BENJAMIN C. MIZER
Principal Deputy Assistant Attorney General
BRIAN STRETCH
United States Attorney
ANTHONY J. COPPOLINO
Deputy Branch Director
ERIC J. SOSKIN
JULIA A. BERMAN
Trial Attorneys
United States Department of Justice
Civil Division, Federal Programs Branch

P.O. Box 883
Washington, D.C. 20044
Telephone: (202) 616-8480
Facsimile: (202) 616-8470
Email: julia.berman@usdoj.gov

Attorneys for Defendants the Attorney General, et al.

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

TWITTER, INC., Plaintiff, v. LORETTA E. LYNCH, United States Attorney General, *et al.*, Defendants.	Case No. 14-cv-4480 **DEFENDANTS' MOTION FOR SUMMARY JUDGMENT** Date: January 17, 2016 Time: 2:00 pm Courtroom 1, Fourth Floor Hon. Yvonne Gonzalez Rogers

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Other Authorities

NOTICE OF MOTION

PLEASE TAKE NOTICE that, on January 17, 2016, at 2:00 p.m., before Judge Yvonne Gonzalez Rogers, the Defendants will move this Court for summary judgment.

Pursuant to Federal Rule of Civil Procedure 56, Defendants seek dismissal of the Plaintiff's Second Amended Complaint for the reasons set forth in Defendants' accompanying Memorandum of Points and Authorities.

MEMORANDUM OF POINTS AND AUTHORITIES

INTRODUCTION

Plaintiff Twitter, Inc. alleges in its Second Amended Complaint (ECF No. 114) ("SAC") that it seeks to publish information contained in a draft "Transparency Report" describing the amount of national security legal process that it received for the period of July 1 to December 31, 2013, pursuant to the Foreign Intelligence Surveillance Act ("FISA") and National Security Letter ("NSL") statutes.[1] *See* SAC ¶ 4. Twitter challenges the Government's determination that certain data contained in the draft report concerning FISA process it received during that period, if any, is properly classified. *See id.* ¶ 5. Twitter brings three overlapping claims, each of which alleges that restrictions on Twitter's dissemination of information determined by the Government to be classified impermissibly infringe on Twitter's First Amendment rights. *See id.* ¶¶ 71–96. After granting and denying in part the Government's motion to dismiss the First Amended Complaint, the Court directed the Government to move for summary judgment. *See* ECF No. 134. As set forth below, Twitter's challenges to the Government's classification determination are meritless, and the Government is therefore entitled to summary judgment on all claims.

Release of the information in Twitter's draft Transparency Report would harm national security. As explained in the Unclassified Declaration of Michael Steinbach ("Steinbach Decl.", attached as Ex. 1), disclosure of granular aggregate data regarding the Government's use of national security process would harm national security by providing foreign adversaries (such as

[1] Defendant's discussion of FISA process that Plaintiff could have received is not intended to confirm or deny that plaintiff has, in fact, received any such national security legal process.

terrorist organizations, intelligence services, and investigative targets) with insight into the Government's investigative and intelligence activities, and the evolution of those activities over time.[2] *See* Steinbach Decl. ¶¶ 6, 7. The Government has also prepared and made available to the Court, solely for *ex parte, in camera* review, a classified declaration by EAD Steinbach, which provides additional explanation as to why disclosure of the classified information in the draft report reasonably can be expected to cause serious damage to national security.[3] *See* Notice of Lodging of Classified Decl. of Michael Steinbach for *Ex Parte, In Camera* Review, ECF No. 144. These submissions, "with reasonable specificity, demonstrat[e] a logical connection between the detailed information [at issue] and the reasons for classification." *Shaffer v. DIA*, 102 F. Supp. 3d 1, 11 (D.D.C. 2015) (citing *McGehee v. Casey*, 718 F.2d 1137, 1148 (D.C. Cir. 1983)). The law is clear that courts should not "second guess" classification determinations by the Executive Branch, and should decline to substitute the speculation of plaintiffs or the Court's own intuition where, as here, the Government has provided a reasonably specific explanation of the logical connection between the information at issue and the reasons for its classification. *See, e.g.*, *Shaffer*, 102 F. Supp. 3d at 11; *Al-Haramain Islamic Found., Inc. v. Bush*, 507 F.3d 1190, 1203 (9th Cir. 2007).

Indeed, the case for deference is particularly strong here, where both Congress and the Executive Branch have reached a judgment regarding the appropriate balance between transparency and national security in disclosures concerning legal process. Specifically, the Director of National Intelligence ("DNI"), recognizing the importance of appropriate transparency with respect to the issuance of national security legal process served on

---

[2] Michael Steinbach is the Executive Assistant Director ("EAD") of the National Security Branch of the Federal Bureau of Investigation ("FBI"). *See* Steinbach Decl. ¶ 1. EAD Steinbach oversees, *inter alia*, the national security operations of the FBI's Counterintelligence Division, Counterterrorism Division, and Terrorist Screening Center, and holds original classification authority delegated by the Director of the FBI. *Id.* ¶¶ 2–3.

[3] It is well-established that Courts may rely on classified submissions provided *ex parte* and *in camera* to decide whether classification restrictions imposed by the Government on persons subject to non-disclosure obligations comply with the First Amendment. *See, e.g.*, *Stillman v. CIA*, 319 F.3d 546, 548–49 (D.C. Cir. 2003); *In re: Nat'l Sec. Letter*, 930 F. Supp. 2d 1064, 1078–79 (N.D. Cal. 2013); *In re: Nat'l Sec. Letters*, Case Nos. 11-cv-02173-SI, etc., 2016 WL 4501210 (N.D. Cal. Mar. 29, 2016).

communication service providers such as Twitter, has declassified the public reporting of certain aggregate data regarding the Government's use of national security process by recipients of such process. The DNI's declassification is coextensive with the "reporting bands" set forth in Section 603 of the USA FREEDOM Act, Pub. L. No. 114-23, 129 Stat. 268 (2015). These authorities reflect the judgment of the two political branches as to how much aggregate data regarding the receipt of national security process may be disclosed "while attempting not to compromise sensitive sources and methods of intelligence operations." Select Comm. On Intelligence, H. R. Rep. No. 113-452, pt. 2, § 701 (2015) ("HPSC/I Rep"). Twitter expends much ink criticizing these bands, but its contention that there would be no harm to national security from disclosure of the more granular classified information in its report is mistaken, particularly in light of the deference owed to the contrary judgment set forth in the EAD's declarations, the DNI's declassification, and the USA FREEDOM Act. As set forth in EAD Steinbach's declarations, disclosure of the information redacted from Twitter's report reasonably could be expected to result in damage to the national security, and that information is therefore properly classified.

Because all three Counts of the Complaint challenge the Government's classification determination on First Amendment grounds, *see* SAC ¶¶ 71–96, and, as Plaintiff acknowledges, it has no First Amendment right to publish classified information, *see id.* ¶ 73, Plaintiff's claims fail as a matter of law. Plaintiff's peripheral challenge to statutory requirements of the FISA is also meritless. For all of these reasons, as set forth in the instant submission and in EAD Steinbach's declarations, the Defendants respectfully request that the Court grant their motion for summary judgment.

BACKGROUND

I. Statutory and Regulatory Background

The President has charged the FBI with primary authority for conducting counterintelligence and counterterrorism investigations in the United States. *See* Exec. Order No. 12333 §§ 1.14(a), 3.4(a), 46 Fed. Reg. 59941 (Dec. 4, 1981). Today, the FBI carries out national security operations, including counterintelligence, counterterrorism, and other activities

to defeat national security threats directed against the United States through the FBI's National Security Branch, which is overseen by EAD Steinbach. *See* Steinbach Decl. ¶ 2.

The conduct of national security investigations and the collection, production, and dissemination of intelligence to support counterterrorism, counterintelligence, and other U.S. national security objectives requires the FBI to collect, analyze, and disseminate information. Congress has authorized the FBI to collect such information with a variety of legal tools, including various authorities under the FISA and pursuant to the supervision of the Foreign Intelligence Surveillance Court ("FISC"), an Article III court. *See* 50 U.S.C. § 1801 *et seq*. Because the targets of national security investigations and others who seek to harm the United States will take countermeasures to avoid detection, secrecy is often essential to protecting national security while effectively carrying out counterterrorism and counterintelligence investigations. *See Snepp v. United States*, 444 U.S. 507, 509 n.3 (1980). Recognizing that, Congress has empowered the FISC and the Executive Branch to maintain the confidentiality of national security legal process. *See, e.g.*, 50 U.S.C. §§ 1805(c)(2)(B), 1881a(h)(1)(A). In the USA FREEDOM Act, Congress likewise expressed its judgment regarding the manner in which recipients of national security process may publish information about their receipt of such process, in the aggregate, without imposing an unacceptable risk of harm to the national security.

A. FISA

Multiple provisions of FISA provide that the FISC may issue orders that "direct" recipients to provide certain information "in a manner that will protect the secrecy of the acquisition." *See, e.g.*, 50 U.S.C. §§ 1805(c)(2)(B), 1881a(h)(1)(A). For example, Titles I and VII of FISA provide that FISC orders "shall direct," and FISA directives issued by the Attorney General and DNI after FISC approval of an underlying certification "may direct," recipients to provide the Government with "all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition," without limitation. 50 U.S.C. § 1881a(h)(1)(A) (Title VII); *see also id.* § 1805(c)(2)(B) (similar language for Title I). Additionally, the orders "shall direct" and the directives "may direct" that recipients "maintain under security procedures approved by the Attorney General and the [DNI] any

records concerning the acquisition or the aid furnished" that such recipient maintains. 50 U.S.C. § 1881a(h)(1)(B) (Title VII); *see also id.* § 1805(c)(2)(C) (similar language for Title I). Consistent with the Executive Branch's authority to control classified information, these provisions explicitly provide for Executive Branch approval of the companies' procedures for maintaining the secrecy of records associated with FISA-authorized surveillance.

Other FISA titles that provide search or surveillance authorities also provide for secrecy obligations to be imposed. *See* 50 U.S.C. § 1824(c)(2)(B)-(C) (requiring Title III orders to require the recipient to assist in the physical search "in such a manner as will protect its secrecy" and to provide that "any records concerning the search or the aid furnished" that the recipient retains be maintained under appropriate security procedures); 50 U.S.C. § 1842(d)(2)(B) (requiring Title IV orders to direct that recipients "furnish any information, facilities, or technical assistance necessary to accomplish the installation and operation of the pen register or trap and trace device in such a manner as will protect its secrecy," and that "any records concerning the pen register or trap and trace device or the aid furnished" that the recipient retains shall be maintained under appropriate security procedures); 50 U.S.C. § 1861(d)(1) (providing that "[n]o person shall disclose to any other person that the [FBI] has sought or obtained tangible things pursuant to an order under" Title V of FISA). Accordingly, to the extent that Plaintiff has received any process pursuant to Titles I and VII of FISA, the Title VII directives would contain the statutorily permitted nondisclosure provisions, while the Title I orders would contain nondisclosure requirements that track the statutory provision. Likewise, Title III, IV, or V orders would be accompanied by the statutory requirements described above.

B. USA FREEDOM Act

Between 2013 and 2015, Congress considered various bills relating to the appropriate level of transparency regarding the Government's use of national security process. *See* Steinbach Decl. ¶ 18; *e.g.*, H.R. 3361, 113th Cong. (2014); S. 2685, 113th Cong. (2014). The bills were introduced to address developments affecting the Government's use of national security process, including the public interest in greater transparency, and the decision of the Second Circuit Court of Appeals in *John Doe, Inc. v. Mukasey*, 549 F.3d 861 (2d Cir. 2008).

These efforts culminated with enactment of the Uniting and Strengthening America By Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 ("USA FREEDOM Act").

In Section 603, codified at 50 U.S.C. § 1874, the USA FREEDOM Act reflects both Congress's and the Executive's judgment regarding the manner in which providers may lawfully report aggregate data reflecting their receipt of national security process. This section sets forth two reporting methods that are similar or identical to options previously available to communications providers following the declassification of such aggregate data by the DNI on January 27, 2014. *See* 50 U.S.C. §§ 1874(a)(1), (a)(3). In addition, Section 603 sets forth two additional methods of reporting on the receipt of national security process, which allow for even more precise numerical reporting of the number of process received over a longer time period. *See* 50 U.S.C. §§ 1874(a)(2), (a)(4). On July 2, 2015, the DNI, in his discretion and consistent with Section 603, declassified data related to national security process received by providers if publicly reported by means of one of the four options which are set forth in the USA FREEDOM Act. *See* Steinbach Decl. ¶ 20 (citing ODNI Memorandum for Distribution (ES 2015-00366)). Thus, in accordance with the DNI's discretionary declassification and as provided in the USA FREEDOM Act, recipients of national security process now may choose to publicly report information about the quantity of national security process they receive in one of four ways. The DNI's 2015 declassification decision and the four public reporting options enumerated in the USA FREEDOM Act thereby superseded the previous framework for public reporting set forth at the time of the January 27, 2014 DNI declassification determination.

II. Factual and Procedural Background

On April 1, 2014, Twitter sent a draft proposed Transparency Report to the FBI, seeking advice from the FBI as to which, if any, parts of the proposed report were classified and which could be lawfully published. *See* Steinbach Decl. ¶ 22. The report contained data reflecting the specific numbers and types of national security legal process that Twitter had received during the preceding six month period, from July 1 through December 31, 2013, in figures much more precise than had been declassified at that time, or have been declassified today. *Id.*

By letter dated September 9, 2014, the FBI General Counsel informed counsel for Twitter that, after careful review of Twitter's proposed Transparency Report, the FBI had concluded that certain information contained in the report was classified and could not lawfully be publicly released. *Id.* ¶ 23. The General Counsel specifically identified the information in question, informing Twitter that its proposed report "would disclose specific numbers of orders received, including characterizing the numbers in fractions or percentages, and would break out particular types of process received" in a manner that would disclose classified information. *Id.* On November 17, 2014, DOJ provided Twitter, through counsel, an unclassified version of Twitter's draft Transparency Report from which classified information had been redacted. *Id.* ¶ 24.

As the legal framework described above has evolved, so has this action. Plaintiff's original Complaint, ECF No. 1, focused on the disclosure options available in connection with the January 27, 2014 DNI declassification. The Court held that the claims therein were mooted by the passage of the USA FREEDOM Act. *See* ECF No. 85. Subsequently, the Court also dismissed Plaintiff's First Amended Complaint, finding that Plaintiff's constitutional claims were not viable absent a challenge to the classification of information in the draft Transparency Report. Order, ECF No. 113 at 8. The claims now operative, as set forth in Plaintiff's Second Amended Complaint, are detailed below.

Plaintiff's Claims in the Second Amended Complaint

Plaintiff asserts three duplicative causes of action, *see* SAC ¶¶ 71–96, based on which it seeks declaratory and injunctive relief to allow it to publish the information from the draft Transparency Report that the Government determined to be properly classified, as well as similar information covering future periods of time, *see id.*, Prayer for Relief.

Count I is styled as an implied cause of action under the First Amendment. *See id.* at 17. Plaintiff acknowledges that there is no First Amendment right to publish the information at issue if it is properly classified, *see id.* ¶ 73, but alleges, in sum, that because the information redacted from the draft Transparency Report is not properly classified, any prohibition on its disclosure constitutes a unconstitutional prior restraint on its speech, *see id.* ¶¶ 72, 76, 79–82, 84–86. There are several separate components to Count I.

First, Plaintiff alleges that the information redacted from the draft Transparency Report is not properly classified because it does not satisfy the requirements of Executive Order 13526. *Id.* ¶¶ 73–81. In support, Plaintiff cites media reports that it claims show "[t]he federal government often classifies information that could not be expected to cause damage to U.S. national security," *id.* ¶ 77, as well as legislation that the President signed into law in 2010 that was designed to reduce over-classification, *id.* ¶ 78. Specifically, as to the information at issue here, Plaintiff asserts "on information and belief" that the Government cannot demonstrate that the information at issue "poses a threat to U.S. national security, let alone one that is 'serious' or 'exceptionally grave.'" *Id.* ¶ 79. Further, Plaintiff argues that, because it seeks to publish information about activity it has conducted "using its own personnel and resources," the information at issue "is not 'owned by, produced by or for, or under the control of the United States Government.'" *Id.* ¶ 80 (quoting Exec. Order 13526 § 1.1). Plaintiff concludes that by "improperly classif[ying] information and then prevent[ing] its publication," the Government has violated the First Amendment. *Id.* ¶ 85.

Also as part of Count I, Plaintiff contends that the Court should issue a declaratory judgment that "the standards set forth in Executive Order 13526 constitute the only grounds on which the government may rely to prohibit disclosure of the redacted information in the draft Transparency Report." *Id.* It appears that this request is based on Plaintiff's contention that "[i]f the information that Twitter seeks to publish is not properly classified under Executive Order 13526, then the government has no other basis for prohibiting its disclosure." *Id.* ¶ 82. Although Plaintiff discusses its contention that FISA and FISC orders do not prohibit disclosure of aggregate data, and its alternative argument that FISA and FISC orders are unconstitutional if they do restrict the publication of such information, *id.* ¶¶ 83–84, Plaintiff does not otherwise explain the grounds for its position that no other authority could restrict the disclosure of the information at issue. *See id.* ¶¶ 71–86.

Count II is a duplicative First Amendment claim that mirrors the substance of the claim and relief sought in Count I, *compare id.* ¶¶ 85–86 *with id.* ¶¶ 90–91, but is asserted through the waiver of sovereign immunity provided under the Administrative Procedure Act ("APA"), *see id.*

at 21. Like Count I, the essence of Count II is Plaintiff's allegation that the information redacted from the draft Transparency Report is not properly classified, and that Plaintiff therefore has a First Amendment right to publish it. *See id.* ¶¶ 88–89. In Count II, Plaintiff challenges the "decision to censor Twitter's transparency report" as a "final agency action" through which it has suffered a legal wrong, because the agency decision not to allow publication "violates the First Amendment." *Id.* ¶ 88–89. Count II does not specifically identify the action to which it refers, but the SAC refers elsewhere to the September 9, 2014 letter from FBI General Counsel James A. Baker to counsel for Plaintiff, which advised Plaintiff that "information contained in the report is classified and cannot be publicly released." ECF No. 1-5 ("FBI Letter"); SAC ¶ 57 (describing and quoting the FBI Letter). The SAC also refers to the Government's production, on November 17, 2014, of a redacted version of the draft Transparency Report, from which the Government redacted classified national security information; *see* SAC ¶ 61. In any event, this "APA" claim amounts to another version of the same challenge to the Government's determination that information in the draft Transparency Report is classified, and for which Plaintiff seeks the same relief that it does with Count I: injunctive relief permitting publication of information that is not properly classified and three forms of declaratory relief.[4] *Compare id.* ¶¶ 85–86 *with id.* ¶¶ 90–91.

In Count III, Plaintiff raises another First Amendment claim, again nearly identical in scope, asserting that the Espionage Act is unconstitutional as it would allegedly be applied to it to foreclose publication of the information the Government has determined to be classified.[5] *See id.* ¶¶ 92–96. Plaintiff avers that it has a "reasonable concern" that it would face prosecution if it

[4] Specifically, Plaintiff seeks: 1) a declaration that Executive Order 13526 is the only basis on which the Government can restrict publication of the information reacted from the draft Transparency Report; 2) a declaration that the FISA nondisclosure provisions do not restrict publication of the information redacted from the draft Transparency Report; and 3) a declaration that the information redacted from the draft Transparency Report was improperly classified, and that Plaintiff therefore has the right to publish such information. Id. ¶ 90. Only the last listed declaration pertains to the decision that Plaintiff seeks to challenge—the Government determination that information is classified, see id. ¶¶ 57, 61, 88.

[5] The Espionage Act of 1917, 40 Stat. 217, was enacted to protect information related to national defense from being used to the advantage of adversaries. It has been amended numerous times and is currently codified at 18 U.S.C. § 793 *et seq*.

were to disclose the classified information redacted from its draft Transparency Report. *Id.* ¶ 93. Arguing that any such prosecution would violate its First Amendment right to speak truthfully about matters of public interest, Plaintiff seeks declaratory and injunctive relief barring any such prosecution. *Id.* ¶¶ 95–96. In short, all three Counts are First Amendment claims that turn on one issue: whether the Government properly determined that information redacted from the Transparency Report is classified, *i.e.*, that its disclosure reasonably could be expected to harm national security.

The Prayer for Relief largely reflects the requests for relief in Plaintiff's Counts I–III, but also contains a freestanding request that the Court enter a declaratory judgment that "[t]he FISA secrecy provisions are facially unconstitutional under the First Amendment because they do not require nondisclosure orders to contain a defined duration." *See id.* Prayer for Relief, (A)(v). That request is not tethered to Plaintiff's request to publish its draft Transparency Report, which, as described above, is the focus of all three of the Counts asserted in the SAC. *See id.* ¶¶ 71–96.

LEGAL STANDARD

Summary judgment is appropriate where "there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a); *see Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 247 (1986). Summary judgment is properly regarded "not as a disfavored procedural shortcut, but rather as an integral part of the Federal Rules as a whole, which are designed 'to secure the just, speedy and inexpensive determination of every action.'" *Celotex Corp. v. Catrett*, 477 U.S. 317, 327 (1986) (quoting Fed. R. Civ. P. 1). In cases where the central dispute is whether information is properly classified, summary judgment is proper if the Court is able to reach such a determination based upon materials submitted by the Government, including through *in camera* and *ex parte* review. *See Stillman*, 517 F. Supp. 2d 32 (D.D.C. 2007) (granting summary judgment upon remand).

ARGUMENT

I. The Court Should Grant Judgment for Defendants Based on the Detailed Showing that Information in the Transparency Report is Properly Classified.

All three Counts of the Complaint rest on Plaintiff's claim that it has a First Amendment right to publish the information found by the Government to be classified in Twitter's draft

Transparency Report. As this Court recognized, however, "[t]he First Amendment does not permit a person subject to secrecy obligations to disclose classified national security information." ECF No. 113 at 8 (citing *Snepp*, 444 U.S. at 509 n.3; *Wilson v. CIA*, 586 F.3d 171, 183 (2d Cir. 2009); *and Stillman*, 319 F.3d 548–49); *see also Berntsen v. CIA*, 618 F. Supp. 2d 27, 29-30 (D.D.C. 2008). Indeed, Plaintiff acknowledges that it has no First Amendment right to publish properly classified information. SAC ¶ 73.

It is therefore undisputed that Plaintiff has no First Amendment right to publish the information redacted from the draft Transparency Report if that information is properly classified. As discussed below, EAD Steinbach, a senior FBI official with extensive experience in FBI national security operations and who exercises original classification authority, has determined that this information meets the standards set forth in Executive Order 13526, 75 Fed. Reg. 707 (Dec. 29, 2009). Section A explains why the Court should grant deference to the judgment of the Executive Branch on this issue, while Section B describes, to the extent possible on the public record, the reasons for EAD Steinbach's determination.

A. The Government's Classification Decision Warrants the Utmost Deference.

"[C]ourts have traditionally shown the utmost deference" to the Executive Branch's constitutional authority to classify and control access to national security information. *Dep't of Navy v. Egan*, 484 U.S. 518, 530 (1988) (quoting *United States v. Nixon*, 418 U.S. 683, 710 (1974)); *Ctr. for Nat'l Sec. Studies v. U.S. Dep't of Justice*, 331 F.3d 918, 928 (D.C. Cir. 2003) (noting the D.C. Circuit has emphatically "reject[ed] any attempt to artificially limit the long-recognized deference to the executive on national security issues) (reviewing cases)). Consistent with that practice, the Ninth Circuit has "acknowledge[d] the need to defer to the Executive on matters of . . . national security," emphasizing that the Court "surely cannot legitimately find [itself] second guessing the Executive in this arena." *Al-Haramain*, 507 F.3d at 1203.

In *Al-Haramain*, the Ninth Circuit (reviewing an assertion of the state secrets privilege) considered the Government's conclusion that release of information about whether Al-Haramain had been subject to Government surveillance under the "Terrorist Surveillance Program" would damage national security. In particular, the court considered whether the Government could

protect a classified document, marked TOP SECRET, that had been inadvertently disclosed by the Government to the plaintiff during an administrative process involving whether the plaintiff should be designated as a global terrorist organization. The Court observed that "at some level, the question whether Al-Haramain has been subject to NSA surveillance may seem, without more, somewhat innocuous." *Id.* Underscoring the point, the Court noted Al-Haramain's argument that "[its] status as a 'Specially Designated Global Terrorist' suggest[ed] that the government [was] in fact intercepting [its] communications" under the Terrorist Surveillance Program. *Id.* However, the Court emphasized that its "judicial intuition about this proposition [was] no substitute for documented risks and threats posed by potential disclosure of national security information." *Id.*[6]

The deference given to the Executive in this sphere makes sense. Because of the President's constitutional role in national security matters, the Executive Branch is uniquely situated to assess the national security consequences of the disclosure of particular information. *Frugone v. CIA*, 169 F.3d 772, 775 (D.C. Cir. 1999) ("Mindful that courts have little expertise in either international diplomacy or counterintelligence operations, we are in no position to dismiss the CIA's facially reasonable concerns."); *Egan*, 484 U.S. at 529 (judgments as to harm that would result in the disclosure of certain information "must be made by those with the necessary expertise in protecting classified information"). The Executive Branch, in particular the United States Intelligence Community, has the complete picture of the manner in which particular disclosures may pose a danger to national security. In large part, this is due to the fact that adversaries can combine any individual disclosure with information from other sources to draw conclusions harmful to national security, a process that courts commonly refer to as the "mosaic" theory of intelligence-gathering:

> It requires little reflection to understand that . . . foreign intelligence gathering in this age of computer technology is more akin to the construction of a mosaic than it is to the management of a cloak and dagger affair. Thousands of bits and pieces

[6] While *Al-Haramain* involved an assertion of the state secrets privilege, review of the classification determination at issue here entails the same inquiry—whether information may properly be protected in the interests of national security—and thus the same deference is due. The Court in *Al-Haramain* found that the privilege had been appropriately invoked based on the Government's public and *in camera* and *ex parte* submissions. 507 F.3d at 1203–04.

> of seemingly innocuous information can be analyzed and fitted into place to reveal with startling clarity how the unseen whole must operate . . . . "The courts, of course, are ill-equipped to become sufficiently steeped in foreign intelligence matters to serve effectively in the review of secrecy classifications in that area."

Halkin v. Helms, 598 F.2d 1, 8–9 (D.C. Cir. 1978) (quoting *United States v. Marchetti*, 466 F.2d 1309, 1318 (4th Cir. 1972)). The Government's assessment of potential harm must be given deference because of the expertise and experience of intelligence officials in understanding when and why "each individual piece of intelligence information, much like a piece of jigsaw puzzle, may aid in piecing together other bits of information even when the individual piece is not of obvious importance itself." *Gardels v. CIA*, 689 F.2d 1100, 1106 (D.C. Cir. 1982) (quoting *Halperin v. CIA*, 629 F.2d 144, 150 (D.C. Cir. 1980)).

In light of the absence of such necessary experience and "broad view" of foreign intelligence matters, *see Marchetti*, 466 F.2d at 1318, the judiciary should not second-guess the national security and foreign relations concerns articulated by the Executive Branch. *See Al-Haramain*, 507 F.3d at 1203 (discussed above); *Ctr. for Nat'l Sec. Studies*, 331 F.3d at 928 ("It is abundantly clear that the government's top counterterrorism officials are well-suited to make this predictive judgment. Conversely, the judiciary is in an extremely poor position to second-guess the executive's judgment in this area of national security."); *McGehee*, 718 F.2d at 1149 ("[J]udicial review of CIA classification decisions, by reasonable necessity, cannot second-guess CIA judgments on matters in which the judiciary lacks the requisite expertise."). For these reasons, "it is the responsibility of the [Executive], not that of the judiciary, to weigh the variety of complex and subtle factors in determining whether disclosure of information may lead to an unacceptable risk of compromising the Agency's intelligence-gathering process." *CIA v. Sims*, 471 U.S. 159, 180 (1985); *see also Holder v. Humanitarian Law Project*, 561 U.S. 1, 34 (2010) ("when it comes to collecting evidence and drawing factual inferences [on national security matters], the lack of competence on the part of the courts is marked, and respect for the Government's conclusions is appropriate"). This Court should, therefore, accord substantial weight to the Government's determination concerning the national security harms that could reasonably be expected to result from disclosure of the information redacted from Twitter's draft Transparency Report.

Moreover, the views of the Executive should be afforded even greater weight, where, as here, Congress and the Executive agree on the need and manner for protecting the type of information at issue. *Cf. Zivotofsky v. Kerry*, 135 S. Ct. 2076, 2083–84 (2015) (quoting *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 635 (1952) (Jackson, J. concurring)) ("when the President acts pursuant to an express or implied authorization of Congress, his authority is at its maximum, for it includes all that he possesses in his own right plus all that Congress can delegate."). Actions taken by the Executive with specific congressional endorsement, therefore, are "supported by the strongest presumptions and the widest latitude of judicial interpretation, and the burden of persuasion would rest heavily upon any who might attack it." *Dames & Moore v. Regan*, 453 U.S. 654, 656 (1981) (quoting *Youngstown*, 343 U.S. at 637) (Jackson, J., concurring). Here, the reporting options available under Section 603 reflect both the judgment of the DNI to declassify aggregate data concerning national security process, if reported in a manner consistent with one of the four formats set forth in the Act, and Congressional judgment regarding the measure of disclosure that can be permitted "while attempting not to compromise sensitive sources and methods of intelligence operations." HPSC/I Rep. § 701.

Plaintiff's claims seeking to publish even more granular data than that permitted by the bands is therefore contrary not only to the judgment of the Executive Branch, but also the informed policy judgment of Congress. Plaintiff's speculation that no harm would be wrought by its proposed disclosure, *see* SAC ¶ 79, cannot outweigh the determinations of both political branches. Indeed, courts have repeatedly, and necessarily, rejected such non-governmental views regarding whether a particular disclosure may harm national security, even when presented by former intelligence officers. *See, e.g.*, *Snepp*, 444 U.S. at 512 ("When a former agent relies on his own judgment about what information is detrimental, he may reveal information that the CIA – with its broader understanding . . . could have identified as harmful."); *Gardels*, 689 F.2d at 1106 & n.5 (former agent's "own views as to the lack of harm which would follow the disclosure" are insufficient to justify further inquiry beyond the

Government's "plausible and reasonable" informed position).[7] Here, too, the Court should reject Plaintiff's apparent view that its proposed disclosures would be innocuous; that view cannot overcome the Executive Branch's judgment and determination that disclosure of the classified information at issue reasonably could be expected to damage national security. *See* Steinbach Decl. at ¶¶ 29, 39.

B. The Information Redacted from the Draft Transparency Report is Properly Classified Pursuant to Executive Order 13526.

Pursuant to the President's constitutional authority to protect and control national security information, *see Egan*, 484 U.S. at 527 (citing U.S. Const., Art. II, § 2), the President issued Executive Order 13526: Classified National Security Information. This Executive Order requires four conditions for the classification of national security information: (1) the information must be classified by an "original classification authority"; (2) the information must be "owned by, produced by or for, or [be] under the control of" the Government; (3) the information must fall within one of the authorized classification categories listed in section 1.4 of the Executive Order; and (4) the original classification authority must "determine[ ] that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security" and must be "able to identify or describe the damage." Exec. Order 13526, § 1.1. Additionally, Executive Order 13526 contains procedures for "derivative" classification, which occurs when "information that is already classified" is "incorporat[ed], paraphras[ed], restat[ed], or generat[ed] in new form." *Id.* § 6.1(o). Persons who "reproduce, extract, or summarize classified information . . . need not possess original classification authority" and are directed to "observe and respect original classification decisions," including by "carry[ing] forward to any newly created documents the pertinent classification markings." *Id.* § 2.1(a), (b). Here, the information at issue meets all four classification requirements, pursuant to established principles governing original and derivative classification.

[7] *See also Halperin v. Nat'l Sec. Council*, 452 F. Supp. 47, 51 (D.D.C. 1978) (Even though plaintiff was a self-proclaimed "scholar and actor in the field of foreign policy and national security," nothing in "plaintiff's submissions justifie[d] the substitution of this Court's judgment or the informed judgment of plaintiff for that of the officials constitutionally responsible for the conduct of United States foreign policy as to the proper classification of [documents]."), *aff'd*, 612 F.2d 586 (D.C. Cir. 1980).

1. An Original Classification Authority Has Determined that the Information Is Classified.

The information redacted from the draft Transparency Report has been determined to be properly classified by an original classification authority. Executive Order 13526 defines "Original Classification Authority" as "an individual authorized in writing . . . by agency heads or other officials designated by the President, to classify information in the first instance." Exec. Order 13526, § 6.1(gg). As described above, EAD Steinbach, as the head of the FBI's National Security Branch, exercises original classification authority delegated by the Director of the FBI. *See* Steinbach Decl. ¶ 3. In the exercise of that authority, he has determined that the information redacted from the Transparency report is properly classified, satisfying the criteria set forth in Section 1.1(1) of Executive Order 13526. *Id.* ¶¶ 29, 39.

2. The Information "Is Owned By, Produced By or For, or Is Under the Control of" the Government.

The information at issue is also "owned by, produced by or for, or is under the control of" the Government, as required under Section 1.1(2). At issue in this case are aggregate numbers concerning national security process the Government has served upon Twitter. In particular, Plaintiff puts at issue the disclosure of information concerning FISA process it has received, if any, or may receive in the future, as well as NSLs issued by the Government. Any FISA orders or directives served upon Twitter, or any NSLs issued to Twitter, were undoubtedly "owned by" and "produced by or for" the Government. Such materials do not lose their secrecy protections when they are served upon third parties. To the contrary, parties who are served with such process are subject to secrecy obligations imposed by the Government, typically in the form of nondisclosure agreements with recipients of such process, *see* E.O. 13526, § 4.1(2). Furthermore, secrecy obligations may be supported by judicial orders (such as from the FISC) to maintain the secrecy of legal process where the Government determines that is required to protect national security interests. *See supra*, Background, I.A (describing FISA secrecy authorities); *see also, e.g.*, 18 U.S.C. § 2709(c) (providing for imposition of nondisclosure requirements on NSL recipients). These materials, therefore, do not lose the characteristics of

having been owned, produced by, and under control of the Government when the Government seeks to serve legal process on third parties and entrusts those parties with sensitive information.

The principles concerning derivative classification underscore this point. Executive Order 13526 recognizes that individuals may "reproduce, extract, or summarize classified information." In such instances, the material need not be classified by an original classification authority; instead, people who produce such materials are directed to "observe and respect original classification decisions." E.O. 13526 § 2.1(a), (b). Otherwise, classified materials would lose their protections anytime another person summarized or discussed those materials in some other form. The same principles apply here to Twitter's summary of any classified materials it has received: where sensitive materials are produced by the Government, served upon a third party, and subject to binding secrecy requirements, the materials do not lose their protected character whenever a third party seeks to summarize those materials in some other form. Aggregate descriptions concerning receipt of national security process thus flow directly from any materials that the Government has created and given to Twitter.[8]

3. The Information Falls Within the Classification Categories of Section 1.4 of Executive Order 13526.

The information redacted from the draft Transparency Report falls squarely within three of the classification categories under Section 1.4 of Executive Order 13526. As relevant here, that section provides that information shall be considered for classification if it pertains to: intelligence activities (including covert action), intelligence sources or methods, or cryptology, Exec. Order 13526, § 1.4 (c); foreign relations or foreign activities of the United States, *id.* § 1.4 (d); or vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, *id.* § 1.4 (g).

As stated in EAD Steinbach's Declaration, the disclosure of the information at issue would provide our adversaries a clear picture of the Government's surveillance activities pertaining to national security investigations, thereby revealing information pertaining to

[8] To be sure, Twitter also contends that the information at issue here is not properly classified because it has been summarized in such a way as to avoid the risk of any harm to national security. In that regard, Twitter is mistaken for the reasons explained in Section B.4.

intelligence sources and methods, and foreign relations or foreign activities of the United States, falling within Section 1.4(c) and 1.4 (d). *See* Steinbach Decl. ¶¶ 30–38. Such disclosures also would allow adversaries to infer whether or not the Government has acquired a collection capability on particular communication services, thereby revealing information pertaining to "capabilities of systems . . . relating to the national security," falling within Section 1.4(g). *See id.* Similarly, because such disclosures could also permit adversaries to identify "safe" platforms on which their communications are not likely to be subject to surveillance, they would also reveal information pertaining to "vulnerabilities . . . of systems . . . relating to the national security." E.O. 13526 at § 1.4(g); *see id.* The classified Declaration of EAD Steinbach, submitted to the Court *in camera* and *ex parte*, further elaborates on why the information at issue falls within the protections of the Executive Order.

4. Disclosure of the Information Reasonably Could Be Expected to Cause Identifiable Harm to National Security.

Finally, in satisfaction of Section 1.1(4) of the Executive Order, EAD Steinbach, an original classification authority, "has determined that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security," and EAD Steinbach has been "able to identify or describe the damage." The Supreme Court and Ninth Circuit guidance discussed above, as well as the approach taken by other courts to have considered the Government's explanations of its classification determinations, *see* Argument Section I.A, indicate that the Court should review the judgments of EAD Steinbach (and related classification judgments by the DNI) with "utmost deference," consistent with the expertise and constitutional authority of the Executive in national security matters. And here as well, the judgment of Congress, reflected in the disclosure bands set forth in the USA FREEDOM Act, provides still more reason to give great weight to the Executive's judgment regarding the level of detail about a company's receipt of national security process that can be publicly disclosed without incurring an unacceptable risk to national security.

Of course, deferential review does not mean that courts have no role to play in the review of a Government decision that information cannot be published because it is classified. *See Ctr. for Nat'l Sec. Studies*, 331 F.3d at 932. In such cases, courts focus on whether the Government

"in fact had good reason to classify, and therefore censor the materials at issue." *Shaffer*, 102 F. Supp. 3d at 11 (citing *McGehee*, 718 F.2d at 1148). Specifically, courts require that the Government justify its redactions "with reasonable specificity, demonstrating a logical connection between the detailed information and the reasons for classification." *Id.* (citing *McGehee*, 718 F.2d at 1148–49); *accord*, *e.g.*, *Wilson v. CIA*, 586 F.3d 171, 185–86 (2d Cir. 2009) (same). "The court's task is not to second-guess the Agency, but simply to ensure that its reasons for classification are rational and plausible ones." *Wilson*, 586 F.3d at 185–86.

As the Government explained in its Opposition to the Plaintiff's Motion for an Order Directing Defendants to Initiate an Expedited Security Clearance Process for Plaintiff's Counsel, *see* ECF No. 133 at 2–3, 4–6, in analogous cases addressing a challenge by persons subject to nondisclosure obligations pursuant to a Government determination that information cannot be published because it is classified, courts conduct the above inquiry by examining both the materials submitted by the Government in its publicly-available briefing, as well as the Government's classified explanations, submitted *in camera* and *ex parte*. The D.C. Circuit in *McGehee* "anticipate[d] that *in camera* review of affidavits, followed if necessary by further judicial inquiry, would be the norm" in such cases," 718 F.2d at 1149, and, in *Stillman*, held that the district court had erred when it did not begin its review with that step. *See* 319 F.3d at 548–49 (remanding to the district court for that court "to determine first whether it [could] resolve the classification [of the information at issue] ex parte"). Since *Stillman*, courts have followed this guidance. *See Shaffer*, 102 F. Supp. 3d at 10 ("a district court must first attempt to resolve a classification challenge ex parte") (citing *Stillman*, 319 F.3d at 548–49); *Boening v. CIA*, 579 F. Supp. 2d 166, 174 (D.D.C. 2008); *Berntsen*, 618 F. Supp. 2d at 28, 30.

This line of authority presents the closest analogue to the present situation, and, as this Court noted in its May 2, 2016 Order, these cases "describ[e] [the] procedures for [a] challenge to classification decision[s]" in this setting. ECF No. 113 at 8 (citing *Stillman*, 319 F.3d at 548–49). Accordingly, the Government has followed those procedures, and submitted the Classified Declaration of EAD Steinbach, solely for *in camera* and *ex parte* review, which provides a detailed explanation of the reasons why, in the judgment of the EAD of the FBI, the disclosure of

the information at issue here reasonably could be expected to cause serious damage to the national security.

To the extent possible consistent with national security, EAD Steinbach's unclassified declaration discusses those reasons on the public record. *See generally* Ex. 1. Specifically, EAD Steinbach explains that disclosure of the granular aggregate data in the draft Transparency Report would "allow our adversaries and targets of investigations to piece together a mosaic of information that would provide them significant insight into the U.S. Government's counterterrorism and counterintelligence efforts and capabilities." *Id.* ¶ 30; *see also* ¶¶ 7–8, 36. Relying on that mosaic, adversaries could "undermine both current and future efforts by the Government to collect foreign intelligence and to detect, obtain information about, or prevent or protect against threats to the national security" by, among other possibilities, taking "operational security measures to conceal their activities, alter[ing] their methods of communication to exploit secure channels of communication, or otherwise counter[ing], thwart[ing], or frustrat[ing] the ability of the Government to pursue them." *Id.* ¶ 31. Adversaries thereby could "not only [] ascertain the direction and focus of past national security investigation, but also . . . proactively exploit transparency reporting to detect and thwart current and future surveillance by the Government." *Id.* Data released at the level of granular specificity sought by Twitter, moreover, would reveal or tend to reveal highly valuable information about the Government's national security collection capabilities and investigative interests. *Id.* ¶¶ 7, 36. And, of course, if Plaintiff were to make such disclosures, other companies likely would publish similar data, and our adversaries could soon obtain a comprehensive picture of the Government's national security surveillance activity. *See id.* ¶ 6 n.4, ¶ 32. Importantly, our adversaries actively "gather publicly available information to learn about the capabilities, sources, and methods of U.S. intelligence and law enforcement agencies," and react to the information they learn by taking countermeasures to limit the effectiveness of U.S. intelligence and law enforcement activities. *See* Steinbach Decl. ¶¶ 33–35.[9] These factors demonstrate that the disclosure of the information

[9] *Accord In re Mot. for Release of Ct. Records*, 526 F. Supp. 2d 484, 494 (F.I.S.C. 2007) ("The identification of . . . methods of surveillance would permit adversaries to evade

at issue here could significantly harm counterterrorism and counterintelligence efforts, and otherwise could reasonably be expected to cause at least serious damage to the national security.

Taken together, EAD Steinbach's unclassified declaration and the more-detailed discussion in his classified declaration demonstrate that the Government "in fact had good reason to classify, and therefore censor," *Shaffer*, 102 F. Supp. at 11, the information redacted from the Plaintiff's draft Transparency Report. Through these materials, the Government has justified its redactions "with reasonable specificity, demonstrating a logical connection between the [redacted information] and the reasons for classification." *Id.* Under the authority discussed above, such a showing establishes that the information at issue is properly classified.

*****

As this Court has recognized, "[t]he First Amendment does not permit a person subject to secrecy obligations to disclose classified national security information." ECF No. 113 at 8 (dismissing First Amendment claims because Plaintiff had not challenged the classification of the information that it sought to publish). Now that the Government has established that the information in question is properly classified, that showing is dispositive; Plaintiff has no First Amendment right to publish such information, and summary judgment should be entered for the Government on Counts I–III.[10]

II. The Legislative and Judicial Branches Also Lawfully May Take Steps to Safeguard National Security Information.

As part of Count I and Count II, Plaintiff seeks a declaration under the First Amendment that Executive Order 13526 "constitute[s] the only grounds on which the government may rely to prohibit disclosure of the redacted information in the draft Transparency Report," SAC ¶¶ 85, 90. Plaintiff also seeks a declaration that FISA does not prohibit the disclosures at issue here, or that, insofar as it does prohibit them, it is unconstitutional. But the Court need not, and should not,

---

surveillance, conceal their activities, and possibly mislead investigators through false information.").

[10] Because Twitter acknowledges that it has no First Amendment right to publish properly classified information, *see* SAC ¶ 73, and the Government has demonstrated that the information at issue is properly classified, no inquiry into whether "the restriction on Twitter's speech is [] narrowly tailored to serve a compelling governmental interest," SAC ¶ 84, is necessary.

reach these questions; if the Court finds that the information at issue is properly classified, as discussed above, then there is no First Amendment right to publish it. The Ninth Circuit recently reiterated that, as a "'fundamental rule of judicial restraint,' [a court] 'must consider nonconstitutional grounds for decision' before 'reaching any constitutional questions.'" *In re Ozenne*, --- F.3d ---, 2016 WL 6608963, at *4 (9th Cir. Nov. 9, 2016) (quoting *Jean v. Nelson*, 472 U.S. 846, 854 (1985)). Based on the same principle, the D.C. Circuit in *Stillman* held that the district court had abused its discretion by deciding a First Amendment issue before determining, based on the Government's *ex parte* submission, whether the information that the plaintiff sought to publish was classified. 319 F.3d at 547–49. In so holding, the D.C. Circuit highlighted that "[i]f the Government classified the information properly, then Stillman simply [had] no first amendment right to publish it." *Id.* at 548. So, too, in this case. *See supra* 11.

In any event, if the Court were to consider Plaintiff's other arguments, the Court would find that Plaintiff's attempts to limit the protection for the information at issue are without merit. Plaintiff cites no authority for the proposition that the only manner in which national security information can be protected from disclosure is through Executive Order. To be sure, the protection of classified information by the Executive Branch, which is based on the President's Article II constitutional authority, is undoubtedly the paramount consideration in deciding whether information should be protected from disclosure. *See supra* Argument, I.A. But, as discussed below, other authorities may also apply to protect the information redacted from the draft Transparency Report from disclosure, including statutes and court orders.

To begin with, Plaintiff's contention that FISA nondisclosure provisions would not protect aggregate data from disclosure is contrary to the text of the statute as written by Congress. For example, Title I provides that FISC orders, under certain conditions, "shall direct" recipients to assist the Government "in such a manner as will protect [the] secrecy [of the acquisition]," 50 U.S.C. § 1805(c)(2)(B), and "maintain under security procedures approved by the Attorney General and the [DNI] any records concerning [the acquisition] or the aid furnished," *id.* § 1805(c)(2)(C). Title VII contains similar provisions that may be included in directives issued thereunder. *See* 50 U.S.C. § 1881a(h)(1)(A), (B). These provisions are not

limited, as Plaintiff contends, to "the contents of specific FISA orders, their targets, and details of ongoing investigations," SAC ¶ 83. Instead, in them, Congress instructs broadly that the "secrecy of the acquisition" must be protected. The most natural reading of this statutory language is that the fact of the acquisition—the existence of the FISC order or directive—must not be disclosed. Indeed, the orders typically issued by the FISC under Title I pursuant to Section 1805(c)(2)(B) expressly require recipients "not to disclose to the targets or to any other person the existence of the order. . . or the fact of any of the activities authorized [in the order]." Of course, the disclosure that a company has received a certain aggregate number of FISC orders, by the plain meaning of the terms, would disclose "the existence" of the orders. Titles III and IV of FISA, which also contain provisions authorizing FISC orders protecting information from disclosure, likewise speak broadly of protecting the "secrecy" of each acquisition—without limitation—and provide for Government control of the security procedures under which information related to each acquisition is maintained. *See* 50 U.S.C. § 1824(c)(2)(B), (C) (Title III); 50 U.S.C. § 1842(d)(2)(B) (Title IV).

Finally, Title V, the last provision of FISA that might be applicable here, imposes nondisclosure obligations directly on recipients of FISC orders issued thereunder. Title V provides: "No person shall disclose to any other person that the [FBI] has sought or obtained tangible things pursuant to an order under [Title V of FISA]." Once again, protection for aggregate data falls within the meaning of the statutory text. A disclosure that a company received a specific number of orders would "disclose . . . that the [FBI] has sought . . . tangible things pursuant to an order under" Title V of FISA as many times as the number of orders disclosed. And, as with the other four FISA provisions discussed above, the nondisclosure requirement is not limited to "the contents of specific FISA orders, their targets, and details of ongoing investigations," SAC ¶ 83.[11] Whether the specific terms of any order have been violated

[11] Section 603 of USA FREEDOM Act reinforces that Congress understands aggregate data regarding receipt of national security process to be protected from disclosure. In Section 603, Congress introduced the reporting bands that outline the permissible bounds of disclosure by explaining that: "A person subject to a nondisclosure requirement accompanying an order or directive under [FISA] or a national security letter may, with respect to such order, directive, or national security letter, publicly report the following information using one of the following

may entail further examination by the Government and issuing court, depending on what information is disclosed. But Plaintiff's contention that no other authority would apply to protect the information at issue is meritless on its face.

Furthermore, apart from the statutory protections that shield the data in question from disclosure, nothing prevents an Article III court from reinforcing with a court order other protections against disclosure. *Cf. In re Grand Jury Proceedings*, 417 F.3d 18, 26 (1st Cir. 2005) ("Absent restriction, courts have inherent power, subject to the Constitution and federal statutes, to impose secrecy orders incident to matters occurring before them"); *In re Grand Jury Proceedings*, 17 F. Supp. 3d 1033, 1035-36 (S.D. Cal. 2013). Plaintiff cites no contrary authority; indeed, if there were a rule that prevented courts from issuing such orders, the provisions of FISA that authorize FISC nondisclosure orders all would amount to a nullity. Indeed, there is nothing anomalous about the presence of multiple legal nondisclosure requirements overlapping to protect the same sensitive national security information.

For the foregoing reasons, Plaintiff's challenges to statutory or judicially-imposed nondisclosure obligations, if any, prohibiting the disclosure of classified aggregate data, fail as a matter of law.[12]

---

structures." Section 603(a). While Section 603(c) clarifies that the Government may, in its discretion, permit other forms of reporting, the quoted language from Section 603(a) reflects that Congress understood other formats of reporting aggregate data as being prohibited unless the Government took such actions.

[12] Unconnected with the three Counts asserted in the Complaint, Plaintiff asks the Court, to find "[t]he FISA secrecy provisions are facially unconstitutional under the First Amendment because they do not require nondisclosure orders to contain a defined duration." *See* SAC, Prayer for Relief, (A)(v). It is not clear what, precisely, Plaintiff is challenging; if this language relates to the disclosure of aggregate data in the format presented in the draft Transparency Report, then the Court should not reach this constitutional issue because the data is classified as discussed in Section I. If this objection is untethered to the request to disclose aggregate data, then Plaintiff cannot establish that it has standing to raise such a broad challenge; instead, if it has received any process from the FISC (which, if true, would be a classified fact), then Plaintiff must challenge the duration of obligations imposed by the FISC before that court.

But even if Plaintiff could bring this challenge as currently framed, it would be without merit because the Government has long interpreted the FISA nondisclosure obligations as protecting only information that is classified. *See, e.g.*, Notice, In re Mot. for Decl. J. (Jan. 27, 2014), submitted as Exh. 2 to Plaintiff's Compl., ECF No. 1-1 (explaining that because the DNI had declassified aggregate data reported in a manner consistent with the January 27, 2014

CONCLUSION

The Supreme Court has recognized that "no governmental interest is more compelling than the security of the Nation." *Haig v. Agee*, 453 U.S. 280, 307 (1981). The Government has demonstrated, through the Declarations of EAD Steinbach, that disclosure of the information redacted from the draft Transparency Report reasonably could be expected to cause serious damage to the national security, including by providing adversaries with a roadmap of the Government's surveillance activities and capabilities, and thus is properly classified. *See supra* 18–21. As this Court has recognized, restrictions on the disclosure of classified information by persons subject to secrecy obligations are lawful under the First Amendment. *See* ECF No. 113 at 8. For the foregoing reasons, the Court should grant Defendants' motion for summary judgment and dismiss the Plaintiff's Second Amended Complaint.

Dated: November 22, 2016

Respectfully submitted,

BENJAMIN C. MIZER
Principal Deputy Assistant Attorney General

BRIAN STRETCH
United States Attorney

ANTHONY J. COPPOLINO
Deputy Branch Director

/s/ Julia A. Berman
ERIC J. SOSKIN
JULIA A. BERMAN, Bar No. 241415

---

framework, the Government would "therefore treat such disclosures as no longer prohibited under any legal provision that would otherwise prohibit the disclosure of classified data, including data relating to FISA surveillance"). Classification, in turn, as Plaintiff notes in its Complaint, cannot be indefinite. *See* SAC ¶ 39 (citing Exec. Order No. 13526, § 2.2(f)); *see also* Exec. Order 13526, § 1.5(d) ("No information may remain classified indefinitely"). Because "[i]t is well established that courts should resolve ambiguities in statutes in a manner that avoids substantial constitutional issues," *Mukasey*, 549 F.3d at 872, and equally well-established that time limitations may be read into statutes where that is consistent with the legislative purpose, *see id.* (citing *United States v. Thirty–Seven Photographs*, 402 U.S. 363, 368–70 (1971)), Plaintiff is mistaken that the lack of express time limitations in the FISA "secrecy provisions" renders those provisions unconstitutional.

Trial Attorneys
U.S. Department of Justice
Civil Division, Federal Programs Branch
P.O. Box 883
Washington, D.C. 20044
julia.berman@usdoj.gov

Attorneys for Defendants