


## Electronic Privacy Information Center v. National Security Agency: How Glomar Responses Benefit Businesses and Provide an Epic Blow to Individuals

Joshua R. Chazen

Follow this and additional works at: <http://digitalcommons.law.umaryland.edu/jbtl>

 Part of the [Administrative Law Commons](#), [Banking and Finance Law Commons](#), [Business and Corporate Communications Commons](#), [Communications Law Commons](#), [Defense and Security Studies Commons](#), [First Amendment Commons](#), [Internet Law Commons](#), [National Security Law Commons](#), [President/Executive Department Commons](#), [Privacy Law Commons](#), and the [Technology and Innovation Commons](#)

---

### Recommended Citation

Joshua R. Chazen, *Electronic Privacy Information Center v. National Security Agency: How Glomar Responses Benefit Businesses and Provide an Epic Blow to Individuals*, 9 J. Bus. & Tech. L. 315 (2014)

Available at: <http://digitalcommons.law.umaryland.edu/jbtl/vol9/iss2/8>

This Notes & Comments is brought to you for free and open access by the Academic Journals at DigitalCommons@UM Carey Law. It has been accepted for inclusion in Journal of Business & Technology Law by an authorized editor of DigitalCommons@UM Carey Law. For more information, please contact [smccarty@law.umaryland.edu](mailto:smccarty@law.umaryland.edu).

## *Electronic Privacy Information Center v. National Security Agency*: How *Glomar* Responses Benefit Businesses and Provide an Epic Blow to Individuals

IN *ELECTRONIC PRIVACY INFORMATION CENTER v. NATIONAL SECURITY AGENCY*,<sup>1</sup> the United States Court of Appeals for the District of Columbia Circuit reviewed the issuance of a *Glomar* response<sup>2</sup> by the National Security Agency<sup>3</sup> (“NSA”) in response to a Freedom of Information Act<sup>4</sup> (“FOIA”) request submitted to the NSA by the Electronic Privacy Information Center<sup>5</sup> (“EPIC”).<sup>6</sup> The district court granted the NSA’s motion for summary judgment because an NSA affidavit supported the claim that the information sought by EPIC pertained to the NSA’s functions or activities.<sup>7</sup> The information sought by EPIC was protected under Section 6 of the

---

© 2014 Joshua R. Chazen

\* J.D. Candidate, University of Maryland Francis King Carey School of Law, 2014; B.B.A., University of Miami, 2011. I would like to thank my *Journal of Business & Technology Law* colleagues, past and present; in particular, I would like to thank my note editors, Paul H. Farmer, Jr., Whitney Levandusky, and Zachary K. Ostro, for their feedback during the writing process. Additionally, I would like to thank Professors Michelle Harner and James Grimmelmann and Hilary Hansen for their support as faculty advisors. I dedicate this note to my family for their love and support prior to and during law school. Lastly, I would like to thank Beverly Klyn, my ninth grade English teacher, high school yearbook advisor, and first mentor, for teaching me the power that can come from a pen, piece of paper, and an analytical mind; without your support, encouragement, and unwillingness to give up on me when so many others did, I would not be where I am today.

1. 678 F.3d 926 (D.C. Cir. 2012).
2. A *Glomar* response is when an agency neither confirms nor denies the existence of records. *Infra* Part II.C.
3. For more information on the NSA, see <http://www.nsa.gov/>.
4. 5 U.S.C. § 552 (2012).
5. “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.” Brief for Appellant at i, *Elec. Privacy Info. Ctr. v. Nat’l Sec. Agency*, 678 F.3d 926 (D.C. Cir. 2012) (No. 11-5233).
6. *Elec. Privacy Info Ctr.*, 678 F.3d at 929.
7. *Id.* at 930 (quoting *Elec. Privacy Info. Ctr. v. Nat’l Sec. Agency*, 798 F. Supp. 2d 26, 31–32 (D.D.C. 2011)).

National Security Agency Act of 1959<sup>8</sup> (“NSA Act”), which prohibits the release of information relating to the organization, function, or activities of the NSA.<sup>9</sup> The issue before the D.C. Circuit was whether the material withheld by the NSA satisfied an exemption under FOIA.<sup>10</sup>

The court held that the NSA’s *Glomar* response sufficiently satisfied the exemption requirements of the Act because threat assessment is an undisputed function of the NSA and, therefore, the NSA was not required to confirm or deny existence of any responsive records.<sup>11</sup> Although the D.C. Circuit had a sound legal basis in making its ruling, the court’s holding should have been more narrowly tailored.<sup>12</sup> While the court’s holding creates a positive effect on the ability of federal agencies and businesses to work together to handle cyber threats encountered in the private sector,<sup>13</sup> it does not properly balance this relationship with the goals of FOIA and the public’s ability to trust businesses protecting its personal information.<sup>14</sup>

## I. THE CASE

In January 2010, Google, Inc. (“Google”) was victim to a cyber attack<sup>15</sup> directed at Gmail<sup>16</sup> accounts belonging to Chinese human rights activists.<sup>17</sup> Soon after the cyber attack, Google opted to change the privacy settings of Gmail so all incoming

---

8. Section 6 states:

(a) Except as provided in subsection (b) of this section, nothing in this Act or any other law (including, but not limited to, the first section and section 2 of the NSA Act of August 28, 1935 (5 U.S.C. 654) (repealed by Pub. L. 86-626, title I, Sec. 101, July 12, 1960, 74 Stat. 427)) 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 NSA Activities thereof, or of the names, titles, salaries, or number of the persons employed by such agency.

(b) The reporting requirements of section 1582 of title 10, United States Code, shall apply to positions established in the National Security Agency in the manner provided by section 4 of this Act.

National Security Agency Act, P.L. No. 86-36, 73 Stat. 63, codified at 50 U.S.C. § 402 note (2013).

9. *Elec. Privacy Info. Ctr.*, 678 F.3d at 930.

10. *Id.* at 931. See also *infra* Part II.A.2.

11. *Elec. Privacy Info. Ctr.*, 678 F.3d at 934–35.

12. See *infra* Part IV.

13. See *infra* Part IV.A.

14. See *infra* Part IV.B.

15. “A cyber attack consists of any action taken to undermine the functions of a computer network for a political or national security purpose.” Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 826 (2012).

16. For a brief description on the Google suite of products and services, including Gmail, see Michael Zimmer, *Privacy on Planet Google: Using the Theory of “Contextual Integrity” to Clarify the Privacy Threats of Google’s Quest for the Perfect Search Engine*, 3 J. BUS. & TECH. L. 109, 121–22 (2008).

17. Timothy Thomas, *Google Confronts China’s “Three Warfares”*, PARAMETERS, Summer 2010, 101, 101.

and outgoing traffic from its servers was automatically encrypted.<sup>18</sup> Google notified other companies potentially affected by the cyber attack and stated it was working with U.S. authorities to determine the source of the attack.<sup>19</sup> In February 2010, both the Wall Street Journal and Washington Post reported that Google contacted the NSA after the cyber attack.<sup>20</sup> The Washington Post also reported, based on comments by former NSA director Mike McConnell, that the NSA’s collaboration with private companies was “inevitable.”<sup>21</sup> EPIC submitted its FOIA request to the NSA on February 4, 2010, which requested:

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.*<sup>22</sup>

The NSA responded to the request on March 10, 2010,<sup>23</sup> invoking Exemption 3 of FOIA and Section 6 of the Act by issuing a *Glomar* response.<sup>24</sup> The *Glomar* response meant that the NSA “neither confirmed nor denied the existence of any responsive records.”<sup>25</sup> EPIC filed an administrative appeal, stating that the “NSA’s response was unlawful” because the NSA failed to issue factual support that the documents requested by EPIC fell within Section 6, which broadly prohibits the

---

18. Joe Wolverton, II, *Is the NSA Using Google to Spy on Account Holders?*, NEW AM. (May 18, 2012, 6:36 AM), <http://www.thenewamerican.com/usnews/constitution/item/11428-is-the-nsa-using-google-to-spy-on-account-holders>.

19. David Drummond, *A New Approach to China*, OFFICIAL GOOGLE BLOG (Jan. 12, 2010), <http://googleblog.blogspot.com/2010/01/new-approach-to-china.html>; see also Thomas, *supra* note 17, at 103 (reporting that Adobe Systems, Rackspace Hosting, CyberSitter, Gipson Hoffman & Pancione, Juniper Networks, Northrop Grumman, Yahoo, and Dow Chemical were hit by the attackers).

20. Siobhan Gorman & Jessica Vascellaro, *Google Working With NSA to Investigate Cyber Attack*, WALL ST. J., Feb. 4, 2010, <http://online.wsj.com/article/SB10001424052748704041504575044920905689954.html>; Ellen Nakashima, *Google to Enlist NSA to Ward Off Attacks*, WASH. POST, Feb. 4, 2010, at A01.

21. Mike McConnell, *How to Win the Cyber-War We’re Losing*, WASH. POST, Feb. 28, 2010, <http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html>.

22. Brief for Appellant at 7, *Elec. Privacy Info. Ctr. v. Nat’l Sec. Agency*, 678 F.3d 926 (D.C. Cir. 2012) (No. 11-5233).

23. *Id.*

24. *Id.*

25. *Id.*

disclosure of information pertaining to the organization, function, or activities of the NSA.<sup>26</sup>

Prior to the resolution of the administrative appeal, EPIC filed suit in the D.C. Circuit to challenge the NSA's *Glomar* response.<sup>27</sup> EPIC and the NSA both moved for summary judgment.<sup>28</sup> The NSA's motion for summary judgment included a declaration by NSA Deputy Associate Director for Policy and Records, Diane M. Janosek ("Janosek Declaration").<sup>29</sup> The district court granted the NSA's motion for summary judgment because the Janosek Declaration was "logical and plausible" and had "sufficient detail, pursuant to Section 6, to support the NSA's claim that the protected information" deals with the NSA's organization, functions, or activities.<sup>30</sup> On appeal, the D.C. Circuit attempted to determine whether the NSA's acknowledgement of the existence or nonexistence of the EPIC-requested material would reveal a function or activity of the NSA.<sup>31</sup>

## II. LEGAL BACKGROUND

The issue in *Electronic Privacy Information Center* was whether the NSA could issue a *Glomar* response in regard to EPIC's FOIA request for records pertaining to the agency's communications with Google.<sup>32</sup> The interplay of the Freedom of Information Act,<sup>33</sup> the National Security Agency Act of 1959,<sup>34</sup> and the *Glomar* response<sup>35</sup> was instrumental to the D.C. Circuit's decision.

### A. The Freedom of Information Act

#### 1. Overview

The major tenet of FOIA is that it gives the public access to government-held information.<sup>36</sup> FOIA was the first law to give Americans a right to records of federal agencies.<sup>37</sup> Under FOIA, a request can be made for any agency record.<sup>38</sup> "[A]s the

26. *Id.*

27. *Elec. Privacy Info. Ctr. v. Nat'l Sec. Agency*, 798 F. Supp. 2d 26, 29 (D.D.C. 2011).

28. *Id.*

29. Joint Appendix at 47, *Elec. Privacy Info. Ctr. v. Nat'l Sec. Agency*, 678 F.3d 926 (D.C. Cir. 2012) (No. 11-5233).

30. *Elec. Privacy Info. Ctr. v. Nat'l Sec. Agency*, 678 F.3d 926, 930 (D.C. Cir. 2012) (quoting *Elec. Privacy Info. Ctr.*, 798 F. Supp. 2d at 31-32).

31. *Id.* at 931.

32. *Id.*

33. *See infra* Part II.A.

34. *See infra* Part II.B.

35. *See infra* Part II.C.

36. Edward A. Tomlinson, *Use of the Freedom of Information Act for Discovery Purposes*, 43 MD. L. REV. 119, 120 (1984).

37. *History of the Freedom of Information Act*, PBS, <http://www.pbs.org/now/politics/foia.html> (last visited Feb. 26, 2014).

law that keeps citizens in the know about their government,”<sup>39</sup> FOIA’s roots are embedded in traditional American principles of democracy, allowing access to information unless it is protected from public disclosure.<sup>40</sup> Since its enactment in 1966, the statute has undergone various changes.<sup>41</sup> What has remained constant, however, are the nine exemptions that agencies often utilize when responding to FOIA requests.<sup>42</sup> Since the Executive Branch oversees FOIA, each administration

---

38. *What is FOIA?*, <http://www.foia.gov/about.html> (last visited Feb. 26, 2014).

39. *Id.*

40. *Id.*

41. Karen Saunders, *History of the Freedom of Information Act*, DREXEL UNIV., [http://www.cis.drexel.edu/faculty/shelfer/public\\_html/busrefpapers/foiahis.htm](http://www.cis.drexel.edu/faculty/shelfer/public_html/busrefpapers/foiahis.htm) (last visited Feb. 26, 2014); *see also History of FOIA*, ELEC. FRONTIER FOUND., <https://www.eff.org/issues/transparency/history-of-foia> (last visited Feb. 26, 2014) (“Congress amended FOIA to become the bill that it is today” in 1974).

42. The nine exemptions apply to records that are:

(1)

(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and

(B) are in fact properly classified pursuant to such Executive order;

(2) related solely to the internal personnel rules and practices of an agency;

(3) specifically exempted from disclosure by statute (other than section 552b of this title [5 USCS § 552b]), 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 [enacted Oct. 28, 2009], specifically cites to this paragraph.

(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the

takes a different stance on how agencies should handle FOIA requests.<sup>43</sup> FOIA applies to executive branch government agencies, which include the Central Intelligence Agency, Department of State, Federal Election Commission, United States Postal Service, and Department of Defense (which has numerous agencies, including the NSA, under its umbrella).<sup>44</sup> All agencies receive different numbers of FOIA requests; for example, the NSA received 1,809 FOIA requests during Fiscal Year 2012, as compared to 3,745 requests and 60 requests to the CIA and FEC, respectively.<sup>45</sup>

The intent of Congress in adopting FOIA was to end the policy of withholding, rather than releasing, government-held information.<sup>46</sup> Before FOIA was adopted, executive agencies were able to prevent information from being disclosed to the public due to lax policies under the Administrative Procedure Act.<sup>47</sup> After FOIA was adopted, an agency receiving a FOIA request would: (1) release the requested records; (2) inform the individual that the requested records do not exist; or (3) determine that, even though the requested records exist, one of the exemptions applied and therefore the FOIA request cannot be granted.<sup>48</sup>

---

identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;

(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(9) geological or geophysical information and data, including maps, concerning wells.

5 U.S.C. § 552(b) (2012).

43. *History of FOIA*, *supra* note 41.

44. FOIA, <http://www.foia.gov/data.html> (last visited Feb. 26, 2014).

45. *Id.*

46. H.R. REP. NO. 89-1497, 2d Sess. 2 (1966); S. REP. NO. 89-813, 1st Sess. (1965) (stating the objective of FOIA is allowing for the fullest disclosure possible, so long as the disclosure is responsible).

47. See Jill Nylander, *The Administrative Procedure Act*, MICH. BAR. J. 38 (Nov. 2006).

48. 5 U.S.C. § 552(a) (2012).

## 2. Exemption 3 of FOIA

Although agencies utilize all nine FOIA exemptions, the only exemption relevant to the case is Exemption 3 of FOIA.<sup>49</sup> Exemption 3 protects information that other federal statutes require or permit to be withheld from release under FOIA by incorporating all federal nondisclosure statutes.<sup>50</sup> As a result, FOIA incorporates the National Security Agency Act of 1959, which permits the NSA to withhold information pertaining to the functions or organization of the NSA as well as certain information pertaining to NSA employees.<sup>51</sup>

One of the first cases to review the scope of Exemption 3 of FOIA was *Gardels v. CIA*,<sup>52</sup> in which the D.C. Circuit addressed whether the CIA may say whether it had covert contacts at the University of California without damaging the confidentiality of its intelligence sources.<sup>53</sup> The D.C. Circuit established that the applicable test is “whether on the whole record[,] the Agency’s judgment objectively survives the test of reasonableness, good faith, specificity, and plausibility in this field of foreign intelligence in which the CIA is expert and given by Congress a special role.”<sup>54</sup> The main takeaway from FOIA disputes is that a court will not argue with an agency’s decision to invoke an exemption so long as it is “logical” or “plausible.”<sup>55</sup>

## 3. Official Acknowledgment Doctrine

When challenging an agency’s decision to issue a *Glomar* response, plaintiffs often center their claims on a specific theory: if an agency disclosed information to the

49. 5 U.S.C. § 552(b)(3) (2012). Exemption 3, as amended, allows agencies to not disclose information if supported by a federal statute that, “(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.” *Id.*

50. Office of Info. Policy, U.S. Dep’t of Justice, Statutes Found to Qualify Under Exemption 3 of the FOIA, available at <http://www.justice.gov/oip/exemption3.pdf>.

51. *Id.*; see also *Larson v. Dep’t of State*, 565 F.3d 857, 868–69 (D.C. Cir. 2009).

52. 689 F.2d 1100 (D.C. Cir. 1982).

53. *Id.* at 1104. In representing its position, the CIA stated that admitting it had covert contact at UCLA or any other University of California campus would give foreign intelligence agencies the opportunity to identify exactly what the nature of those relationships were. *Id.* The D.C. Circuit was also concerned with the fact that “[t]he CIA has received more than 125 similar FOIA requests for information on covert contacts with American colleges and universities—covering about 100 different schools. If the Agency were required to indicate those schools with which it had had no covert contact, the work of foreign intelligence bodies would obviously be much easier; they could and would concentrate their efforts on the remaining American colleges and universities, and their sphere of activity could be appreciably narrowed.” *Id.*

54. *Id.* at 1105. Based on this test, as well as common law precedent, the D.C. Circuit accepted the CIA’s judgment because the CIA met the burden of proving that it maintained appropriate judgment in its decision that to divulge or acknowledge covert contacts with UCLA would disclose some foreign intelligence procedures. *Id.*; see also *Halperin v. CIA*, 629 F.2d 144, 149 (D.C. Cir. 1980) (“[T]he purpose of national security exemptions to the FOIA is to protect intelligence sources before they are compromised and harmed, not after. . .”).

55. *Larson*, 565 F.3d at 862 (quoting *Wolf v. CIA*, 473 F.3d 370, 374–75 (D.C. Cir. 2007)); *Gardels*, 689 F.2d at 1105; *Hayden v. Nat’l Sec. Agency*, 608 F.2d 1381, 1388 (D.C. Cir. 1979).



public, then the agency cannot protect that information through a *Glomar* response.<sup>56</sup> The D.C. Circuit has made clear that “when information has been ‘officially acknowledged,’ its disclosure may be compelled even over an agency’s otherwise valid exemption claim.”<sup>57</sup>

For the court to recognize that an agency officially acknowledged information, three criteria must be met.<sup>58</sup> The three criteria are set as requirements “because they acknowledge the fact that in the arena of intelligence and foreign relations there can be a critical difference between official and unofficial disclosures.”<sup>59</sup> For *Glomar* responses, if any prior disclosure establishes the existence or nonexistence of records responsive to a FOIA request, the prior disclosure will be regarded as an official acknowledgement.<sup>60</sup> Official acknowledgment does not include mere public speculation, even if the media heavily reports the information.<sup>61</sup>

## B. National Security Agency Act of 1959

### 1. Overview

The NSA Act provides that the Secretary of Defense will appoint officers and employees of the NSA to ensure the functions of the NSA are carried out and outlines the powers and duties of the NSA director.<sup>62</sup> The NSA Act initially did not describe the functions of the NSA, but dealt with other matters such as pay, training, acquisitions, and leasing.<sup>63</sup> The NSA Act has been amended and its current version serves as the statutory basis for various NSA personnel policies.<sup>64</sup> The NSA Act allows the NSA to serve as a vital safeguard in ensuring that America is protected.<sup>65</sup>

56. *Wolf*, 473 F.3d at 378 (appellant asserting that CIA waived its right to use FOIA Exemptions 1 and 3 because it officially acknowledged the existence of records in a congressional testimony nearly six decades prior).

57. *Fitzgibbon v. CIA*, 911 F.2d 755, 765 (D.C. Cir. 1990).

58. *Id.* (citing *Afshar v. Dep’t of State*, 702 F.2d 1125, 1133 (D.C. Cir. 1983)) (“First, the information requested must be as specific as the information previously released. Second, the information requested must match the information previously disclosed. . . . Third, . . . the information requested must already have been made through an official and documented disclosure.”).

59. *Id.* (citing *Abbotts v. Nuclear Regulatory Comm’n*, 766 F.2d 604, 607–08 (D.C. Cir. 1985); *Military Audit Project v. Casey*, 656 F.2d 724, 742–45 (D.C. Cir. 1981); *Phillippi v. CIA*, 655 F.2d 1325, 1332–33 (D.C. Cir. 1981)).

60. *Wolf*, 473 F.3d at 379.

61. *Frugone v. CIA*, 169 F.3d 772, 774–75 (D.C. Cir. 1999) (supporting the rationale that the national media are not capable of waiving an agency’s statutory authority to protect information related to its functions and activities); *see also Afshar*, 702 F.2d at 1130.

62. National Security Agency Act, P.L. No. 86-36, 73 Stat. 63 (1959).

63. RICHARD A. BEST, JR., CONG. RESEARCH SERV., RL30740, THE NATIONAL SECURITY AGENCY: ISSUES FOR CONGRESS 16 (2001).

64. *Id.*

65. *See id.* at 18.

## 2. Section 6 of the NSA Act

No law shall be construed to require the disclosure of, inter alia, the functions or activities of NSA.<sup>66</sup> Despite this general policy, the FOIA office at the NSA aims to release as much information as possible.<sup>67</sup> However, the information being released cannot compromise the NSA's goal of protecting classified and sensitive information.<sup>68</sup>

The D.C. Circuit has addressed an NSA denial of a FOIA request after the NSA invoked the NSA Act and Exemption 3 of FOIA to move for dismissal of the proceeding or, alternatively, for summary judgment.<sup>69</sup> Critical in the D.C. Circuit's analysis in *Founding Church of Scientology* was its belief that Section 6 of the NSA Act is an Exemption 3 statute.<sup>70</sup> Section 6 states 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, of any information with respect to the activities thereof, or of names, titles, salaries, or number of the persons employed by such agency."<sup>71</sup> The D.C. Circuit recognized that the congressional intent in implementing the NSA Act was to preserve national security.<sup>72</sup> Thus, the D.C. Circuit interpreted Section 6 as a statute qualifying under Exemption 3, and, in certain situations, permits the NSA to withhold information.<sup>73</sup>

At a later date, the D.C. Circuit addressed a question it left open in *Founding Church of Scientology*: what is the proper scope to give to the exemption under the Act?<sup>74</sup> The D.C. Circuit answered this question by determining that the plain wording of the statute conclusively qualified the NSA Act as an Exemption 3 statute.<sup>75</sup> The D.C. Circuit held that, "where the function or activity is authorized by statute and not otherwise unlawful, NSA materials integrally related to that function or activity fall within [the Act] and Exemption 3."<sup>76</sup> The D.C. Circuit also held that

66. National Security Agency Act, P.L. No. 86-36, § 6, 73 Stat. 63 (1959).

67. See *Freedom of Information Act Handbook*, NSA/CSS, [http://www.nsa.gov/public\\_info/foia/foia\\_handbook.shtml](http://www.nsa.gov/public_info/foia/foia_handbook.shtml) (last updated Aug. 23, 2013).

68. See *id.*

69. *Founding Church of Scientology v. Nat'l Sec. Agency*, 610 F.2d 824, 826 (D.C. Cir. 1979).

70. *Id.*

71. *Id.* at 827 (quoting Pub. L. No. 86-36, § 6, 73 Stat. 64 (1959)).

72. See *id.* at 826–27.

73. *Id.* at 828. Despite these findings, the D.C. Circuit reversed the decision of the district court because it felt the district court could make a stronger effort to ensure that NSA implemented proper search procedures during the initial FOIA request. *Id.* at 837–38. In 2008–09, the Department of Defense used Exemption 3 to withhold information from FOIA requesters 35,835 times. *Dept. of Defense FOIA Exemptions*, PROPUBLICA, <http://projects.propublica.org/foia-exemptions/agencies/16>. Of these, the Department of Defense used Section 6 of the NSA Act to withhold information from 1,681 claims. *Id.*

74. *Hayden v. Nat'l Sec. Agency*, 608 F.2d 1381, 1389 (D.C. Cir. 1979).

75. *Id.*

76. *Id.* (The D.C. Circuit concluding that if the NSA released the documents requested by appellant, it would disclose a function of the NSA – the signals intelligence function).

in order to satisfy Exemption 3, an agency “must show specifically and clearly that the requested materials fall into the category of the exemption” in its affidavits.<sup>77</sup>

### C. Glomar Responses

During the years immediately following President Johnson signing FOIA into law, agencies took one of three actions when responding to FOIA requests.<sup>78</sup> However, beginning in the 1970s, agencies developed a fourth option when it came to responding to FOIA requests: the *Glomar* response.<sup>79</sup> When agencies refuse to confirm or deny whether responsive records exist, this is known as a *Glomar* response.<sup>80</sup>

*Phillippi v. CIA* established the *Glomar* response option.<sup>81</sup> That case centered on a journalist’s FOIA request to the CIA regarding its relationship with the *Hughes Glomar Explorer*.<sup>82</sup> In *Phillippi*, appellant, believing that the CIA persuaded members of the media not to publish information regarding the CIA’s alleged relationship with the *Glomar Explorer*, filed a FOIA request for all CIA records relating to contacts with the media.<sup>83</sup> On appeal, the D.C. Circuit addressed only one issue: whether the CIA was required to support its response on the basis of the public record.<sup>84</sup> The court determined that when the CIA claims it can neither confirm nor deny the existence of requested records, the only documents that the court can examine are affidavits submitted by the agency to explain its refusal to confirm or deny the records.<sup>85</sup>

A *Glomar* response is appropriate when an agency believes that “to confirm or deny the existence of records . . . would cause harm cognizable under a[] FOIA exception.”<sup>86</sup> The D.C. Circuit has held that the NSA can present a rational explanation for withholding documents and information under Section 6 of the NSA Act by submitting declarations from agency directors.<sup>87</sup> So long as the NSA uses reasonable specificity and plausible logic to show that it appropriately withheld

77. *Id.* at 1390.

78. *Supra* note 48 and accompanying text.

79. *See* *Phillippi v. CIA*, 546 F.2d 1009, 1012 (D.C. Cir. 1976) (reviewing the CIA’s decision to neither confirm nor deny U.S. Government activities in the interest of national security).

80. *ACLU v. CIA*, 710 F.3d 422, 425 (D.C. Cir. 2013).

81. *OIP Guidance: Privacy “Glomarization”*, FOIA Update, Vol. VII, No. 1 (Winter 1986), DEP’T OF JUSTICE, [http://www.justice.gov/oip/foia\\_updates/Vol\\_VII\\_1/page3.htm](http://www.justice.gov/oip/foia_updates/Vol_VII_1/page3.htm).

82. *Phillippi*, 546 F.2d at 1011.. The *Hughes Glomar Explorer* was a large vessel supposedly owned and operated by Summa Corporation. However, there were reports that expressed belief that the ship was actually owned and operated by the U.S. Government. For more on the *Hughes Glomar Explorer*, see *Military Audit Project v. Casey*, 656 F.2d 724, 728–29 (D.C. Cir. 1981).

83. *Id.*

84. *Id.* at 1012.

85. *Id.* at 1013.

86. *Id.* (quoting *Gardels v. CIA*, 689 F.2d 1100, 1103 (D.C. Cir. 1982)).

87. *See* *People for the Am. Way v. Nat’l Sec. Agency*, 462 F. Supp. 2d 21, 30 (D.D.C. 2006).

the information, the D.C. Circuit has made clear that it will not overturn *Glomar* response determinations made by executive branch agencies.<sup>88</sup> Federal agencies utilize *Glomar* responses because they believe that disclosing whether or not the agencies have records about a particular topic may, on its own, reveal protected information.<sup>89</sup> This standard is difficult for plaintiffs to overcome because a *Glomar* response will be overruled only if the specific information requested through the FOIA claim was already in the public domain and officially disclosed by the agency.<sup>90</sup>

The problem that litigants face when courts consider an agency's motion for summary judgment as a result of the agency issuing a *Glomar* response is that litigants do not have the ability to demonstrate the existence of a genuine issue of material fact because they have no way of obtaining records or information. When an agency, without using a *Glomar* response, denies an individual's FOIA request, the individual, if he decides to protest the agency's decision in court, has the ability to ask the judge to conduct *in camera* review<sup>91</sup> or use Vaughn indices,<sup>92</sup> both of which can help the individual make his argument for disclosure of the requested records. However, these two options are not available during appeals of *Glomar* responses.<sup>93</sup>

### III. THE COURT'S REASONING

In *Electronic Privacy Information Center v. National Security Agency*, a three-judge panel of the United States Court of Appeals for the District of Columbia Circuit affirmed the district court's order granting summary judgment in favor of the NSA.<sup>94</sup> Judge Janice Rogers Brown, joined by Judge Brett Kavanaugh and Senior Judge Douglas Ginsburg, held that cyber security threat assessments fall under the

---

88. *Id.* at 31; *see also* Wilner v. Nat'l Sec. Agency, 592 F.3d 60, 70 (2d Cir. 2009) (holding that "an agency may invoke the *Glomar* doctrine in response to a FOIA request regarding a publicly revealed matter. An agency only loses its ability to provide a *Glomar* response when the existence or nonexistence of the particular records covered by the *Glomar* response has been officially and publicly disclosed").

89. *See FOIA Basics*, THE NAT'L SECURITY ARCHIVE, <http://www.gwu.edu/~nsarchiv/nsa/foia/guide.html> (last visited Feb. 26, 2014) (stating that *Glomar* responses are typically used if an agency wishes to not disclose the existence or non-existence of records because whether or not the records exist is, by itself, classifiable).

90. *Wolf v. CIA*, 473 F.3d 370, 378 (D.C. Cir. 2007).

91. "A judicial proceeding is said to be heard *in camera* either when the hearing is had before the judge in his private chambers or when all spectators are excluded from the courtroom" BLACK'S LAW DICTIONARY 760 (6th ed. 1991).

92. A Vaughn index is a document that agencies prepare in FOIA litigation to justify each withholding of information under a FOIA exemption. The term stems from a D.C. Circuit decision that remanded a case so that the government could justify its assertion of exemption by indexing information so that the decision to use an exemption was detailed, specific, and adequate. *Vaughn v. Rosen*, 484 F.2d 820, 826–28 (D.C. Cir. 1973).

93. An *in camera* review cannot be utilized because there are no records eligible for review once an agency issues a *Glomar* response. *See Phillippi v. CIA*, 546 F.2d 1009, 1013 n.7 (D.C. Cir. 1976) (implying that the creation of a Vaughn index is impossible because it requires the agency to acknowledge that records exist).

94. 678 F.3d 926, 929 (D.C. Cir. 2012).

NSA's Information Assurance mission.<sup>95</sup> Since the Information Assurance mission qualifies under Section 6 of the Act, and Section 6 of the Act qualifies under FOIA Exemption 3, FOIA requests that implicate the NSA's Information Assurance mission can be answered by the NSA with a *Glomar* response.<sup>96</sup>

The D.C. Circuit focused on the Janosek Declaration's claim that one of the NSA's missions is its Information Assurance mission, which gives the NSA authority to protect Government information systems.<sup>97</sup> In meeting this mission, the NSA has the right to take action against any threats to U.S. Government information systems, even those that come from commercial technologies.<sup>98</sup> The Janosek Declaration also stated that if the NSA unveiled whether there are records of communications between Google and the NSA regarding the cyber attack on Google, that admission could reveal whether the NSA undertook an investigation responding to the threat.<sup>99</sup>

As a result of the Janosek Declaration, the D.C. Circuit concluded that any information pertaining to this specific relationship between Google and the NSA would disclose protected information about the NSA's implementation of the Information Assurance mission.<sup>100</sup> Critical in the D.C. Circuit's decision was that a relationship or communication between the NSA and any private company would constitute an activity as outlined in Section 6 of the NSA Act.<sup>101</sup> Therefore, if the NSA held any records regarding its interactions with Google, then this would be an NSA activity falling under NSA's Information Assurance mission.<sup>102</sup>

The most critical part of Judge Brown's opinion is the determination that the NSA's Information Assurance mission may be hindered if private entities believed their attempts to seek out the NSA's assistance would be made public as a result of a FOIA request.<sup>103</sup> The Janosek Declaration, which outlined NSA functions that would be implicated by disclosure, clearly defended the NSA's reasons for answering EPIC's FOIA request with a *Glomar* response.<sup>104</sup> The D.C. Circuit held that a NSA function includes determining whether or not certain vulnerabilities in Google technologies pose a risk to the government's information system.<sup>105</sup> Moreover, a formed relationship between the NSA and Google is also a function of the NSA.<sup>106</sup>

---

95. *Id.* at 932. For more on the NSA's Information Assurance mission, visit <http://www.nsa.gov/ia/index.shtml> (last visited Mar. 27, 2014).

96. *Elec. Privacy Info. Ctr.*, 678 F.3d at 932.

97. *Id.*

98. *Id.*

99. *Id.*

100. *Id.*

101. *Id.*

102. *Id.*

103. *Id.*

104. *Id.*

105. *Id.* at 933.

106. *Id.*

The D.C. Circuit reasoned that even though the NSA released statements regarding its Information Assurance mission, it does not follow that the NSA waived protection under FOIA.<sup>107</sup> In handling EPIC's prior disclosure claim against the NSA, the D.C. Circuit determined that EPIC did not meet its burden of proof, requiring EPIC to cite evidence of information that is accessible in the public domain that is similar to the information being withheld by the NSA.<sup>108</sup> EPIC fell short of the burden of proof requirement because EPIC's FOIA request covered a substantially wider range of information than what was published on the NSA's website.<sup>109</sup>

The D.C. Circuit also rejected EPIC's argument that the NSA be required to conduct a "search and segregability" analysis before issuing a *Glomar* response.<sup>110</sup> The court stated that when an agency claims it can neither confirm nor deny any existence of requested records, it makes it impossible for the court to review any documents other than affidavits explaining why the agency came to that decision.<sup>111</sup>

EPIC stated that the D.C. Circuit upheld *Glomar* responses only when the agency performed a search and segregability analysis.<sup>112</sup> However, the court rejected this statement as inaccurate, stating that the cited cases all involved the agency conducting a search and segregability analysis on its own accord before issuing the *Glomar* response.<sup>113</sup> Further, in none of the cited cases did the court imply, let alone hold, that a search and segregability analysis by the agency was required.<sup>114</sup> EPIC also attempted to argue that even when an agency issues a *Glomar* response, they are not exempt from performing a segregability analysis.<sup>115</sup> The argument was rebuffed based on precedent.<sup>116</sup> As a result of this precedent, the court concluded that forcing the NSA to conduct a search and segregability analysis would be

---

107. *Id.*

108. *Id.*

109. *Id.*

110. *Id.* at 934. When an agency issues a *Glomar* response but fails to establish that all the records would be protected under a specific FOIA exemption, the agency must search through the records and segregate information that is not exempted from disclosure from the information that is exempted from disclosure. *Id.* (quoting *Nation Magazine, Wash. Bureau v. U.S. Customs Serv.*, 71 F.3d 885, 890 (D.C. Cir. 1995)). Once the information is segregated, the agency must release the information that is not exempted. *Id.* (quoting *Roth v. Dep't of Justice*, 642 F.3d 1161, 1167 (D.C. Cir. 2011)). Here, the D.C. Circuit found the Janosek Declaration sufficiently supportive of the NSA's *Glomar* response to allow the NSA to forego the search and segregability analysis. *Id.*

111. *Id.* (citing *Wolf v. CIA*, 473 F.3d 370, 374 n. 4 (D.C. Cir. 2007)).

112. *Id.* (citing Brief for Appellant at 25, *Elec. Privacy Info. Ctr. v. Nat'l Sec. Agency*, 678 F.3d 926 (D.C. Cir. 2012) (No. 11-5233)).

113. *Id.*

114. *Id.*

115. *Id.* (citing Brief for Appellant at 24, *Elec. Privacy Info. Ctr. v. Nat'l Sec. Agency*, 678 F.3d 926 (D.C. Cir. 2012) (No. 11-5233)).

116. *Id.* In support of this claim, EPIC cited *Wolf v. CIA*, 473 F.3d 370 (D.C. Cir. 2007). However, *Wolf* expressly rejected this argument in a footnote. See *Wolf*, 473 F.3d at 374 n. 4.

meaningless and costly because the Janosek Declaration provided sufficient support for the *Glomar* response.<sup>117</sup>

In affirming the decision of the District Court for the District of Columbia Circuit, the D.C. Circuit held that the NSA responding to EPIC's FOIA request might reveal the agency's considerations regarding a particular cyber attack, or security settings of a private entity, was a potential risk to Government information systems.<sup>118</sup> This type of "threat assessment," or any ensuing decision or indecision, involves an uncontested NSA "function"—NSA's Information Assurance mission—and therefore satisfies Section 6 of the Act.<sup>119</sup>

#### IV. ANALYSIS

In *Electronic Privacy Information Center v. National Security Agency*, the D.C. Circuit held that the NSA's *Glomar* response sufficiently satisfied the exemption requirements of the Act because threat assessment is an undisputed NSA function and, therefore, the NSA was not required to confirm or deny existence of any responsive records.<sup>120</sup> In reaching this holding, the court correctly determined that if private companies knew their attempts to contact the NSA could be made public through a FOIA request, these companies might not contact the agency, thereby limiting NSA's activities or functions.<sup>121</sup> This decision not only puts federal agencies in a power position but also facilitates public-private partnerships in combating cyber threats.<sup>122</sup> However, this decision negatively impacts the purpose of FOIA and the rights of individuals,<sup>123</sup> and ultimately goes too far by ignoring the public's interest in ensuring their information is under constant protection by companies.<sup>124</sup>

##### *A. The D.C. Circuit's Decision Paves the Way for Private Companies and the Government to Collaborate Freely, Without Fear that the Government Will Have to Reveal Information Regarding Breaches in Cyber Security Infrastructure*

The digital era produces massive amounts of information that can be stored and made readily available on the Internet.<sup>125</sup> Much of this data includes personal and confidential information, collected and held for the benefit of a complex, search-

---

117. *Elec. Privacy Info. Ctr.*, 678 F.3d at 934.

118. *Id.* at 934–35.

119. *Id.* at 935.

120. *Id.* at 934–35.

121. *Id.* at 932.

122. *See infra* IV.A.

123. *See infra* IV.B.

124. *See infra* IV.B.

125. *See* Jonathan Band, *Google and Fair Use*, 3 J. BUS & TECH. L. 1, 2 (2008) (stating that Google's crown jewel is its search engine); *see also* Matthias Hild, *The Google IPO*, 3 J. BUS & TECH. L. 41, 41–43 (2008) (outlining a brief history of Google and its global impact).

friendly business world. However, this search-friendly world provides complexities from a business perspective.<sup>126</sup> Perhaps one of the biggest problems businesses face in the twenty-first century is the constant threat of having their technological systems compromised.<sup>127</sup> While this threat is not worrisome only for businesses across the globe,<sup>128</sup> businesses have the most to lose as they compete for market share, investors, and revenue.<sup>129</sup> If a company's servers were compromised via a cyber attack, it could have devastating effects on its position in the market.<sup>130</sup>

Cyber conflict is the new threat to national security, replacing traditional warfare as the method of attack on global infrastructure.<sup>131</sup> With an increase in cyber threats, businesses are consistently facing more problems<sup>132</sup> Google, as the world's top web parent company<sup>133</sup> and a Fortune 500 Company,<sup>134</sup> is no exception.<sup>135</sup> But Google is not alone in dealing with cyber security issues.

For example, on December 19, 2013, Target Corporation, one of the largest retailers in the United States, reported that it suffered a security breach resulting in hackers gaining access to as many as 40 million credit and debit cards used by customers.<sup>136</sup> Most unsettling perhaps in the eyes of the typical American consumer was the fact that the breach occurred during the height of the winter holiday season, where Americans spend over \$500 billion buying gifts for family, friends, co-

126. See, e.g., Frank Pasquale, *Debating a Right of Reply on Search Results*, 3 J. BUS & TECH. L. 61, 84 (2008) (quoting Brian McNeill, *UVA Professor Takes on 'Googlization'*, DAILY PROGRESS, Sept. 30, 2007, available at [http://www.dailyprogress.com/news/article\\_36efefb6-74ca-5eb0-81db-e8afeb5b8064.html](http://www.dailyprogress.com/news/article_36efefb6-74ca-5eb0-81db-e8afeb5b8064.html)) (claiming that Google has managed to play a role in so many parts of the economy).

127. See Gary Loveland & Mark Lobel, *Cybersecurity: The New Business Priority*, PRICEWATERHOUSECOOPERS, <http://www.pwc.com/us/en/view/issue-15/cybersecurity-business-priority.jhtml> (last visited Feb. 27, 2014) (less than half of all survey respondents identified their companies as having an effective information security strategy).

128. See, e.g., *Hype and Fear*, ECONOMIST (Dec. 8, 2012), <http://www.economist.com/news/international/21567886-america-leading-way-developing-doctrines-cyber-warfare-other-countries-may> (reporting that a senior official in the Department of Defense predicted that a cyber attack on America could potentially make the attacks on September 11, 2001 "look like a tea party").

129. See Loveland & Lobel, *supra* note 127 (reporting that 41% of survey respondents faced one or more security incidents in 2011 and of those respondents, 37.5% saw their companies suffer financial losses as a result).

130. See *id.* (revealing that 31.2% of survey respondents who experienced a security incident in 2011 saw their company's brand/reputation become compromised as a direct result of the attack).

131. Jason Ryan, *FBI Director Says Cyberthreat Will Surpass Threat from Terrorists*, ABC NEWS (Jan. 31, 2012, 7:20 PM), <http://abcnews.go.com/blogs/politics/2012/01/fbi-director-says-cyberthreat-will-surpass-threat-from-terrorists/>.

132. See, e.g., Ariana Eunjung Cha and Ellen Nakashima, *Google Attack Part of Vast Campaign*, WASH. POST, Jan. 14, 2010, at A01.

133. *Top Tens & Trends*, NIELSEN, <http://nielsen.com/us/en/insights/top10s/internet.html> (last visited Feb. 27, 2014).

134. *Fortune 500 2012*, FORTUNE 500, [http://money.cnn.com/magazines/fortune/fortune500/2012/full\\_list/](http://money.cnn.com/magazines/fortune/fortune500/2012/full_list/) (last visited Feb. 7, 2013).

135. Thomas, *supra* note 17, at 101.

136. Craig Timberg, Jia Lynn Yang, & Hayley Tsukayama, *Huge Breach of Data Security at Target*, WASH. POST, Dec. 20, 2013, at A01.



workers, and loved ones.<sup>137</sup> The hackers, who gained access to Target shoppers' names, credit card numbers, expiration dates, and security codes, exposed major vulnerabilities in existing technologies.<sup>138</sup> The negative impact of this attack carried over into 2014, where Target recorded a 52-week low in its stock price nearly every day between January 22nd through February 5th.<sup>139</sup> Additionally, profits at Target during the fourth fiscal quarter of 2013 fell nearly 50% and declined by more than a third for all of 2013.<sup>140</sup>

Using Target as an example of a company that did not seek the help of any federal agency following a security breach helps to show how the D.C. Circuit's decision could give businesses confidence to confide in federal agencies, such as the NSA, when things go wrong. Businesses would be more willing to confide in federal agencies because agencies can just issue a *Glomar* response in the event that a FOIA request is made, so long as the reasons for invoking the exception are "logical" or "plausible."<sup>141</sup> Federal agencies, such as the NSA, are tasked with preventing attacks on American infrastructure;<sup>142</sup> being able to assure private actors that communications between the agency and a business can be protected from the public eye is key in ensuring that this goal can be met. The fact that Google, perhaps the world's largest innovator in how we share private information, was involved in this proceeding is particularly significant. If a major company like Google can be protected, there might be no limit on the types of businesses that will be assisted by NSA's use of the *Glomar* response.<sup>143</sup>

---

137. See *Holiday FAQ*, NAT'L RETAIL FED'N, [https://www.nrf.com/modules.php?name=Pages&sp\\_id=1140](https://www.nrf.com/modules.php?name=Pages&sp_id=1140) (last visited Mar. 30, 2014).

138. Timberg et al., *supra* note 136.

139. Steven Russolillo, *Target Takes Another Hit; Shares Drop to 52-Week Low*, WALL ST. J. (Jan. 21, 2014, 3:48 PM), <http://blogs.wsj.com/moneybeat/2014/01/21/target-takes-another-hit-shares-drop-to-52-week-low/>.

140. Maggie McGrath, *Target Profit Falls 46% on Credit Card Breach and the Hits Could Keep on Coming*, FORBES (Feb. 26, 2014, 9:21 AM), <http://www.forbes.com/sites/maggiemcgrath/2014/02/26/target-profit-falls-46-on-credit-card-breach-and-says-the-hits-could-keep-on-coming/>.

141. *Larson v. Dept. of State*, 565 F.3d 857, 862 (D.C. Cir. 2009).

142. According to the National Security Agency/Central Security Service, "[t]he Information Assurance mission confronts the formidable challenge of preventing foreign adversaries from gaining access to sensitive or classified national security information. The Signals Intelligence mission collects, processes, and disseminates intelligence information from foreign signals for intelligence and counterintelligence purposes and to support military operations. This Agency also enables Network Warfare operations to defeat terrorists and their organizations at home and abroad, consistent with U.S. laws and the protection of privacy and civil liberties." <http://www.nsa.gov/about/mission/index.shtml>.

143. This is particularly true in the wake of Edward Snowden's reveal of the NSA's massive communications collections. From 2010 to 2013, the number of FOIA requests filed with the NSA tripled. In this same time period, the denial rate increased from 33% to 82% as individuals sought their own records. Despite Edward Snowden's reveal of the NSA's information collection, it appears that NSA is playing close to the vest when it comes to revealing any sensitive information, which would provide greater protection for businesses. See Marisa Taylor & Jonathan S. Landay, *Americans Find Swift Stonewall on Whether NSA Vacuumed Their Data*, MCLATCHYDC (Feb. 11, 2014), <http://www.mcclatchydc.com/2014/02/11/217755/americans-find-swift-stonewall.html>.

For example, it was recently reported that the NSA was helping major national banks deal with cyber security issues.<sup>144</sup> These problems stemmed from an onslaught of attacks on the financial institutions' websites.<sup>145</sup> It was reported that leading financial institutions, such as Bank of America, PNC Bank, Wells Fargo, Citigroup, HSBC, and SunTrust, were overcome by attacks on their servers and systems.<sup>146</sup> But why, all of a sudden, are banks coming forward seeking help from NSA?<sup>147</sup>

Mike McConnell,<sup>148</sup> former director of the NSA, has long advocated for a relationship between the public sector and private businesses to better prepare American agencies for any and all cyber attacks.<sup>149</sup> McConnell believes that by pooling together their resources, the NSA and large corporations like Google can defeat cyber terrorists from wreaking havoc on American technological processes.<sup>150</sup> McConnell suggested that, "For this to work, the private sector needs to be able to share network information—on a controlled basis—without inviting lawsuits from shareholders and others."<sup>151</sup> A relationship between the private sector and the Government that revolves around national security issues is ultimately a good thing because the goal would be to protect American citizens from future harm. However, agencies should be required to disclose what they are working on for the companies, particularly when the agencies receive FOIA requests.

The D.C. Circuit's holding furthers McConnell's idea by allowing the NSA to issue *Glomar* responses in regards to EPIC's request for information regarding NSA communications with Google.<sup>152</sup> By justifying the NSA's decision to issue *Glomar* responses, the court opens the door for businesses to begin communicating with NSA without fear that their problems will be exposed as a result of a FOIA request.<sup>153</sup> This has huge benefits to businesses, which can use NSA resources without fear of private communications with government agencies becoming exposed.<sup>154</sup>

Had the court come out in the opposite direction, private companies, as the D.C. Circuit analyzed, in the event of a cyber attack on its operations or servers, would be

144. Bea Edwards, *The NSA and BofA: Working Together for Us?*, GOV'T ACCOUNTABILITY PROJECT (Jan. 14, 2013), <http://www.whistleblower.org/blog/44-2013/2468-the-nsa-and-bofa-working-together-for-us>.

145. *Id.*

146. Ellen Nakashima, *Banks Seek NSA Help with Computer System Attacks*, WASH. POST, Jan. 13, 2013, at A03.

147. *Id.*

148. For more information on McConnell, who as of this writing is the Vice Chairman of Booz Allen Hamilton, see <http://www.boozallen.com/about/leadership/executive-leadership/McConnell> (last visited Mar. 30, 2014).

149. See McConnell, *supra* note 21.

150. *Id.*

151. *Id.*

152. Elec. Privacy Info. Ctr. v. Nat'l Sec. Agency, 678 F.3d 926 (D.C. Cir. 2012).

153. Nakashima, *supra* note 146.

154. *But see* Roth v. Dep't of Justice, 642 F.3d 1161 (D.C. Cir. 2011) (reversing the district court's approval of the FBI's *Glomar* response).

reluctant to work with federal agencies.<sup>155</sup> If private companies are unwilling to report cyber attacks, it would likely limit the ability of federal agencies, such as the NSA or CIA, to determine the source of these cyber attacks, how to stop or contain them, and analyze the attacks so that they do not happen again. This decision firmly puts businesses in the driver seat and gives the government the means to pursue stronger methods of defense.<sup>156</sup> The NSA can justify its actions based on its Information Assurance mission.<sup>157</sup>

If the United States is going to be able to confront foreign and domestic terrorists engaging in cyber warfare, agencies must be able to assure businesses and their executives that by coming forward with information, there is no risk of potential exposure. Perhaps the only true way to make this a reality is for the D.C. Circuit to continue allowing the use of *Glomar* responses by federal agencies.

*B. By Categorizing Any Activity Between the NSA and a Private Business as Protected, the D.C. Circuit Undermined FOIA and the Public Trust*

The D.C. Circuit broadly concluded that records evidencing any interaction between Google and NSA would comprise an NSA “activity.”<sup>158</sup> This proposition reduces the right of individuals to request any records held by a federal agency, a right they are entitled under FOIA.<sup>159</sup> The decision dramatically inhibits President Obama’s goal of making federal agencies more transparent.<sup>160</sup> In fact, the D.C. Circuit undermined President Obama’s presumption that, “[i]n the face of doubt, openness prevails.”<sup>161</sup>

The issue remains: should any communication made by the NSA constitute an activity of the NSA? It is clear that allowing any communication with any private company is too broad of a standard, allowing federal agencies too much power in rejecting FOIA requests through the use of *Glomar* responses without the need to “make a specific showing of potential harm to national security in order to justify withholding information. . . .”<sup>162</sup> Agencies already had strong protection as a result of the official acknowledgment doctrine.<sup>163</sup> Since the NSA never officially

155. *Elec. Privacy Info. Ctr.*, 678 F.3d at 932.

156. Elisabeth Bumiller, *Pentagon Expanding Cybersecurity Force to Protect Networks Against Attacks*, N.Y. TIMES, Jan. 28, 2013, at A7.

157. *Supra* note 142.

158. *Elec. Privacy Info. Ctr.*, 678 F.3d at 932.

159. 5 U.S.C. § 552(a)(3)(A) (2012).

160. Freedom of Information Act: Memorandum for the Heads of Executive Departments and Agencies, 74 Fed. Reg. 4683 (Jan. 21, 2009).

161. *Id.* But see *History of FOIA*, *supra* note 41 (stating that, “[i]n 2012, in a test of the Obama administration’s FOIA practices, 19 out of 20 agencies failed to respond in time to a FOIA request sent by Bloomberg News as they were required to by law”).

162. *Elec. Privacy Info. Ctr.*, 678 F.3d at 931.

163. *Supra* Part II.A.3.

acknowledged a collaborative relationship with Google, the official acknowledgment doctrine did not apply.<sup>164</sup> The requirement that the specific information sought by the plaintiff must already be provided to the public by official disclosure is circular itself because the plaintiff would not need to request information that is already available.<sup>165</sup> If the new battleground between nations is going to take place online rather than on the ground, then there should be some sort of dialogue between private and public sector leaders to discuss collaborative strategies without minimizing the rights of individuals under FOIA.<sup>166</sup>

The fact that any communication between any private business and the NSA constitutes an activity of the agency is confusing. While the NSA made clear that its communications with Google should be protected because they would disclose a function of the agency and had a strong legal framework to support that claim, it does not appear rational to allow the NSA to have free reign to communicate with all private actors because it prevents companies from being accountable for not having best technological practices. The only true justification is the fact that an agency's judgment to issue a *Glomar* response is given "substantial weight"<sup>167</sup> and the D.C. Circuit did not find it necessary to overturn the NSA's decision to issue a *Glomar* response in this scenario. Section 6 of the NSA Act was already regarded as broad enough to allow agencies to defend their withholding of records more easily.<sup>168</sup> But this broad scope granted to Section 6 of the NSA Act allows government officials to consider information to be classified even when the public already knows about the information.<sup>169</sup>

The NSA alleged that it would only enter into an agreement with Google if the NSA believed the cyber attack on Google posed a potential threat to government information systems.<sup>170</sup> Given reports that the NSA is working with major financial institutions,<sup>171</sup> it is more than likely that the NSA will take the same approach: issuing a *Glomar* response and stating that the NSA cannot confirm or deny communications with the banks because doing so would reveal the NSA's thoughts on whether there is a security threat that concerns the United States Government.<sup>172</sup>

164. *Elec. Privacy Info. Ctr.*, 678 F.3d at 933 n. 5.

165. See *Wolf v. CIA*, 473 F.3d 370, 378 (D.C. Cir. 2007).

166. McConnell, *supra* note 21.

167. *Students Against Genocide v. Dep't of State*, 257 F.3d 828, 840 (D.C. Cir. 2001).

168. *Larson v. Dep't of State*, 565 F.3d 857, 868 (D.C. Cir. 2009); *Wilner v. Nat'l Sec. Agency*, 592 F.3d 60, 75 (2d Cir. 2009).

169. *ACLU v. Dep't of Def.*, 389 F. Supp. 2d 547, 561 (S.D.N.Y. 2005).

170. Brief for Appellee at 21, *Elec. Privacy Info. Ctr. v. Nat'l Sec. Agency*, 678 F.3d 926 (D.C. Cir. 2012) (No. 11-5233).

171. Nakashima, *supra* note 146.

172. Brief for Appellant at 21, *Elec. Privacy Info. Ctr. v. Nat'l Sec. Agency*, 678 F.3d 926 (D.C. Cir. 2012) (No. 11-5233).. Although the D.C. Circuit weakens FOIA and prevents individuals and public-interest groups from gaining access to potentially important information, the *Glomar* response is ultimately necessary to protect state secrets from being revealed. This fact justifies the court's decision in this case because national security breaches are perhaps the most important issue businesses and the government face in the digital era.

In the event that there is a FOIA request for records regarding the existence of a relationship between the NSA and the banks, it will be interesting to see how the D.C. Circuit would handle another *Glomar* response. If businesses that have a primary focus in technology (Google) and financial markets (banks) are both protected, then what individual interests will be left for FOIA to protect? As individuals and public-interest groups struggle to come to terms with the fact that *Glomar* responses prevent full disclosure by government agencies, it will be interesting to see how the government reacts to political pressures from pro-FOIA groups. Part of the solution can come from the Executive Branch, since each President of the United States has offered a different approach in regards to how much emphasis should be placed on FOIA.<sup>173</sup> This might be the route to take because the D.C. Circuit's *Glomar* response decisions indicate a preference for business over the individual. But for now it appears that the courts are willing to favor alleged matters of national security over individual access to information.

## V. CONCLUSION

In *Electronic Privacy Information Center v. National Security Agency*,<sup>174</sup> the United States Court of Appeals for the District of Columbia Circuit held that the NSA's *Glomar* response, in regard to EPIC's FOIA request regarding communications between NSA and Google, was valid under the broad ambit of Section 6 of the National Security Agency Act because any threat assessment conducted by NSA constitutes as an undisputed NSA function.<sup>175</sup> The result is that the court protects business interests at the expense of individual rights regarding free access to information.<sup>176</sup> This decision benefits businesses because they get to work with NSA in handling cyber security issues without the fear of potential backlash from the public as a result of information being turned over to individuals as a result of a FOIA request.<sup>177</sup> Even though the decision was supported in a legal context, its decision to place national security concerns ahead of the right to access government-held information undermines FOIA and the ability for the public to know about the effects of cyber attacks on businesses.<sup>178</sup>

---

173. See *History of FOIA*, *supra* note 41 (comparing President Reagan's issuance of Executive Order 12356, which made withholding sensitive government records much easier, with President Clinton's signature of the Electronic Freedom of Information Act Amendments, which would allow for greater transparency).

174. 678 F.3d 926 (D.C. Cir. 2012).

175. *Id.* at 935.

176. See *supra* Part IV.

177. See *supra* Part IV.A.

178. See *supra* Part IV.B.