not of obvious importance in itself." *Larson*, 565 F.3d at 864 (citing *Gardels v. CIA*, 689 F.2d 1100, 1106 (D.C. Cir. 1982)). For example, the existence or nonexistence of agency records relating to the abduction and disappearance of a Guatemalan family in 1981 would reveal that the NSA did, or did not, gather such records through its intelligence sources. *See, e.g., id. at* 861.

The NSA's Information Assurance mission, on the other hand, is not analogous to the complex, and necessarily secret, "jigsaw puzzle" of its SIGINT mission. Under the NSA's Information Assurance mission, the Agency is "charged with protecting Department of Defense and other national-security information systems," as well as other "critical" government information systems. JA 0048. This mission involves "vulnerability discovery and testing," participating in various public-private initiatives, monitoring "malicious activity and, where possible, malicious actors." JA 0049.

The NSA plainly acknowledges in its affidavit that its mission includes investigating vulnerabilities in "commercial technology for [U.S. government] information systems." *Id.* The U.S. government uses Google applications. *See, e.g.,* Product Detail, Google Apps for Government, Apps.Gov, U.S. General Services Administration (Feb. 13, 2012).[5] None of this is a secret. Indeed, the fact that the NSA is investigating security vulnerabilities in Google's commercial products, used by the Government, is publicly acknowledged in the Agency's own affidavit. *See* JA 0052. In fact, the NSA has already stated *on its public website* that it considers the routine deployment of SSL, which Google failed to do prior to January 2010, to be a best practice. *See* BEST PRACTICES FOR KEEPING YOUR HOME NETWORK SECURE 1, 5 (National Security Agency 2011) (explaining that cyber threats are widespread and asserting that "web-based applications such as browsers should be set to force the use of SSL.").

[5] *Available at* https://www.apps.gov/cloud/catalog/product_detail.do?contractNumber=GS-35F-0460X&itemNumber=GAPPSPREM1USER12MO.

In order to satisfy the *Glomar* requirements, the mere existence or nonexistence of responsive records relating to the NSA's Information Assurance mission must reveal more than what is publicly acknowledged by the NSA. *See Wolf v. CIA*, 473 F.3d 370, 379 (D.C. Cir. 2007) ("In the *Glomar* context, then, if the prior disclosure establishes the *existence* (or not) of records responsive to the FOIA request, the prior disclosure necessarily matches both the information at issue-the existence of records-and the specific request for that information."). Insofar as the NSA argues for a broad application of Section 6 in regard to its Information Assurance mission, the Agency's stance is inconsistent with its public disclosures on the same subject matter. *See* Janosek Declaration, JA 0047-0054; BEST PRACTICES FOR KEEPING YOUR HOME NETWORK SECURE (National Security Agency 2011).

The mere existence or nonexistence of communications records with a government information services vendor simply does not implicate the same secrecy concerns as the NSA's intelligence reports. Technical information that might be routinely transmitted by a commercial vendor to the Agency, posted on the Internet, and also made available to millions of users of a product, simply cannot be analogized to highly subjective reports prepared in a classified setting as part of the Agency's intelligence gathering function.

The NSA's ultimate argument, that the court should give "substantial weight" to its judgment, Br. of Appellee at *22, is unavailing where it clearly fails to acknowledge the existence of records that would be subject to disclosure. Even in *Students Against Genocide*, 257 F.3d 828, the Agency identified responsive records to plaintiff's request, released certain segregable portions, withheld other exempt portions, and issued a *Glomar* response as to certain classes of documents. Such a response clearly deserves the "substantial weight" that the court granted, but that is not the case here. In response to EPIC's request, the NSA refused to even perform a search for records. JA 0051. The Agency asserted an interpretation of Section 6 that would, for the first time, cover the existence or nonexistence of *third party records* relating to commercial services.

### B. The NSA's Refusal to Conduct a Search Denies the Court of the Opportunity to Meaningfully Review Agency Action

The NSA argues that the Janosek Declaration is sufficient to support the Agency's *Glomar* assertion. Br. of Appellee at *29. The District Court relied on the Janosek Declaration in upholding the *Glomar* response. *EPIC v. NSA*, 798 F. Supp. 2d 26, 31 (D.D.C. 2011). However, the Janosek Declaration is insufficient because the declaration does not tether the NSA's *Glomar* assertion to a document or category of documents. Furthermore, the Janosek Declaration is insufficient because it provides neither "logical" nor "plausible" arguments as to how the *mere* *existence or nonexistence* of a communication from Google can reveal the NSA's functions and activities. *See Larson*, 565 F.3d at 862.

The Janosek Declaration acknowledges that the Agency refused to perform a search in response to EPIC's FOIA request, JA 0051; Janosek Decl. at ¶ 10, such a refusal is evidence of bad faith. The Agency relies on *Larson* for the proposition that a *Glomar* assertion can be proper absent a search. Br. of Appellee at *29. But the D.C. Circuit upheld the *Glomar* response in *Larson* only after the Agency performed a search for responsive records, determined that those records (or category of nonexistent records) was exempt under the FOIA, and determined that the FOIA exemption supported the Agency's *Glomar* response. *Larson*, 565 F.3d at 861-62. ) Indeed, *Larson* is typical of the cases in which courts uphold *Glomar* responses – it involves a search as the necessary predicate to a sufficient declaration. *E.g.* Motion for Summary Judgment by National Security Agency, Attachment 3 to Pet'r's Opening Br. at 5, *People for the American Way Foundation*, 462 F.Supp.2d 21 (D.C. Cir. May 5, 2006) (No. 06-00206); *Founding Church of Scientology*, 610 F.2d at 825-26; *Moore v. Bush*, 610 F. Supp. 2d 6, 15 (D.D.C. 2009). Unsupported by a search, the Janosek Declaration does not provide the good faith factual basis necessary to support the Agency's claim that Exemption 3 applies to the records sought by EPIC's FOIA Request.

Critically, reliance on the Janosek Declaration, absent a search for records, deprives the court of the ability to meaningfully assess the propriety of the Agency's *Glomar* assertion. The law of this Circuit requires courts to develop as full a record as possible when assessing agency withholdings and *Glomar* responses. *See Phillipi v. CIA*, 546 F.2d 1009, 1013 (D.C. Cir. 1976). Congress has directed "that in reviewing agency rejections of Freedom of Information Act requests, the court…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 in subsection (b)." *Founding Church of Scientology*, 610 F.2d at 830.

In reviewing agency action, "[t]he court is to require the agency to create as full a public record as possible." *Hayden*, 608 F.2d at 1384. If the Court is not satisfied with the record created, "the court may accept classified affidavits In camera, or it may inspect the documents In camera." *Id*. An agency is required to provide documents for In camera review upon request of the Court. *Founding Church of Scientology*, 610 F.2d 824. In FOIA cases, additional information is often requested or offered by the Agency in order to supplement the record and supply additional information. *See id*. (compelling agency to file a supplemental affidavit and twenty-page classified affidavit for In camera review); *Nation Magazine, Washington Bureau v. United States Customs Service*, 71 F.3d 885

(D.C. Cir. 1995) (remanding to District Court and requiring further affidavits). This requirement is also true in cases against the NSA where the Agency invoked Section 6 authority to withhold documents and the Agency affidavits made up the entirety of the record for the Court. *Founding Church of Scientology*, 610 F.2d 824 (remanding to District Court based on insufficiency of the proffered affidavit to allow the NSA to submit more detailed public or classified affidavits).

## 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: February 16, 2012

## TYPE/VOLUME CERTIFICATE OF COMPLIANCE WITH RULE 32(a)

I hereby certify that the foregoing reply 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). EPIC's reply brief contains 4,333 words.

___*/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 16th day of February 2012, he caused the foregoing brief to be served by ECF and two hard copies by first-class mail, postage prepaid, on the following:

___*/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*