United States Court of Appeals

FOR THE DISTRICT OF COLUMBIA CIRCUIT

Argued March 20, 2012 Decided May 11, 2012

No. 11-5233

ELECTRONIC PRIVACY INFORMATION CENTER,
APPELLANT

v.

NATIONAL SECURITY AGENCY,
APPELLEE

Appeal from the United States District Court
for the District of Columbia
(No. 1:10-cv-01533)

Marc Rotenberg argued the cause for appellant. With him on the briefs was *John Verdi*.

Catherine Y. Hancock, Attorney, U.S. Department of Justice, argued the cause for appellee. With her on the brief were *Tony West*, Assistant Attorney General, *Ronald C. Machen Jr.*, U.S. Attorney, and *Douglas N. Letter*, Attorney.

Before: BROWN and KAVANAUGH, *Circuit Judges*, and GINSBURG, *Senior Circuit Judge*.

Opinion for the Court filed by *Circuit Judge* BROWN.

BROWN, *Circuit Judge*: Plaintiff-appellant Electronic Privacy Information Center ("EPIC") filed a Freedom of Information Act ("FOIA") request with the National Security Agency ("NSA") seeking disclosure of any communications between NSA and Google, Inc regarding encryption and cyber security. NSA issued a *Glomar* response pursuant to FOIA Exemption 3, indicating that it could neither confirm nor deny the existence of any responsive records. EPIC challenged NSA's *Glomar* response in the district court, and the parties cross-moved for summary judgment. The district court entered judgment for NSA, and EPIC appealed. We affirm.

I.

EPIC's FOIA request arose out of a January 2010 cyber attack on Google that primarily targeted the Gmail accounts of Chinese human rights activists.[1] Google subsequently changed Gmail's privacy settings to automatically encrypt all traffic to and from its servers. David Drummond, Google's Senior Vice President for Corporate Development and Chief Legal Officer, stated that the company was notifying other companies that may have been targeted and was "also working with the relevant U.S. authorities." David Drummond, *A New Approach to China*, Official Google Blog (Jan. 12, 2010), http://googleblog.blogspot.com/2010/01/new-approach-to-china.html. On February 4, 2010, the Wall Street Journal and Washington Post reported that Google had contacted the NSA immediately following the attack. Former

[1] Gmail is a "cloud-based" email program, meaning the data and applications of the user reside on remote computer servers operated by Google. Prior to January 2010, Google allowed Gmail users to encrypt the mail that passed through Google servers using Hypertext Transfer Protocol Secure, but it did not provide encryption by default.

NSA director Mike McConnell commented in the Washington Post that collaboration between NSA and private companies like Google was "inevitable." Mike McConnell, *Mike McConnell on How to Win the Cyber-War We're Losing*, Washington Post (Feb. 28, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html.

On February 4, 2010, EPIC submitted a FOIA request to NSA, specifically requesting three categories of records:

1. All records concerning an agreement or similar basis for collaboration, final or draft, between the NSA and Google regarding cyber security;
2. All records of communication between NSA and Google concerning Gmail, including but not limited to Google's decision to fail to routinely encrypt Gmail messages prior to January 13, 2010; and
3. All records of communications regarding NSA's role in Google's decision regarding the failure to routinely deploy encryption for cloud-based computing service, such as Google Docs.

NSA responded to EPIC's request on March 10, 2010 by invoking Exemption 3 of the FOIA and Section 6 of the National Security Agency Act[2] to issue a *Glomar* response, in which the agency neither confirmed nor denied the existence of any responsive records.

[2] Section 6 of the National Security Agency Act provides that "nothing in this Act or any other law . . . shall be construed to require the disclosure of the organization or any function of the National Security Agency, [or] of any information with respect to the activities thereof . . . ." Pub. L. No. 86–36, § 6(a), 73 Stat. 63, 64 (1959).

EPIC filed suit in the district court challenging NSA's *Glomar* response.[3] The parties cross-moved for summary judgment. In support of its motion for summary judgment, NSA filed a declaration by Diane M. Janosek, NSA Deputy Associate Director for Policy and Records (the "Janosek Declaration"). The district court held that NSA was entitled to summary judgment because the Janosek Declaration was "both logical and plausible" and "contain[ed] sufficient detail, pursuant to Section 6, to support NSA's claim that the protected information [sought by EPIC] pertains to" NSA's organization, functions, or activities. *Elec. Privacy Info. Ctr. v. NSA*, 798 F. Supp. 2d 26, 31–32 (D.D.C. 2011). We review the district court's grant of summary judgment *de novo*. *See Larson v. Dep't of State*, 565 F.3d 857, 862 (D.C. Cir. 2009).

II.

The Freedom of Information Act, 5 U.S.C. § 552(a), provides that "[e]ach agency shall make available to the public" records in its possession unless the information is covered by one of Section 552(b)'s nine statutory exemptions. As relevant here, FOIA Exemption 3 shields from disclosure records that are "specifically exempted from disclosure by statute" if such statute either "requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue" or "establishes particular criteria for withholding or refers to particular types of matters to be withheld." 5 U.S.C. § 552(b)(3).

[3] EPIC initially filed an administrative appeal, arguing that NSA's response was unlawful because the agency had failed to present factual evidence that the requested documents fell within Section 6, but filed suit in the district court prior to the resolution of that appeal.

In addition to withholding records that are exempt, an agency may issue a *Glomar* response, *i.e.*, refuse to confirm or deny the existence or nonexistence of responsive records if the particular FOIA exemption at issue would itself preclude the acknowledgement of such documents. *See Wolf v. CIA*, 473 F.3d 370, 374 (D.C. Cir. 2007).[4] An agency may issue a *Glomar* response when "to answer the FOIA inquiry would cause harm cognizable under" an applicable statutory exemption. *Id.* The agency must demonstrate that acknowledging the mere existence of responsive records would disclose exempt information. *Id*.

In *Glomar* cases, courts may grant summary judgment on the basis of agency affidavits that contain "reasonable specificity of detail rather than merely conclusory statements, and if they are not called into question by contradictory evidence in the record or by evidence of agency bad faith." *Gardels v. CIA*, 689 F.2d 1100, 1105 (D.C. Cir. 1982). The supporting affidavit must justify the *Glomar* response based on "general exemption review standards established in non-*Glomar* cases." *Wolf*, 473 F.3d at 374–75. "Ultimately, an agency's justification for invoking a FOIA exemption is sufficient if it appears 'logical' or 'plausible.'" *Larson*, 565 F.3d at 862. NSA need not make a specific showing of potential harm to national security in order to justify withholding information under Section 6, because "Congress has already, in enacting the statute, decided that disclosure of NSA activities is potentially harmful." *Hayden v. NSA*, 608 F.2d 1381, 1390 (D.C. Cir. 1979). In reviewing an agency's *Glomar* response, this Court exercises caution when the

[4] The *Glomar* response takes its name from the *Hughes Glomar Explorer*, "a ship built (we now know) to recover a sunken Soviet submarine, but disguised as a private vessel for mining manganese nodules from the ocean floor." *Bassiouni v. CIA*, 392 F.3d 244, 246 (7th Cir. 2004).

information requested "implicat[es] national security, a uniquely executive purview." *Ctr. for Nat'l Sec. Studies v. Dep't of Justice*, 331 F.3d 918, 926–27 (D.C. Cir. 2003).

NSA issued a *Glomar* response to EPIC's request for records pertaining to the agency's contact with Google, claiming that any responsive records would be exempt from disclosure under Exemption 3 and Section 6 of the National Security Agency Act, and that acknowledgement of the existence of such records would cause harm cognizable under the exemption. Because Section 6 of the National Security Agency Act "is a statute qualifying under Exemption 3," *Founding Church of Scientology of Washington, D.C. v. NSA*, 610 F.2d 824, 828 (D.C. Cir. 1979), the only question is whether the withheld material satisfies the criteria of the exemption statute, *i.e.*, whether acknowledging the existence or nonexistence of the requested material would reveal a function or an activity of the NSA. *See Larson*, 565 F.3d at 868 (NSA "need only demonstrate that the withheld information relates to the organization of the NSA or any function or activities of the agency"). The agency bears the burden of proving that the withheld information falls within the exemption it invokes. 5 U.S.C. § 552(a)(4)(B); *King v. Dep't of Justice*, 830 F.2d 210, 217 (D.C. Cir. 1987).

EPIC claims its request seeks some records that are not covered by Exemption 3 and Section 6 of the NSA Act—specifically, unsolicited communications from Google to NSA, which would fall within the second category of information described in the request. In light of the broad language of Section 6, however, we find the Janosek Declaration provides adequate support for NSA's *Glomar* response. As the Declaration explains, one of NSA's primary cryptologic missions is its Information Assurance mission, under which NSA is tasked with protecting Government

information systems. Because the Government is "largely dependent on commercial technology for its information systems," NSA also monitors commercial technologies purchased by the government for security vulnerabilities. Janosek Dec'l ¶ 6. If NSA concludes that vulnerabilities in those commercial technologies pose a threat to U.S. Government information systems, NSA may take action against the threat.

The Declaration further explains that if NSA disclosed whether there are (or are not) records of a partnership or communications between Google and NSA regarding Google's security, that disclosure might reveal whether NSA investigated the threat, deemed the threat a concern to the security of U.S. Government information systems, or took any measures in response to the threat. As such, any information pertaining to the *relationship* between Google and NSA would reveal protected information about NSA's implementation of its Information Assurance mission. The existence of a relationship or communications between the NSA and any private company certainly constitutes an "activity" of the agency subject to protection under Section 6. Whether the relationship—or any communications pertaining to the relationship—were initiated by Google or NSA is irrelevant to our analysis. Even if EPIC is correct that NSA possesses records revealing information *only* about Google, those records, if maintained by the agency, are evidence of some type of interaction between the two entities, and thus still constitute an NSA "activity" undertaken as part of its Information Assurance mission, a primary "function" of the NSA. Moreover, if private entities knew that any of their attempts to reach out to NSA could be made public through a FOIA request, they might hesitate or decline to contact the agency, thereby hindering its Information Assurance mission.

EPIC's attempt to liken this case to *Founding Church of Scientology,* in which this Court found the agency's affidavit too conclusory to support the NSA's rejection of a FOIA request, *see* 610 F.2d at 833, is unpersuasive. The affidavits at issue in the two cases differ substantially in their level of specificity. In *Founding Church of Scientology,* the affidavit summarily stated, without further elucidation, that "[d]isclosure of specific information which may be related to a specific individual or organization . . . in the context of [the agency's] singular mission would reveal certain functions and activities of the NSA . . . ." *Id.* at 831. Here, by contrast, the NSA's affidavit describes which functions and activities would be implicated by disclosure, as well as how acknowledging the existence or nonexistence of requested records would reveal those functions or activities.

EPIC also attempts to distinguish this Court's prior interpretations of Section 6 because those cases involved requests for records relating to the NSA's classified intelligence gathering activities and sources. *See, e.g.*, *Larson,* 565 F.3d at 867–69. EPIC contends that the same logic that requires secrecy in intelligence gathering does not apply to the NSA's Information Assurance mission because it is public knowledge that the U.S. government uses Google applications and that NSA is investigating security vulnerabilities in Google's commercial products. The language of the NSA Act, however, does not distinguish between the agency's various missions, and does not invite this Court to do so. Rather, the statute broadly exempts *any* information pertaining to the agency's "activities" or "functions." NSA's determination that certain security vulnerabilities in Google technologies pose (or do not pose) a risk to the government's information systems constitutes an "activity" of the agency, as does a relationship between the agency and Google.

Moreover, NSA does not waive its protection under FOIA by disclosing basic information about its information assurance activities. The fact that limited information regarding a clandestine activity has been released does not mean that all such information must be released. *See Students Against Genocide v. Dep't of State*, 257 F.3d 828, 836 (D.C. Cir. 2001). *See also Wilner v. NSA*, 592 F.3d 60, 69–70 (2d Cir. 2009) (holding that the President's decision to make public the existence of an NSA intelligence-gathering program did not force the government to reveal the program's operational details). A plaintiff asserting a claim of prior disclosure bears the burden of pointing to "specific information in the public domain that appears to duplicate that being withheld." *Wolf*, 473 F.3d at 378. EPIC has failed to meet its burden because its blanket request for "[a]ll records of communication between NSA and Google concerning Gmail" covers a substantially broader swath of information than what NSA has voluntarily published on its website. General security guidance, even involving recommended security settings for Gmail, does not "appear[] to duplicate" private communications between NSA and Google; it does not even disclose whether the two entities have engaged in such communications.[5]

[5] EPIC's claim that collaboration between Google and NSA was "widely reported in the national media and acknowledged by the former director of the NSA" is similarly unavailing. Appellant's Br. 19. NSA has never officially acknowledged a collaborative relationship with Google, and the national media are not capable of waiving NSA's statutory authority to protect information related to its functions and activities. *See Frugone v. CIA*, 169 F.3d 772, 774–75 (D.C. Cir. 1999) (holding that only official acknowledgement from the agency from which the information is being sought can waive an agency's protective power over records sought under the FOIA); *Wolf*, 473 F.3d at 378 (waiver of

III.

Subsection (b) of the FOIA provides that "[a]ny reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt under this subsection." 5 U.S.C. § 552(b). In response to a FOIA request, agencies "must make a good faith effort to conduct a search for the requested records, using methods which can be reasonably expected to produce the information requested." *Nation Magazine, Washington Bureau v. U.S. Customs Serv.*, 71 F.3d 885, 890 (D.C. Cir. 1995). "[E]ven if [the] agency establishes an exemption, it must nonetheless disclose all reasonably segregable, nonexempt portions of the requested record(s)." *Roth v. Dep't of Justice*, 642 F.3d 1161, 1167 (D.C. Cir. 2011).

EPIC argues that Section 552(b) requires NSA to search for responsive documents and conduct a segregability analysis prior to issuing a *Glomar* response. We rejected a similar argument in *Wolf*, and EPIC is no more persuasive. In *Wolf*, the requester claimed that *de novo* review of the agency's response "requires the district court to order the Agency to search for responsive records and to submit a *Vaughn* index." 473 F.3d at 374 n.4. The Court disagreed, explaining that the requester's argument "misunderstands the nature of a *Glomar* response, which narrows the FOIA issue to the existence of records *vel non*." *Id.* When the agency takes the position that it can neither confirm nor deny the existence of the requested records, "there are no relevant documents for the court to examine other than the affidavits which explain the Agency's

---

protection under the FOIA "cannot be based on mere public speculation, no matter how widespread").

refusal." *Id.; see also Wheeler v. CIA*, 271 F. Supp. 2d 132, 141 (D.D.C. 2003) (affirming a *Glomar* response when the agency did not identify "whether or to what extent it had conducted a search"). The same logic applies here. Because we find the Janosek Declaration sufficient to support NSA's *Glomar* response, requiring NSA to conduct a search and segregability analysis would be a meaningless—not to mention costly—exercise.

EPIC claims this Court has upheld *Glomar* responses "only in cases where it is apparent from the record that the Agency first conducted a search and segregability analysis, and even disclosed or withheld specific responsive records," Appellant's Br. 25. This is inaccurate. In the cases cited by EPIC, the agency conducted a search and segregability analysis of its own volition prior to issuing the *Glomar* response. *See, e.g., Larson*, 565 F.3d at 861–62. In none of these cases, however, did the Court hold—or even imply—that such a search and analysis is *required. See People for the Am. Way Found. v. NSA*, 462 F. Supp. 2d 21, 30 n.5 (D.D.C. 2006) ("[A] *Vaughn* index is not required here, where it could cause the very harm that section 6 was intended to prevent."). Likewise, EPIC's assertion that "[a]gencies are not exempt from performing a segregability analysis, even in cases where they assert a *Glomar* response," Appellant's Br. 24, is also incorrect. Although EPIC cites *Wolf* in support of its proposition, that case expressly rejected EPIC's argument in a footnote. *See Wolf*, 473 F.3d at 374 n.4.

EPIC's reliance on *Jefferson v. Dep't of Justice, Office of Prof'l Resp.*, 284 F.3d 172 (D.C. Cir. 2002), is also misplaced. In *Jefferson*, the Court held that the Office of Professional Responsibility ("OPR") was not entitled to make a *Glomar* response as to all of its files in the absence of an evidentiary showing to support that response. *Id.* at 179. But

that case turned on two factors not present here: (1) it applied Exemption 7(C), which protects only "records or information compiled for law enforcement purposes," 5 U.S.C. § 552(b)(7); and (2) not all records of the OPR are necessarily law enforcement records. *Jefferson*, 284 F.3d at 178–79. Because the request asked for "all records" pertaining to a particular AUSA, and not simply those compiled for law enforcement purposes, the Court held that *Glomar* response was inappropriate in light of OPR's failure to show that all of the responsive records were covered by the Exemption, *i.e.*, were compiled for law enforcement purposes. *Id.* at 179. Here, by contrast, it is apparent that any response to EPIC's FOIA request might reveal whether NSA did or did not consider a particular cybersecurity incident, or the security settings in particular commercial technologies, to be a potential threat to U.S. Government information systems. Any such threat assessment, as well as any ensuing action or inaction, implicates an undisputed NSA "function"—its Information Assurance mission—and thus falls within the broad ambit of Section 6 of the National Security Agency Act.

IV.

For the foregoing reasons, the decision of the district court is

Affirmed.