UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

AGILITY PUBLIC WAREHOUSING COMPANY K.S.C., Plaintiff, v. NATIONAL SECURITY AGENCY, Defendant.	Civil Action No. (BAH) 14-0946 Judge Beryl A. Howell

MEMORANDUM OPINION

The plaintiff, Agility Public Warehousing Company K.S.C., brings suit against the National Security Agency ("NSA"), pursuant to the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552. As part of its FOIA request, the plaintiff sought "all [of the] email, letter, telephonic, or other communications" of the plaintiff in the NSA's possession. *See* Compl. ¶ 11, ECF No. 1. Relying on information leaked to the media regarding various classified NSA communication collection programs, the plaintiff argues that the NSA "indiscriminately collect[s] millions of telephone and email communications" from U.S. citizens and therefore maintains records of the plaintiff's historical communications. *See* Pl.'s Mem. Supp. Cross-Mot. Summ. J. ("Pl.'s Mem.") at 1, ECF No. 19-1. The NSA, however, issued a "Glomar" response—neither confirming nor denying the existence of records responsive to the plaintiff's request.

The plaintiff challenges the NSA's provision of a "Glomar" response regarding the requested documents as well as the adequacy of the NSA's search efforts for certain other requested documents. Now pending before the Court are the parties' cross motions for summary judgment. For the reasons stated below, the NSA's motion for summary judgment is granted and the plaintiff's cross-motion for summary judgment is denied.

I. BACKGROUND

A. The Plaintiff's FOIA Request

The plaintiff is a Kuwaiti logistics company that provided food to U.S. troops stationed in Iraq, Kuwait, Qatar, and Jordan from 2003 through 2010, as part of a series of contracts with the Defense Logistics Agency. Compl. ¶ 3. On November 9, 2009, the plaintiff was indicted in the Northern District of Georgia on charges of conspiracy to defraud the United States in violation of 18 U.S.C. § 371, major fraud against the United States in violation of 18 U.S.C. § 1031, and wire fraud in violation of 18 U.S.C. § 1343, stemming from the plaintiff's provision of goods under these contracts. The charges remain pending. *See United States v. The Public Warehousing Co., K.S.C.*, No. 1:09-CR-490 (N.D. Ga. 2009). The plaintiff was also sued in that same court for violations of the False Claims Act, 31 U.S.C. 3729 *et seq.*, which violations likewise stem from the plaintiff's provision of goods to U.S. soldiers. *See United States ex rel. Kamal Mustafa Al-Sultan v. The Public Warehousing Company, K.S.C.*, No. 1:05-CV-2968 (N.D. Ga. 2005).[1] In defending against these civil and criminal charges, the plaintiff "makes extensive use of email and telephone communications" to communicate from Kuwait with its U.S.-based attorneys at Skadden, Arps, Slate, Meagher & Flom LLP ("Skadden"). Decl. of Emily L. Aviad ¶ 9 ("Pl.'s Aviad Decl."), ECF No. 19-3. Skadden was a "customer of Verizon Business Network Services from 2010 through the first quarter of 2014."[2] *See* Suppl. Decl. of Emily L. Aviad ¶ 2 ("Pl.'s Aviad Suppl. Decl."), ECF No. 26-1.

On December 19, 2013, the plaintiff submitted a FOIA request to the NSA seeking seven categories of documents: (1) "all email, letter, telephonic, or other communications" by the

[1] The civil case has been administratively closed pending an order from the Kuwaiti High Court of Appeals regarding whether the plaintiff was properly served as a defendant in that case. *See Public Warehousing Company*, No. 1:05-CV-2968 (N.D. Ga. 2005).

[2] The plaintiff has not specified whether Verizon Business Network Services provided both telephonic and internet services, only that it was a customer. *See* Pl.'s Aviad Suppl. Decl ¶ 2.

plaintiff; (2) the name of any U.S. or foreign communications provider that intercepted the plaintiff's communications; (3) documents relating to two contracts between the plaintiff and Defense Supply Center Philadelphia; (4) documents relating to the two lawsuits brought against the plaintiff in the Northern District of Georgia; (5) all communications between the NSA and any other investigative or law enforcement agency regarding the plaintiff; (6) documents pertaining to meetings among employees or contractors of any of the Department of Justice, the Office of the Director of National Intelligence, and the NSA regarding the plaintiff; and (7) documents pertaining to meetings between employees or contractors of the NSA and employees or contractors of the Federal Bureau of Investigation, the Central Intelligence Agency, the Department of Defense, and the Department of Homeland Security, relating to the plaintiff. Compl. ¶ 11.

Although the plaintiff and the NSA exchanged communications clarifying the scope of the plaintiff's FOIA request, the NSA never provided a response to the plaintiff prior to this litigation. *Id.* at ¶¶ 14–16. As a result, the plaintiff appealed to the NSA's FOIA Appeal Authority based on the NSA's constructive denial of its FOIA request. *Id.* The NSA indicated that processing of the plaintiff's appeal would be based on a "first-in, first-out" policy, but over the course of two months, the NSA never responded to the plaintiff. *Id.* at ¶¶ 17–19; Decl. of David J. Sherman ("NSA's Sherman Decl.") at ¶ 24, ECF No. 18-2. As a result, the plaintiff filed the instant action. *See generally* Compl.

After the initiation of litigation, the Chief of NSA's FOIA/Privacy Act Office provided the plaintiff with a letter purporting to be a final response to the plaintiff's FOIA request. *See* NSA's Sherman Decl. ¶ 25. The NSA noted that, to the extent the plaintiff sought records concerning the contracts and lawsuits mentioned in the plaintiff's FOIA request, the NSA had

conducted a thorough search and was unable to locate any responsive records. *Id.* ¶ 27. As detailed in two declarations, the NSA tasked "its Office of General Counsel, its acquisition organization, and its logistics organization" to conduct the relevant searches. *Id.* The NSA queried the records of the relevant organizations using variations of the plaintiff's name as specified in the plaintiff's FOIA request—Agility Public Warehousing Company, Agility, and the Public Warehousing Company—and the numbers for the relevant contracts. Supplemental Decl. of David J. Sherman ("NSA's Suppl. Sherman Decl.") at ¶ 3, ECF No. 23-1. The NSA's filing systems contained memoranda, meeting minutes, reports, manuals, and other documents. NSA's Sherman Decl. ¶ 27. Within the Office of General Counsel, attorneys searched their Microsoft Outlook email accounts while administrative personnel and paralegals searched the organization's litigation filings systems. *Id.* The NSA also searched the "contracting management information system database," which is maintained in support of the NSA's contracting activity. *Id.*

In addition, the NSA's response informed the plaintiff that, to the extent the plaintiff's FOIA request called for intelligence information, the NSA could not confirm or deny the existence of any such records as their existence or non-existence is protected by FOIA Exemptions 1 and 3. *See id.* ¶ 26. The NSA's "foreign intelligence mission includes the responsibility to collect, process, analyze, produce and disseminate signals intelligence ('SIGINT') information, of which communications intelligence ('COMINT') is a significant subset, for foreign intelligence and counterintelligence purposes to support national and departmental missions to include the conduct of military operations." *Id.* ¶ 5. In light of its mission, the NSA determined that "[a]cknowledging the existence or non-existence of responsive records on particular individuals or organizations subject to surveillance would provide . . .

adversaries with critical information about the capabilities and limitations" of the NSA and its operations. *Id.* ¶ 33. Likewise, "[c]onfirmation by NSA that a specific person's or organization's activities are not of foreign intelligence interest or that NSA is unsuccessful in collecting foreign intelligence information on their activities" would undermine the NSA's mission and permit adversaries to "accumulate information and draw conclusions about NSA's technical capabilities, sources, and methods." *Id.* As a result, the disclosure of such information "could reasonably be expected to cause exceptionally grave and irreparable damage to the national security by providing . . . adversaries a road map that instructs them on which communication modes or personnel remain safe or are successfully defeating NSA's capabilities." *Id.* ¶34. Moreover, disclosure of such information would permit adversaries to change their communications behavior or otherwise "alert targets that their existing means of communications are potentially safe." *Id.* Accordingly, the NSA did not confirm the existence or non-existence of any such records.

B. The NSA's Metadata Program

Almost seven months before the plaintiff filed the FOIA request at issue, a United Kingdom-based newspaper, *The Guardian*, published, on June 6, 2013, an article claiming that the "National Security Agency is currently collecting the telephone records of millions of US customers of Verizon, . . . under a top secret court order issued in April." *See* Ex. 3, Pl.'s Aviad Decl. (Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, The Guardian, June 6, 2013). *The Guardian* attached to the article a then-classified Foreign Intelligence Surveillance Court ("FISC") "Secondary Order," dated April 25, 2013, which it had obtained from a former U.S. government contractor, Edward Snowden. *Id.*; *see also* Ex. 4, Pl.'s Aviad Decl. (*In re Application of the FBI for an Order Requiring the Prod. of Tangible Things*

From Verizon Bus. Network Servs., Inc., ex rel. MCI Commc'n Servs., Inc., d/b/a Verizon Bus. Servs. ("Secondary Order"), No. BR 13–80 (F.I.S.C. Apr. 25, 2013)). The FISC Secondary Order required Verizon Business Network Services to provide "on an ongoing daily basis . . . all call detail records or 'telephony metadata' created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls." Secondary Order at 2. Telephony metadata includes, *inter alia*, the originating and terminating telephone number along with the time and duration of the call.[3] Telephony metadata "does not include the substantive content of any communication . . . or the name, address, or financial information of a subscriber or customer." *Id.*

In the aftermath of *The Guardian's* disclosure, the government began to release details regarding the telephony metadata program along with declassified and redacted copies of other FISC orders. *See* Ex. 11, Pl.'s Aviad Decl. (Press Release, *DNI Clapper Declassifies Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act (FISA)*, Nov. 18, 2013). These disclosures reveal that since at least May 2006, the FBI has sought orders from the FISC authorizing the bulk collection of telephony metadata from U.S. telecommunications providers pursuant to Section 215 of the USA PATRIOT Act, 50 U.S.C. § 1861. *See In re Application of the Fed. Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted]*, No. BR 06–05, at 2 (F.I.S.C. May 24, 2006); *see also* Ex. 7, Pl.'s Aviad Decl. (Declaration of Teresa H. Shea, Signals Intelligence Director, NSA ("NSA's Shea Decl."), *Smith v. Obama*, No. 13-cv-0257 (D. Idaho Jan. 24, 2013), ECF No. 15-2).

[3] Telephony metadata also includes other "session-identifying information," such as the "International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number . . . trunk identifier, [and] telephone calling card numbers . . . ." Secondary Order at 2.

Section 215 authorizes the FBI to "make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information concerning a United States person or to protect against international terrorism or clandestine intelligence activities . . . ." 50 U.S.C. § 1861. Under the program, the FBI seeks orders from the FISC "directing certain telecommunications service providers to produce all business records created by them (known as call detail records)" for a designated period of time. NSA's Shea Decl. ¶ 14. "FISC orders must be renewed every 90 days, and the program has therefore been renewed 41 times since May 2006." *Am. Civil Liberties Union v. Clapper*, 785 F.3d 787, 796 (2d Cir. 2015). Once the information is obtained from the telecommunications service providers, the "NSA . . . stores and analyzes this information . . . and refers to the FBI information about communications . . . that the NSA concludes have counterterrorism value, typically information about communications between known or suspected terrorist operatives and persons located within the U.S." NSA's Shea Decl. ¶ 16.

Once collected from the telecommunications provider and stored in a secure database, strict procedures govern the NSA's access to and use of the collected telephony metadata. *See In re Application of the FBI for an Order Requiring the Prod. of Tangible Things From* [*REDACTED*], No. BR 13–80, 2013 WL 5460137 (F.I.S.C. Apr. 25, 2013) ("Primary Order"). The government is only permitted to access the collected telephony metadata for the purposes set forth in the Primary Order, which includes "purposes of obtaining foreign intelligence information" and technical maintenance. *See* Primary Order at 2–3; NSA Shea Decl. ¶ 18. The NSA may access the collected telephony metadata only by searching with a telephone number or other "identifier," that is associated with a foreign terrorist organization. NSA's Shea Decl. ¶ 20–

21; Primary Order at 2–4. Before an identifier may be used, one of twenty-two designated officials must determine that a "reasonable articulable suspicion" exists that the identifier is associated with an international terrorist organization subject to an FBI investigation. NSA Shea Decl. ¶ 21; Primary Order at 2–3. Where the identifier is reasonably believed to be used by a U.S. person, such reasonable articulable suspicion may not be based solely upon protected First Amendment activities. NSA's Shea Decl. ¶ 21; Primary Order at 2. The reasonable articulable suspicion requirement was intended to prevent the generalized browsing of data. NSA's Shea Decl. ¶ 20. The NSA must destroy all metadata no later than five years after the initial collection. NSA's Shea Decl. ¶ 31; Primary Order at 4.

Before information pertaining to any U.S. person may be disseminated outside the NSA, certain high-level officials "must determine that the information identifying the U.S. person is in fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance." Primary Order at 3. The NSA may also share the results from searches of the metadata with the Executive Branch in order to permit the Executive Branch to determine if such "information contains exculpatory or impeachment information or is otherwise discoverable in legal proceedings" or to "facilitate their lawful oversight functions." Primary Order at 3.

Almost immediately following these revelations, individuals and public interest groups filed numerous lawsuits throughout the country challenging the constitutional and statutory basis for the program. *See, e.g.*, *Clapper*, 785 F.3d 787; *Smith v. Obama*, 24 F. Supp. 3d 1005 (D. Idaho 2014), No. 14–35555 (9th Cir. argued Dec. 8, 2014); *Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. 2013), No. 14–5004 (D.C. Cir. argued Nov. 4, 2014); *Schuchardt v. Obama*, 14-705 (W.D. Pa.); *Paul v. Obama*, 14-0262 (D.D.C.); *First Unitarian Church of Los Angeles v. Nat'l*

Sec. Agency, 13-3287 (N.D. Cal.). Additionally, in at least one other instance, a plaintiff has sought records under FOIA that it believed to be in the possession of the NSA based on this bulk collection of metadata. *See Competitive Enter. Inst. v. Nat'l Sec. Agency*, No. 14-975, 2015 WL 151465, at *1 (D.D.C. Jan. 13, 2015).

C. Other Data Collection Programs

In addition to the NSA's telephony metadata program, the NSA's involvement in at least three other classified programs concerning the bulk collection of communications are implicated by the plaintiff's claim. Under the Pen Register and Trap and Trace ("PR/TT") program, the government sought FISC orders permitting the collection from service providers of certain electronic communications metadata, including the "to," "from," and "cc" lines of an email, along with the time and date of an email. *See* Ex. 11, Pl.'s Aviad Decl (Press Release, Office of the Director of National Intelligence, *DNI Clapper Declassifies Additional Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act*, Nov. 18, 2013). Once collected, the information was stored in a secured database. *Id.* The maintenance and searching of the collected database records was subject to strict requirements similar to those set forth for the NSA's telephony metadata program. *Id.* The NSA has not acknowledged a partnership with any specific telecommunications provider regarding the PR/TT program and the program has since been discontinued. *See id.*

Similarly, media reports have also discussed what have been referred to as the NSA's PRISM collection and the "upstream collection" program. Under the PRISM program, the NSA acquired electronic communications, including e-mails, directly from "compelled U.S.-based providers," such as Google, Apple, and Facebook. *See* Ex. 8, Pl.'s Aviad Decl. (Declassified Declaration of Frances J. Fleisch, NSA ("NSA's Fleisch Decl."), at ¶ 38, *Jewel v. Nat'l Sec.*

Agency, No. 08-CV-04373 (N.D. Cal. May 5, 2014), ECF No. 227); Ex. 12, Pl.'s Aviad Decl. (Glenn Greenwald & Ewan MacAskill, *NSA Prism Program Taps into User Data of Apple, Google, and Others*, The Guardian, June 7, 2013). In the separate "upstream collection" program, "the NSA collects electronic communications with the compelled assistance of electronic communication service providers as they transit Internet 'backbone' facilities within the United States." NSA's Fleisch Decl. ¶ 38; *see* [Redacted] Mem. Op., 2011 WL 10945618, at *9 (FISC Oct. 3, 2011). Between these two programs, the NSA "acquires more than two hundred fifty million Internet communications each year." [Redacted] Mem. Op., 2011 WL 10945618, at *9. Like the PR/TT program, the NSA has not acknowledged the identity of any service providers participating in either the PRISM or the upstream collection programs. *See* Pl.'s Mem. at 24 ("[T]he NSA has not specifically named any telecommunications or Internet service providers participating in its bulk electronic communications collections programs . . . .").

II. LEGAL STANDARD

Congress enacted the FOIA as a means "to open agency action to the light of public scrutiny." *Am. Civil Liberties Union v. U.S. Dep't of Justice*, 750 F.3d 927, 929 (D.C. Cir. 2014) (quoting *Dep't of Air Force v. Rose*, 425 U.S. 352, 361 (1976)). Disclosure is the "'basic policy'" of the Act. *Citizens for Responsibility & Ethics in Washington v. U.S. Dep't of Justice (CREW)*, 746 F.3d 1082, 1088 (D.C. Cir. 2014) (quoting *Dep't of Interior v. Klamath Water Users Protective Ass'n*, 532 U.S. 1, 8 (2001). At the same time, the statute represents a "balance [of] the public's interest in governmental transparency against legitimate governmental and private interests that could be harmed by release of certain types of information." *United Techs. Corp. v. U.S. Dep't of Def.*, 601 F.3d 557, 559 (D.C. Cir. 2010) (internal quotation marks and

citations omitted). Reflecting that balance, the FOIA contains nine exemptions set forth in 5 U.S.C. § 552(b), which "are explicitly made exclusive and must be narrowly construed." *Milner v. U.S. Dep't of Navy*, 562 U.S. 562, 565 (2011) (internal quotations and citations omitted) (citing *FBI v. Abramson*, 456 U.S. 615, 630 (1982)); *see CREW*, 746 F.3d at 1088; *Pub. Citizen, Inc. v. Ofc. of Mgmt. and Budget*, 598 F.3d 865, 869 (D.C. Cir. 2010). "[T]hese limited exemptions do not obscure the basic policy that disclosure, not secrecy, is the dominant objective of the Act." *Am. Civil Liberties Union v. U.S. Dep't of Justice (ACLU/DOJ)*, 655 F.3d 1, 5 (D.C. Cir. 2011) (quoting *Nat'l Ass'n of Home Builders v. Norton*, 309 F.3d 26, 32 (D.C. Cir. 2002)).

The agency invoking an exemption to the FOIA "bears the burden of showing that a claimed exemption applies." *Elec. Frontier Found. v. U.S. Dep't of Justice*, 739 F.3d 1, 7 (D.C. Cir. 2014); *see also CREW*, 746 F.3d at 1088; *Loving v. U.S. Dep't of Def.*, 550 F.3d 32, 37 (D.C. Cir. 2008); *Assassination Archives & Research Ctr. v. CIA*, 334 F.3d 55, 57 (D.C. Cir. 2003). In order to carry this burden, an agency must submit sufficiently detailed affidavits or declarations, a *Vaughn* index of the withheld documents, or both, to demonstrate that the government has analyzed carefully any material withheld, to enable the court to fulfill its duty of ruling on the applicability of the exemption, and to enable the adversary system to operate by giving the requester as much information as possible, on the basis of which he can present his case to the trial court. *See DeBrew v. Atwood*, No. 12-5361, 2015 WL 3949421, at *2 (D.C. Cir. June 30, 2015); *see also CREW*, 746 F.3d at 1088 ("The agency may carry that burden by submitting affidavits that 'describe the justifications for nondisclosure with reasonably specific detail, demonstrate that the information withheld logically falls within the claimed exemption, and are not controverted by either contrary evidence in the record nor by evidence of agency bad faith.'" (quoting *Larson v. U.S. Dep't of State*, 565 F.3d 857, 862 (D.C. Cir. 2009)); *Oglesby v.*

U.S. Dep't of the Army, 79 F.3d 1172, 1176 (D.C. Cir. 1996) ("The description and explanation the agency offers should reveal as much detail as possible as to the nature of the document, without actually disclosing information that deserves protection . . . [which] serves the purpose of providing the requestor with a realistic opportunity to challenge the agency's decision.").

The FOIA provides federal courts with the power to "enjoin the agency from withholding agency records and to order the production of any agency records improperly withheld from the complainant." 5 U.S.C. § 552(a)(4)(B). Moreover, a district court has an "affirmative duty" to consider whether the agency has produced all segregable, non-exempt information. *Elliott v. U.S. Dep't of Agric.*, 596 F.3d 842, 851 (D.C. Cir. 2010) (referring to court's "affirmative duty to consider the segregability issue *sua sponte*" (quoting *Morley v. CIA*, 508 F.3d 1108, 1123 (D.C. Cir. 2007))); *Stolt-Nielsen Transp. Grp. Ltd. v. United States*, 534 F.3d 728, 733-735 (D.C. Cir. 2008) ("'[B]efore approving the application of a FOIA exemption, the district court must make specific findings of segregability regarding the documents to be withheld.'" (quoting *Sussman v. U.S. Marshals Serv.*, 494 F.3d 1106, 1116 (D.C. Cir. 2007))); *see also* 5 U.S.C. § 552(b) ("Any reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt under this subsection.").

Summary judgment is appropriate when "there is no genuine dispute as to any material fact." Fed. R. Civ. P. 56. "In FOIA cases, '[s]ummary judgment may be granted on the basis of agency affidavits if they contain reasonable specificity of detail rather than merely conclusory statements, and if they are not called into question by contradictory evidence in the record or by evidence of agency bad faith.'" *Judicial Watch, Inc. v. U.S. Secret Serv.*, 726 F.3d 208, at 215 (D.C. Cir. 2013) (quoting *Consumer Fed'n of Am. v. U.S. Dep't of Agric.*, 455 F.3d 283, 287 (D.C. Cir. 2006) and *Gallant v. NLRB*, 26 F.3d 168, 171 (D.C. Cir. 1994)). "Ultimately, an

agency's justification for invoking a FOIA exemption is sufficient if it appears 'logical' or 'plausible.'" *Judicial Watch, Inc. v. U.S. Dep't of Def.,* 715 F.3d 937, 941 (D.C. Cir. 2013) (quoting *Am. Civil Liberties Union v. U.S. Dep't of Def. (ACLU/DOD),* 628 F.3d 612, 619 (D.C. Cir. 2011)); *Larson v. U.S. Dep't of State,* 565 F.3d 857, 862 (D.C. Cir. 2009) (quoting *Wolf v. CIA*, 473 F.3d 370, 374-75 (D.C. Cir. 2007)).

III. DISCUSSION

In the present case, "to the extent [the] plaintiff's [FOIA] request sought surveillance or other intelligence records, or communications about such records," the NSA issued the plaintiff a so-called "Glomar" response, which neither confirmed nor denied the existence of records relevant to the plaintiff's request.[4] Mem. Supp. Def.'s Mot. Summ. J. ("Def.'s Mem."). at 1, ECF No. 18-1. The Glomar response covered all documents sought by the plaintiff, except for those documents "concerning the government contracts and criminal and civil lawsuits specified by and involving plaintiff, or communications concerning those contracts and court cases."[5] *Id.* With respect to the plaintiff's request for documents concerning lawsuits and contracts, the NSA searched for but found no responsive documents. The plaintiff challenges both the NSA's Glomar response and the adequacy of the NSA's search for responsive documents. Each of those challenges is addressed separately below.

[4] Glomar responses are "named for the Hughes Glomar Explorer, a ship used in a classified Central Intelligence Agency project 'to raise a sunken Soviet submarine from the floor of the Pacific Ocean to recover the missiles, codes, and communications equipment onboard for analysis by United States military and intelligence experts.'" *Roth v. U.S. Dep't of Justice*, 642 F.3d 1161, 1171 (D.C. Cir. 2011) (quoting *Phillippi v. CIA*, 655 F.2d 1325, 1327 (D.C.Cir.1981)).

[5] As noted above, such materials refer primarily to categories 3 and 4 of the plaintiff's request, which sought documents relating to two contracts between the plaintiff and Defense Supply Center Philadelphia and documents relating to the two lawsuits brought against the plaintiff in the Northern District of Georgia. Compl. ¶ 11.

A. The NSA's Glomar Response

A Glomar response is "an exception to the general rule that agencies must acknowledge the existence of information responsive to a FOIA request and provide specific, non-conclusory justifications for withholding that information." *Roth v. U.S. Dep't of Justice*, 642 F.3d 1161, 1178 (D.C. Cir. 2011). Thus, a Glomar response allows an agency to respond to a FOIA request by neither confirming nor denying the existence of any records responsive to the request, on the grounds that "confirming or denying the existence of records would itself 'cause harm cognizable under a[ ] FOIA exception.'" *Id.* (quoting *Wolf*, 473 F.3d at 374). In issuing a Glomar response, the agency bears the burden of showing that the mere acknowledgement of whether it possesses or does not possess the requested records is protected from disclosure under a FOIA exemption. *See Wolf*, 473 F.3d at 374. To determine whether the acknowledgement of the existence or non-existence of agency records "fits a FOIA exemption, courts apply the general exemption review standards established in non-Glomar cases." *Wolf*, 473 F.3d at 374 (citing *Gardels v. CIA*, 689 F.2d 1100, 1103–05 (D.C. Cir. 1982)); *see also Am. Civil Liberties Union v. CIA (ACLU/CIA)*, 710 F.3d 422, 426 (D.C. Cir. 2013).

A Glomar response may be challenged in two distinct but related ways. A plaintiff may challenge the agency's assertion that confirming or denying the existence of any records would result in a cognizable harm under a FOIA exemption. *See, e.g., People for the Ethical Treatment of Animals v. Nat'l Institutes of Health*, 745 F.3d 535, 540 (D.C. Cir. 2014); *Elec. Privacy Info. Ctr. v. Nat'l Sec. Agency (EPIC/NSA)*, 678 F.3d 926, 932 (D.C. Cir. 2012); *Roth*, 642 F.3d at 1172. Alternatively, or in addition, a plaintiff may demonstrate that the agency has "officially acknowledged" the existence of a requested record previously. *See, e.g., ACLU/CIA*, 710 F.3d at 427 ("[T]he plaintiff can overcome a *Glomar* response by showing that the agency has already

disclosed the fact of the existence (or nonexistence) of responsive records, since that is the purportedly exempt information that a *Glomar* response is designed to protect."); *Moore v. CIA*, 666 F.3d 1330, 1333 (D.C. Cir. 2011) ("Moore does not challenge the CIA's reliance on exemptions (b)(1) and (b)(3) . . . . [but instead], Moore argues that the CIA has officially acknowledged that it maintains information responsive to Moore's FOIA request . . . ."); *Wolf*, 473 F.3d at 378 ("Although the CIA properly invoked Exemptions 1 and 3, Wolf asserts that the Agency waived both of them by officially acknowledging the existence of records . . . ."). The official acknowledgment doctrine recognizes that, in certain circumstances, the agency may have waived its right to claim a FOIA exemption over the existence or non-existence of the records. *See ACLU/CIA*, 710 F.3d at 426 ("[W]hen an agency has officially acknowledged otherwise exempt information through prior disclosure, the agency has waived its right to claim an exemption with respect to that information.").

The plaintiff asserts both bases to overcome the NSA's Glomar response. *See* Pl.'s Mem. at 27 ("Even if the Court were to find that the information that [the plaintiff] seeks is properly protected under the exemptions (which it is not), . . . the NSA's official acknowledgements over the last 18 months regarding its bulk collection programs . . . override even valid exemption claims."). The Court first addresses the propriety of the NSA's invocation of Exemptions 1 and 3 for its Glomar response before turning to the plaintiff's argument that the NSA has officially acknowledged the requested records.

1. *The NSA Properly Invoked Exemptions 1 and 3.*

The NSA grounds its Glomar response in Exemptions 1 and 3 of the FOIA statute. *See* Def.'s Mem. at 9. Although the plaintiff expressly challenges the propriety of the NSA's

invocation of Exemptions 1 and 3 for purposes of its Glomar response, the plaintiff devotes only two brief paragraphs of the more than 55 pages of briefing to this argument, and for good reason.

"In reviewing an agency's *Glomar* response, this Court exercises caution when the information requested 'implicat[es] national security, a uniquely executive purview.'" *EPIC/NSA*, 678 F.3d at 931 (quoting *Ctr. for Nat'l Sec. Studies v. U.S. Dep't of Justice*, 331 F.3d 918, 926–27 (D.C. Cir. 2003)). "[A]n agency's justification for invoking a FOIA exemption is sufficient if it appears 'logical' or 'plausible.'" *Wolf*, 473 F.3d at 374–75 (internal citations omitted). In the present case, the NSA invokes both Exemption 1 and Exemption 3 to support its Glomar response. Exemption 1 covers "matters 'specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and . . . in fact properly classified pursuant to such Executive order.'" *Larson v. U.S. Dep't of State*, 565 F.3d 857, 861 (D.C. Cir. 2009) (quoting 5 U.S.C. § 552(b)(1)). Exemption 3 covers "matters 'specifically exempted from disclosure by statute,' provided that such statute leaves no discretion on disclosure or 'establishes particular criteria for withholding or refers to particular types of matters to be withheld.'" *Id.* (quoting 5 U.S.C. § 552(b)(3)). "[I]n the FOIA context, [the D.C. Circuit has] consistently deferred to executive affidavits predicting harm to the national security, and . . . found it unwise to undertake searching judicial review." *Ctr. for Nat'l Sec. Studies*, 331 F.3d at 927.

Exemption 1 protects from disclosure records that are "(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 an Executive order." 5 U.S.C. § 552(b)(1); *see Milner v. U.S. Dep't of Navy*, 562 U.S. 562, 580 (2011) (noting that among the "tools at hand to shield national security information and other sensitive materials,"

the government has "[m]ost notably, Exemption 1 of FOIA [which] prevents access to classified documents."). Thus, an agency attempting to withhold information under Exemption 1 must show that the information has been classified in compliance with the classification procedures set forth in the relevant executive order and that only information conforming to the executive order's substantive criteria for classification has been withheld. *See Judicial Watch*, 715 F.3d at 941 (discussing "substantive and procedural criteria for classification"); *Lesar v. Dep't of Justice*, 636 F.2d 472, 483 (D.C. Cir. 1980) ("To be classified properly, a document must be classified in accordance with the procedural criteria of the governing Executive Order as well as its substantive terms.")).

In this case, the NSA has sufficiently established that the existence or non-existence of responsive records is classified under Executive Order ("E.O.") 13,526. This E.O. sets forth four requirements for the classification of national security information: (1) an original classification authority must classify the information; (2) the U.S. Government must own, produce, or control the information; (3) the information must be within at least one of eight protected categories enumerated in section 1.4 of the E.O.; and (4) the original classification authority must determine that the unauthorized disclosure of the information reasonably could be expected to result in a specified level of damage to the national security, and the classification authority is able to identify or describe the damage. *See* E.O. 13526 § 1.1(a).

The NSA avers that "[a]cknowledgement of the existence or non-existence of intelligence information referencing Plaintiff would reveal information that is currently and properly classified as set forth in Section 1.4(c) of E.O 13,526," which covers "intelligence sources [or] methods." NSA Sherman Decl. ¶ 31. Specifically, "[a]cknowledging the existence or non-existence of responsive records on particular individuals or organizations subject to surveillance

would provide . . . adversaries with critical information about the capabilities and limitations of the NSA . . . ." NSA's Sherman Decl. ¶ 33. As set forth in the NSA's declaration, "[c]onfirmation by NSA that a specific person's or organization's activities are not of foreign intelligence interest or that NSA is unsuccessful in collecting foreign intelligence information on their activities" would undermine the NSA's mission and permit adversaries to "accumulate information and draw conclusions about NSA's technical capabilities, sources, and methods." *Id.* Such information would permit adversaries to change their communications behavior or otherwise "alert targets that their existing means of communications are potentially safe." *Id.* ¶ 34. As a result, disclosure "could reasonably be expected to cause exceptionally grave and irreparable damage to the national security by providing . . . adversaries a road map that instructions them on which communication modes or personnel remain safe or are successfully defeating NSA's capabilities." *Id.*

The plaintiff challenges whether the acknowledgment of the existence or non-existence of the requested records would implicate intelligence sources and methods and would otherwise cause national harm. According to the plaintiff, "the bulk data collection programs under which the NSA obtained the information [the plaintiff] seeks sweep up not just the communications data of individuals that the NSA has specifically targeted, but rather, the data of millions of people whose communications cross the United States border, whether those people are targets of the NSA or not."[6] Pl.'s Mem. at 27. As a result, "the mere fact that the NSA possesses information regarding [the plaintiff's] communications would not reveal anything about [the plaintiff's] status as a target, thus keeping the NSA's 'intelligence sources and methods' intact." *Id.* In other words, because the NSA collects everything, disclosure would reveal nothing.

[6] The plaintiff does not challenge that the materials were classified by an individual with classification authority or that the NSA controls the materials. *See* Pl.'s Mem. at 26–27.

A variant of the plaintiff's argument was considered and rejected in *Competitive Enterprise Institute v. National Security Agency*, 2015 WL 151465, at *10, a case that also considered the NSA's issuance of a Glomar response in the context of documents allegedly maintained as a result of the bulk collection of telephony metadata. In *Competitive Enterprise Institute*, the Court expressly rejected the argument "that because the agency has admitted collecting the records in bulk, it would not reveal important intelligence information to acknowledge that EPA officials' calls were swept up in the collection." *Id.* The court reasoned that "were the agency required to confirm or deny the existence of records for specific individuals, it would begin to sketch the contours of the program, including, for example, which providers turn over data and whether the data for those providers is complete." *Id.* Indeed, the D.C. Circuit has cautioned, "'the fact that some information resides in the public domain does not eliminate the possibility that further disclosures can cause harm to intelligence sources, methods and operations.'" *ACLU/DOD*, 628 F.3d at 625 (quoting *Fitzgibbon v. CIA*, 911 F.2d 755, 766 (D.C. Cir. 1990)). "Minor details of intelligence information may reveal more information than their apparent insignificance suggests because, 'much like a piece of 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 (quoting *Gardels*, 689 F.2d at 1106). Just as in *Competitive Enterprise Institute*, the Court finds the NSA's explanation regarding the classification and potential national harm to be both "logical" and "plausible." *See Competitive Enter. Inst.*, 2015 WL 151465, at *10. Accordingly, the NSA has invoked Exemption 1 properly in support of its Glomar response.

The NSA's invocation of Exemption 3 is likewise proper. The NSA invokes a recognized withholding statute, Section 102A(i)(1) of the National Security Act of 1947, in

support of its Glomar response. *See ACLU/DOD*, 628 F.3d at 619. Section 102A(i)(1) protects "intelligence sources and methods from unauthorized disclosure." 50 U.S.C. § 3024. The plaintiff's challenges to Exemption 3 mirror the arguments made in opposition to Exemption 1. Since the Court has found the plaintiff's argument on that score to be unpersuasive, the plaintiff's Exemption 3 argument is similarly unavailing. [7]

2. *The NSA Officially Acknowledged a Limited Subset of Records.*

The central dispute between the parties concerns whether the NSA has previously acknowledged the existence of the records requested by the plaintiff, thereby waiving its right to claim an exemption regarding the existence *vel non* of any responsive records. The plaintiff claims that the NSA has made "multiple official disclosures that it collects a broad and voluminous scope of the telephone and electronic communications data of Americans through a series of programs with the compelled assistance of some of the largest U.S. telecommunications and internet service providers." Pl.'s Mem. at 20. In light of these disclosures, the plaintiff argues that the NSA has waived its right to issue a Glomar response to the plaintiff's FOIA

[7] The NSA also relies on two additional statutory provisions as support for withholding under Exemption 3: (1) Section 6 of the National Security Act of 1959 (codified at 50 U.S.C. § 3605), which provides that "[n]othing in this Act or any other law . . . shall be construed to require the disclosure of the organization or any function of the National Security Agency, or any information with respect to the activities thereof . . ."; and (2) a criminal statute, 18 U.S.C. § 798, which prohibits a person from knowingly and willfully disclosing "any classified information . . . concerning the communication intelligence activities of the United States . . . or . . . obtained by the processes of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes." Both statutes qualify as Exemption 3 statutes. *See Larson*, 565 F.3d at 868; *Linder v. NSA*, 94 F.3d 693, 698 (D.C. Cir. 1996). The NSA argues that, with respect to Section 6 of the National Security Act, revealing the existence of the requested records would "disclose information with respect to [NSA] activities, since any information about an intercepted communication concerns an NSA activity," *Linder*, 94 F.3d at 696 (quoting *Hayden v. NSA*, 608 F.2d 1381, 1389 (D.C. Cir. 1979)), and that, with respect to 18 U.S.C. § 798, acknowledging the existence of the requested records would disclose classified information "concerning the communication intelligence activities of the United States," *see Larson*, 565 F.3d at 868 (quoting 18 U.S.C. § 798). *See* Def.'s Mem. at 14–17. The Court need not opine about the sufficiency of these alternative bases, since Section 102A(i)(1) of the National Security Act provides ample support for the propriety of the NSA's invocation of Exemption 3.

request, which encompassed "all email, letter, telephonic, or other communications" by the plaintiff. *Id.* at 18–28.

The D.C. Circuit has recognized that if "the agency has officially acknowledged the existence of [a] record, the agency can no longer use a Glomar response, and instead must either: (1) disclose the record to the requester or (2) establish that its contents are exempt from disclosure and that such exemption has not been waived." *Moore*, 666 F.3d at 1333 (citations omitted); *see also Marino v. DEA*, 685 F.3d 1076, 1081 (D.C. Cir. 2012) ("[I]n the context of a Glomar response, the public domain exception is triggered when 'the prior disclosure establishes the existence (or not) of records responsive to the FOIA request,' regardless whether the contents of the records have been disclosed." (quoting *Wolf*, 473 F.3d at 379)). Even so, "[a] strict test applies to claims of official disclosure." *Moore*, 666 F.3d at 1333 (alteration in original) (internal quotation marks omitted). "[I]n order to overcome an agency's Glomar response based on an official acknowledgement, the requesting plaintiff must *pinpoint* an agency record that both matches the plaintiff's request and has been publicly and officially acknowledged by the agency." *Id.* (emphasis added).

> An agency's official acknowledgment must meet three criteria:
>
> 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 public through an official and documented disclosure.

Fitzgibbon, 911 F.2d at 765; *see also Moore*, 666 F.3d at 1333; *ACLU/DOD*, 628 F.3d at 620–21; *Wolf*, 473 F.3d at 378. The plaintiff "bears the burden of pointing to 'specific information in the public domain that appears to duplicate that being withheld.'" *EPIC/NSA*, 678 F.3d at 933 (quoting *Wolf*, 473 F.3d at 378). The plaintiff may not, however, point to mere media speculation. *See id.* at 933 n.5 ("[T]he national media are not capable of waiving NSA's

statutory authority to protect information related to its functions and activities."); *Competitive Enter. Inst.*, 2015 WL 151465, at *10 ("[S]peculation by the press—no matter how widespread—and disclosures in the press from unnamed sources are not sufficient to waive an agency's right to withhold information under FOIA.").[8]

In the present case, the plaintiff points to the NSA's public acknowledgements regarding its various bulk data collection programs—the telephony metadata program, the PR/TT program, the PRISM program, and the upstream collection program—to argue that the NSA has waived its right to issue a Glomar response. As explained below, the Court finds that the NSA has officially acknowledged the collection of certain telephony metadata from Verizon Business Network Services from April 25, 2013 through July 19, 2013, but has not otherwise officially acknowledged its possession of any other records sought by the plaintiff.

a) Telephony Metadata Program

The plaintiff has compiled multiple documents concerning the NSA's telephony metadata program, of which the NSA has acknowledged two publically released FISC orders detailing the program. Specifically, the plaintiff notes that the publically acknowledged FISC Secondary Order directed Verizon Business Network Services to provide to the NSA "on an ongoing daily basis . . . all call detail records or 'telephony metadata' created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls." Secondary Order at 2. The Secondary Order was limited to a 90-day period between April 25, 2013 and July 19, 2013, and included the originating and terminating

[8] Nor may a statement by an anonymous agency insider be deemed an "official acknowledgement" because an anonymous leak is presumptively an unofficial and unsanctioned act. *See ACLU/DOD*, 628 F.3d at 621–22 ("'[I]t is one thing for a reporter or author to speculate or guess that a thing may be so or even, quoting undisclosed sources, to say that it is so; it is quite another thing for one in a position to know of it officially to say that it is so.'" (quoting *Alfred A Knopf, Inc. v. Colby*, 509 F.2d 1362, 1370 (4th Cir. 1975))); *Afshar v. U.S. Dep't of State*, 702 F.2d 1125, 1130–31 (D.C. Cir. 1983) (distinguishing between "official acknowledgement" of information and "[u]nofficial leaks and public surmise").

telephone number along with the time and duration of the call. The plaintiff further contends that the NSA has conceded in public disclosures that the program has been in existence since at least May 2006 and that the NSA has admitted that as of January 3, 2014, "at least 15 different FISC judges have entered a total of 36 orders authorizing NSA's bulk collection of telephony metadata." Reply Supp. Pl.'s Cross Mot. Summ. J. ("Pl.'s Reply") at 9, ECF No. 26 (citing NSA's Shea Decl. ¶¶ 13-14). Taken together, the plaintiff argues that it communicated regularly with its legal counsel, a Verizon Business Network Services subscriber, and therefore, "based on the NSA's own admissions, some of [the plaintiff's] privileged communications with its counsel were almost certainly collected."[9] Pl.'s Reply at 9. Moreover, while the Secondary Order was limited to the period between April 25, 2013 and July 19, 2013, the plaintiff argues that the NSA "has made sufficient public acknowledgements of the recurring, ever-renewing nature of these orders that the existence of prior or subsequent orders is virtually certain." [10] Pl.'s Reply at 9. Thus, the plaintiff argues, at a minimum, the NSA has acknowledged the existence of records relating to its communications sent through Verizon Business Network Services between April 25, 2013 and July 19, 2013, and, at a maximum, has acknowledged the existence of records

[9] Throughout its briefing the plaintiff makes much of the fact that the NSA may have intercepted privileged communications between the plaintiff and its counsel. Regardless of the propriety of such interceptions, FOIA is not the appropriate vehicle to vindicate discovery abuses or otherwise conduct discovery. *See Williams & Connolly v. SEC*, 662 F.3d 1240, 1245 (D.C. Cir. 2011) ("FOIA is . . . [not] an appropriate means to vindicate discovery abuses . . . ."); *see also NLRB v. Sears, Roebuck & Co.*, 421 U.S. 132, 144 n. 10 (1975) ("The Act is fundamentally designed to inform the public about agency action and not to benefit private litigants."); *Renegotiation Bd. v. Bannercraft Clothing Co., Inc.*, 415 U.S. 1, 24 (1974) ("Discovery for litigation purposes is not an expressly indicated purpose of the Act."); *Neary v. Fed. Deposit Ins. Corp.*, No. 14-1167, 2015 WL 2375395, at *4 (D.D.C. May 19, 2015) ("'FOIA was not intended to be a discovery tool for civil plaintiffs.'" (internal quotations omitted)); *Johnson v. U.S. Dep't of Justice*, 755 F. Supp. 2, 5 (D.D.C.1991) ("FOIA is not a discovery statute.").

[10] To showcase the potential breadth of the captured information, the plaintiff points to a draft NSA Inspector General Report from 2009, which indicates that the NSA "could gain access to approximately 81% of the international calls into and out of the United States through three corporate partners: COMPANY A had access to 39%, COMPANY B 28%, and COMPANY C 14%." Pl.'s Mem. at 7. Although the draft report does not identify the three companies, the plaintiff notes that, as of 1999, MCI/Worldcom (now Verizon) was one of the three largest telecommunications providers. *See id.* (citing Common Carrier Bureau, FCC, 1999 International Telecommunications Data (Dec. 2000)).

relating to communications sent through Verizon Business Network Services and other providers since at least May 2006. *See* Pl.'s Reply at 9.

As noted previously, another decision in this District considered the propriety of an NSA Glomar response in light of the NSA's public statements regarding the bulk collection of telephony metadata. In *Competitive Enterprise Institute*, the plaintiff cited many of the same documents relied upon by the plaintiff in the present case: public statements by agency officials; an administration white paper; declarations of agency officials; newspaper reports; court opinions; and the Primary and Secondary Orders. *See* 2015 WL 151465, at *7–*10. After examining the statements, the court concluded that the "the sources . . . do not give any indication that the government collects metadata for *all* U.S. phone customers or even the subset of all Verizon Wireless users. As such, they do not show that the government has the specific records they seek." *Id.* at *5 (emphasis in original). The court's analysis turned on whether the NSA had acknowledged the participation of a service provider in the collection program. The plaintiff seeks to distinguish *Competitive Enterprise Institute* by noting that while the plaintiff in *Competitive Enterprise Institute* sought records relating to Verizon *Wireless*, the plaintiff in the present case has sought records pertaining to Verizon *Business Networks Services*, an acknowledged participant in the program. *See* Pl.'s Supp Aviad. Decl. ¶ 2. The plaintiff is correct, but only with respect to those documents obtained as a result of the officially acknowledged Secondary Order, *i.e.*, the telephony metadata collected from Verizon Business Network Services between April 25, 2013 and July 19, 2013.[11]

[11] Although the Secondary Order reflects only that the government *sought* such records from Verizon Business Network Services, the NSA has subsequently confirmed in public declarations that Verizon Business Network Services produced records and participated in the program. *See* NSA's Fleish Decl. ¶ 71 ("[T]he United States has not confirmed or denied the past or current participation of any specific provider in the telephony metadata program apart from the participation of VBNS for the approximately 90 day duration of the now-expired April 25, 2013 FISC Order.").

With respect to other telephone service providers and other periods of time, the plaintiff has not pointed to any disclosures documenting the specific telephone service providers that participated in the program and during what periods of time. Such imprecision will not suffice to overcome the NSA's Glomar response. The D.C. Circuit has expressly directed courts to apply the "official acknowledgement" exception "strictly," such that the "official acknowledgement" only extends to the *specific* records that are acknowledged by the agency. *See Moore*, 666 F.3d at 1333; *Wolf*, 473 F.3d at 378–79. Indeed, this Circuit requires that a plaintiff "*pinpoint* an agency record that both matches the plaintiff's request and has been publicly and officially acknowledged by the agency." *Moore*, 666 F.3d at 1333 (emphasis added). The plaintiff has been unable to pinpoint specific disclosures regarding the participation of other telephone service providers in the NSA's telephony metadata program, a circumstance present in other cases where courts have determined that the NSA did not officially acknowledge any additional participants in the telephony metadata program. *See Elec. Frontier Found. v. U.S. Dep't of Justice*, No. 11-CV-5221, 2014 WL 3945646, at *5-7 (N.D. Cal. Aug. 11, 2014) (rejecting argument that the identity of participants in the telephony metadata program "has lost its exempt character because the providers' names have been officially acknowledged."); *Competitive Enterprise Institute*, 2015 WL 151465, at *11.

Rather than pinpoint specific acknowledged disclosures, the plaintiff instead makes a series of logical deductions based on the nature of the telephony metadata program and general media speculation regarding the scope of the program to claim that the NSA has acknowledged other participants in the telephony metadata program. *See* Pl.'s Mem. at 7 (discussing implication of "Federal Communications Commission (FCC) report" discussing AT&T, Verizon, and Sprint as the nation's "three largest international telephone call providers"), *id.* at 8 n.6

("[T]he NSA's draft report strongly suggests that AT&T and Verizon have assisted the NSA in collecting both telephonic and email communications in the past); *id.* at 22–25. Logical deductions may not substitute for official acknowledgements, however. *See Valfells v. CIA*, 717 F. Supp. 2d 110, 117 (D.D.C. 2010) ("Logical deductions are not, however, official acknowledgments."), *aff'd sub nom. Moore v. CIA*, 666 F.3d 1330 (D.C. Cir. 2011).

The plaintiff's further reliance on *ACLU v. CIA*, 710 F.3d 422, 428–29 (D.C. Cir. 2013), is inapposite. In *ACLU*, the D.C. Circuit addressed the ACLU's FOIA request for documents relating to drone strikes. The D.C. Circuit rejected the CIA's Glomar response because the CIA "proffered no reason to believe that disclosing whether it has any documents at all about drone strikes will reveal whether the Agency itself—as opposed to some other U.S. entity such as the Defense Department—operates drones." *ACLU/CIA*, 710 F.3d at 428–29. Instead, the CIA's acknowledgment of its possession of documents relating to drones would reveal only that the CIA maintained an intelligence *interest* in drones. *Id.* at 428. In light of official acknowledgments by the CIA and the President, the Court concluded that it was neither "logical or plausible" for the CIA to contend that confirming the CIA's interest in drones would reveal information not already publically acknowledged. *Id.* Similarly, in the present case, the NSA officially acknowledged the collection of telephony metadata information from Verizon Business Network Services, making it neither logical nor plausible for the NSA to deny this fact now. The NSA's acknowledgement of its possession of telephony metadata from Verizon Business Network Services would reveal no new information not already in the public domain. This is not the case, however, with respect to telephony metadata records from other time periods or other service providers. *See EPIC/NSA*, 678 F.3d at 933 ("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."); *Students Against Genocide v. U.S. Dep't of State*, 50 F.Supp.2d 20, 25 (D.D.C. 1999) ("[T]here is certainly no 'cat out of the bag' philosophy underlying FOIA so that any public discussion of protected information dissipates the protection which would otherwise shield the information sought."). The NSA has not acknowledged any additional participants in the telephony metadata program or acknowledged receiving metadata from Verizon Business Network Services for any period outside of April 25, 2013 to July 19, 2013. To require the NSA to acknowledge the existence or non-existence of materials beyond that limited period would require the NSA to acknowledge information that has not otherwise been publically disclosed.

The plaintiff has been unable to pinpoint an official acknowledgment by the NSA of the specific records sought by the plaintiff beyond those records encompassed by the Secondary Order and relating to Verizon Business Network Services. *Moore*, 666 F.3d at 1333 ("[I]n order to overcome an agency's *Glomar* response based on an official acknowledgment, the requesting plaintiff must pinpoint an agency record that both matches the plaintiff's request and has been publicly and officially acknowledged by the agency."). Accordingly, the Court finds that the NSA's Glomar response was improper insofar as the NSA has previously acknowledged that it collected telephony metadata from Verizon Business Network Services between April 25, 2013 and July 19, 2013, and proper as to all other time periods and service providers.

b) Other Electronic Communications

Although the plaintiff compiled a robust record detailing the public disclosures of the NSA's telephony metadata program, the plaintiff has made no such showing regarding any of the other electronic communications programs—the PR/TT program, the PRISM program, and the

upstream collection program.[12] Indeed, to the contrary, the plaintiff *concedes* that the NSA has not acknowledged a service provider with respect to the bulk collection of electronic communications. *See* Pl.'s Mem. at 24 (conceding that the NSA "has not specifically named any telecommunications or Internet service providers participating in its bulk electronic communications collections programs."). Nonetheless, the plaintiff claims that other official acknowledgements are sufficient to override the NSA's Glomar response because the NSA has acknowledged "the broad scope of electronic communications collected through its programs." *Id.* at 25. Yet, for the reasons stated above, speculation by the plaintiff regarding the scope of the programs at issue will not suffice to overcome the NSA's Glomar response. *See Competitive Enter. Inst.*, 2015 WL 151465, at *9 (upholding Glomar response where plaintiff could "not name the specific companies that have produced this data to the government"). As a result, the plaintiff has failed in its burden to overcome the NSA's Glomar response with respect to all other electronic communications programs.

B. Improper Withholding

Although the NSA's Glomar response was improper with respect to certain Verizon Business Network Services documents, this finding does not end the inquiry into the NSA's FOIA response. The NSA makes the alternative argument that even if its Glomar response was improper as to the limited set of documents relating to Verizon Business Network Services, the terms of the Primary Order and Secondary Order do not permit the NSA to disclose any records to the plaintiff. *See* Mem. Further Supp. Def.'s Mot. Summ. J. ("Def.'s Reply") at 13–15, ECF No. 23.

[12] To the extent the NSA has made any acknowledgment regarding the records obtained during the course of the PR/TT program, the NSA has stated that all records obtained through the program have been destroyed. *See* NSA Fleisch Decl. ¶ 76 n.32 ("On December 7, 2011, the NSA completed the destruction of all PR/TT metadata collected under the authorization of the FISC from the agency's repositories.").

FOIA confers jurisdiction on the district court to compel an agency to release requested records only if those records are "improperly withheld." *Morgan*, 923 F.2d at 196 (internal quotation marks omitted). An improper withholding does not occur, and the FOIA does not apply, when documents are withheld pursuant to a court order specifically enjoining their release. In such circumstances, the agency "simply [has] no discretion . . . to exercise" and, thus, "has made no effort to avoid disclosure." *GTE Sylvania, Inc. v. Consumers Union of U.S., Inc.*, 445 U.S. 375, 386 (1980). As the D.C. Circuit explained in *Morgan*, "respect for the judicial process requires the agency to honor the injunction . . . . " 923 F.2d at 197 (citing *GTE Sylvania, Inc.*, 445 U.S. at 386–87). Although *GTE Sylvania* dealt with the situation of a court-ordered injunction, its core holding has not been so limited. Rather, where a court order circumscribes an agency's ability to produce documents such that the agency has "no discretion" to release the documents, the agency's failure to release documents will not be deemed improper. *See, e.g.*, *GTE Sylvania*, 445 U.S. at 386 (injunction); *Morgan*, 923 F.2d at 197 (sealing order); *Judicial Watch, Inc. v. U.S. Dep't of Justice*, 65 F. Supp.3d 50, 52 (D.D.C. Local Civil Rule 84.9); *Wagar v. U.S. Dep't of Justice*, 846 F.2d 1040, 1046-47 (6th Cir. 1988) (consent order); *see also Senate of Commw. of P.R. v. U.S. Dep't of Justice*, No. 84-1829, 1993 WL 364696, at *6 (D.D.C. Aug. 24, 1993) ("The Supreme Court has held that records covered by an injunction, protective order, or held under court seal are not subject to disclosure under FOIA." (internal citations omitted)).

Ultimately, "the proper test for determining whether an agency improperly withholds records [subject to a court order] is whether the [order], like an injunction, *prohibits* the agency from disclosing the records." *Morgan*, 923 F.2d at 197 (emphasis in original). The agency bears the burden of demonstrating that the responsive records are not subject to disclosure under the terms of a court order. *Id.* at 198. Merely stating that responsive records are subject to a court

order or other restriction is insufficient to demonstrate that "the court issued the [order] with the intent to prohibit the agency from disclosing the records," as required under the *Morgan* standard. *See Morgan*, 923 F.2d at 198 ("If the [agency] obtains a clarifying order stating that the [order] prohibits disclosure, the [agency] is obviously entitled to summary judgment."); *see also Awan v. U.S. Dep't of Justice*, 10 F. Supp. 3d 96, 107 (D.D.C 2014) (finding "that the defendants have not established the Southern District's sealing order as a proper basis for withholding the over decade old material witness warrant affidavit under the FOIA" where defendants lacked clarifying order), *vacated* 46 F. Supp. 3d 90, 92 (D.D.C. 2014) (concluding "that the government's withholding of the material witness warrant affidavit in compliance with the sealing order does not constitute an improper withholding under the FOIA" after the government obtained clarifying order); *Concepcion v. FBI*, 699 F.Supp.2d 106, 111–114 (D.D.C. 2010); *Senate of Commw. of P.R*, 1993 WL 364696, at *6–7, (D.D.C. Aug. 24, 1993).

The agency may satisfy its burden under *Morgan* by referring to (1) the order itself; (2) extrinsic evidence, such as papers filed with the court that provide the rationale for the sealing; (3) orders of the same court in similar cases that explain the purpose of the order; or (4) the court's general rules of procedures governing the order. *Morgan*, 923 F.2d at 198; *Concepcion*, 699 F.Supp.2d at 111. Upon finding that an order prohibits the agency from releasing the records, the agency is entitled to summary judgment on its withholding of the records. *Morgan*, 923 F.2d at 198. A review of the *Morgan* factors reveals that the NSA has no discretion to disclose the requested documents and its withholding in the present case was proper.

The text of the Primary Order makes plain the NSA's lack of discretion to access and disclose to the plaintiff the requested metadata. Indeed, the Primary Order permits the agency to access metadata records only in certain defined circumstances. Specifically, the Primary Order

"prohibit[s]" the government "from accessing business record metadata acquired pursuant to this Court's orders in the above-captioned docket and its predecessors . . . for *any purpose except as described herein*." Primary Order at 2 (emphasis added). The Primary Order designates two purposes. First, certain authorized technical personnel "may access the . . . metadata for purposes of obtaining foreign intelligence information." *Id.* Second, "technical personnel may access the . . . metadata to perform those processes needed to make it usable for intelligence analysis." *Id.* Neither scenario affords the NSA the discretion to access the metadata for purposes of complying with the plaintiff's FOIA request.

Although the Primary Order does not make specific reference to FOIA, the Primary Order is clear that the metadata may not be accessed "for *any* purpose except as" permitted by the Primary Order. Given the context of the Primary Order, the broad language regarding "*any* purpose" is sufficient to encompass FOIA. Such strict limitations regarding access to the collected metadata make abundant sense. In permitting the NSA to collect large amounts of personal information regarding U.S. citizens, the FISC was careful to put limitations on its access and use. The metadata may be accessed only for certain limited purposes (foreign intelligence) and only in certain limited ways (using specially approved searches). To permit FOIA plaintiffs (and thereby the public at large) access to all of the collected metadata would be to undermine the careful architecture erected by the FISC and enshrined in the Primary Order.

Likewise, the Primary Order restricts the subsequent dissemination of metadata information. Before the NSA may disseminate information pertaining to any U.S. person, certain high-level officials "must determine that the information identifying the U.S. person is in fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance." Primary Order at 3. To be sure, the

Primary Order does contemplate disclosure of the accessed metadata beyond the NSA in certain limited scenarios, including disclosure to the Executive Branch in order to (1) "enable them to determine whether the information contains exculpatory or impeachment information or is otherwise discoverable in legal proceedings" and (2) "facilitate their lawful oversight functions." *Id.* While such language might ordinarily weigh against the NSA in the *Morgan* analysis, the Primary Order's relative flexibility on disclosure is of less importance in the present case. As discussed, the NSA is forbidden under the terms of the Primary Order from *accessing* the collected telephony metadata in order to respond to the plaintiff's FOIA request. In other words, the only responsive telephony metadata records that the Primary Order might permit the NSA to disseminate concern telephony metadata records *previously accessed* as a result of an authorized search as part of an ongoing investigation. Consequently, the NSA "would only have communications in its searchable intelligence files of entities that are related to foreign intelligence investigations" because those were the only searches that would have been previously authorized under the Primary Order. Def.'s Reply at 9. Yet the existence or non-existence of such records as they relate to the plaintiff has never been acknowledged by the NSA. The records are therefore properly covered by the NSA's Glomar response and no disclosure is required.

Both the limitations upon the Court's holding and the peculiar circumstances of this case require highlighting. The instant case presents multiple competing interests all of significant public concern: personal privacy; national security; and transparency in government, along with the related concern of ensuring agency accountability. Under the plaintiff's theory on the applicability of the FOIA in this case, the telephony metadata records (and any email communications) held in databases by the NSA could potentially be searched and accessed by

any person through the timely submission of a FOIA request.[13] Fortunately, the FISC orders at issue carefully balanced the competing interests: The materials obtained pursuant to the telephony metadata program may be accessed only in the most limited fashion, and *not* for purposes of the FOIA. Given the plain language in the Primary Order and the general context of the telephony metadata program, the Court will not require the NSA to seek clarification from the FISC regarding whether the Primary Order contemplates prohibiting disclosure under the FOIA. Rather, as the Primary Order makes clear, the NSA is not permitted to access the requested materials for purposes of complying with a FOIA request. As a result, the NSA's failure to comply with the plaintiff's request was not "improper" and the NSA will not be required to disclose the requested documents to the plaintiff.

C. Defendant's Search

As noted, the NSA did not issue a Glomar response as to the entirety of the plaintiff's FOIA request. Rather, the NSA conducted a search for documents relating to the non-intelligence records sought by the plaintiff, *i.e.*, the plaintiff's request for documents relating to its business contracts and pending civil and criminal cases. The NSA's search yielded no results and the plaintiff correspondingly challenges the adequacy of the NSA's search for responsive records.

"The court applies a reasonableness test to determine the adequacy of a search methodology." *Morley*, 508 F.3d at 1114 (internal quotations and citations omitted) "[T]he adequacy of a FOIA search is generally determined not by the fruits of the search, but by the appropriateness of the methods used to carry out the search." *Iturralde v. Comptroller of*

[13] The plaintiff's theory also would raise the analytically "fraught" issue of when the querying of a database constitutes the creation of a new record not subject to FOIA. *See Nat'l Sec. Counselors v. C.I.A.*, 960 F. Supp. 2d 101, 160 n.28 (D.D.C. 2013). This issue was not formally framed by the parties and does not require resolution here.

Currency, 315 F.3d 311, 315 (D.C. Cir. 2003). "An agency may establish the adequacy of its search by submitting reasonably detailed, nonconclusory affidavits describing its efforts." *Baker & Hostetler LLP v. U.S. Dep't of Commerce*, 473 F.3d 312, 318 (D.C. Cir. 2006). "'Agency affidavits are accorded a presumption of good faith, which cannot be rebutted by purely speculative claims about the existence and discoverability of other documents.'" *DeBrew*, 2015 WL 3949421, at *2 (quoting *SafeCard Servs., Inc. v. SEC*, 926 F.2d 1197, 1200 (D.C. Cir. 1991)).

Agency affidavits should identify the terms search and explain how the search was conducted. *See Morley*, 508 F.3d at 1122 (citing *Oglesby v. U.S. Dep't of Army*, 920 F.2d 57, 68 (D.C. Cir. 1990)). The agency must submit, "[a] reasonably detailed affidavit, setting forth the search terms and the type of search performed . . . is necessary to afford a FOIA requester an opportunity to challenge the adequacy of the search and to allow the district court to determine if the search was adequate in order to grant summary judgment." *Debrew*, 2015 WL 3949424, at *2 (quoting *Oglesby*, 920 F.2d at 68). Only where "a review of the record raises substantial doubt, particularly in view of 'well defined requests and positive indications of overlooked materials,'" is summary judgment inappropriate. *Iturralde*, 315 F.3d at 314 (quoting *Valencia–Lucena v. U.S. Coast Guard*, 180 F.3d 321, 326 (D.C. Cir. 1999)). In the end, "[t]o prevail on summary judgment, the 'agency must show beyond material doubt . . . that it has conducted a search reasonably calculated to uncover all relevant documents.'" *Elliott v. U.S. Dep't of Agric.*, 596 F.3d 842, 851 (D.C. Cir. 2010) (quoting *Weisberg v. U.S. Dep't of Justice*, 705 F.2d 1344, 1351 (D.C. Cir. 1983)).

The NSA presents two affidavits from the NSA's Associate Director for Policy and Records in support of its search for records in the present case. The NSA tasked "its Office of

General Counsel, its acquisition organization, and its logistics organization" to conduct the relevant searches. NSA's Sherman Decl. ¶ 27. These organizations were chosen as they were deemed to be the organizations "that would possess records responsive to the Plaintiff's FOIA request, if any such records existed," as only those organizations maintained contract and litigation-related records. *Id.* The NSA determined that "[n]o other non-intelligence organization within the NSA would have such records" and that "if any non-intelligence related information response to the Plaintiff's FOIA request existed at the NSA, it would have been located by these three organizations in their respective filing system based on the search methodology" employed. NSA's Suppl. Sherman Decl. ¶¶ 2, 4. The NSA queried the records of the relevant organizations using three variants of the plaintiff's name and the numbers for the relevant contract. The records databases contained memoranda, meeting minutes, reports, manuals, and other documents. NSA's Sherman Decl. ¶ 27. Within the Office of General Counsel, attorneys also searched their Microsoft Outlook email accounts while administrative personnel and paralegals searched the organization's litigation filings systems. *Id.* The NSA also searched the "contracting management information system database," which is maintained in support of the NSA's contracting activity. *Id.* No responsive records were found as a result of any of these searches.

The plaintiff objects to the adequacy of the NSA's search, challenging both the scope of the search and the search terms employed. Neither objection withstands scrutiny. First, the plaintiff attacks the NSA's decision to limit its search of records to those contained in the Office of General Counsel, the acquisitions organization, and the logistics organization. The plaintiff argues that "[b]ecause those organizations only handle matters on behalf of the NSA, there was no reason for them to possess documents regarding contracts and lawsuits that did not involve

the Agency." Pl.'s Mem. at 30. The plaintiff misconstrues the nature of the NSA's search. The NSA searched these organizations because "[n]o other *non-intelligence organization* within the NSA would have [contract or litigation related records] because these other organizations would only have records of individuals and organizations . . . that have some affiliation with the NSA." NSA's Suppl. Sherman Decl. ¶ 2 (emphasis added). The fact that these organizations were unlikely to maintain the requested contracting and litigation records reflects not on the NSA's choice of organizations to search but on the nature of the plaintiff's FOIA request: the plaintiff sought records concerning a company with which the NSA neither engaged in contracts nor contract litigation.

Second, the plaintiff attacks the use of search terms employed by the NSA. The NSA used three variations of the plaintiff's name and the contract numbers for its search.[14] The plaintiff posits that the NSA should have used alternative search terms to yield responsive documents. Specifically the plaintiff suggests that the NSA should have included "PWC" as a search term, along with the legal case numbers for the relevant litigation. Pl.'s Reply at 16–17. Although the parties did agree regarding the scope of one of the plaintiff's requested categories of information, the parties did not discuss, and the plaintiff did not suggest, the use of any specific search terms. *See* NSA's Sherman Decl. ¶ 19.

"In general, the adequacy of a search is 'determined not by the fruits of the search, but by the appropriateness of [its] methods.'" *Hodge v. FBI*, 703 F.3d 575, 579 (D.C. Cir. 2013) (quoting *Iturralde*, 315 F.3d at 315). "[T]here is no bright-line rule requiring agencies to use the search terms proposed" by a plaintiff. *Physicians for Human Rights v. U.S. Dep't of Def.*, 675

[14] The plaintiff argues that the NSA failed to identify its search terms because it did not use quotation marks to designate the search terms identified in its declaration. *See* Pl.'s Reply at 15. The Court declines the plaintiff's invitation to impose a quotation marks requirement on the NSA as context reveals the terms in question to be the search terms employed by the NSA.

F. Supp. 2d 149, 164 (D.D.C. 2009). Federal agencies have discretion in crafting a list of search terms that "they believe[ ] to be reasonably tailored to uncover documents responsive to the FOIA request." *Id.* Where the search terms are reasonably calculated to lead to responsive documents, the Court should not "micro manage" the agency's search. *See Johnson v. Executive Office for U.S. Attorneys*, 310 F.3d 771, 776 (D.C. Cir. 2002) ("FOIA, requiring as it does both systemic and case-specific exercises of discretion and administrative judgment and expertise, is hardly an area in which the courts should attempt to micro manage the executive branch."); *Liberation Newspaper v. U.S. Dep't of State*, No. 13-0836, 2015 WL 709197, at *6 (D.D.C. Feb. 19, 2015) ("Where the agency's search terms are reasonable, the Court will not second guess the agency regarding whether other search terms might have been superior.").

The plaintiff's insistence on its own preferred search terms does not undermine the *reasonableness* of the NSA's search terms. Moreover, the plaintiff's terms are not without their own criticism. Indeed, the plaintiff proffers no explanation for how the inclusion of legal case numbers would be likely to yield responsive documents when the NSA *already* searched by the plaintiff's name. Moreover, while the NSA could have also used an abbreviation of the plaintiff's name as a search term, an abbreviation in a record typically follows after the *full name* is used, and the search terms used employed both full and shortened versions of the plaintiff's name. In short, the plaintiff offers only speculation as to the results of an alternative search, but speculation as to the potential results of a different search does not necessarily undermine the adequacy of the agency's actual search. Although the NSA could have used additional variations of the plaintiff's name or the legal case numbers, the NSA's search terms were reasonably calculated to lead to responsive documents.

Through two declarations by the NSA's Associate Director for Policy and Records, the NSA identified the records systems searched, the rationale for searching those records systems, the search terms employed, and averred that all files likely to contain responsive materials were searched. The plaintiff has presented no grounds for upsetting the presumption of regularity afforded to these declarations, and the Court finds that the declarations are reasonably detailed and the NSA's search was reasonably calculated to lead to responsive documents.[15]

IV. CONCLUSION

For the foregoing reasons, the NSA's Motion for Summary Judgment is granted and the plaintiff's Cross-Motion for Summary Judgment or, in the Alternative, for Limited Discovery is denied. An appropriate Order accompanies this Memorandum Opinion.

Date: July 10, 2015

Digitally signed by Hon. Beryl A. Howell, United States District Court Judge, U.S. District Court for the District of Columbia
DN: cn=Hon. Beryl A. Howell, United States District Court Judge, U.S. District Court for the District of Columbia, o, ou, email=Howell_Chambers@dcd.uscourts.gov, c=US
Date: 2015.07.10 15:26:42 -04'00'

BERYL A. HOWELL
United States District Judge

[15] Since the Court finds that both the declarations and the search itself were adequate, the plaintiff's alternative request for limited discovery regarding the NSA's search, *see* Pl.'s Mem. at 33, is denied.