

JOSEPH H. HUNT
Assistant Attorney General
DAVID L. ANDERSON
United States Attorney
ANTHONY J. COPPOLINO
Deputy Branch Director
JULIA A. HEIMAN
Senior Counsel
CHRISTOPHER HEALY
Trial Attorney
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.heiman@usdoj.gov

Attorneys for Defendants

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA**

TWITTER, INC.,

Plaintiff,

v.

WILLIAM P. BARR, Attorney
General of the United States, *et al.*,

Defendants.

Case No. 14-cv-4480-YGR

**DEFENDANTS' RENEWED
MOTION FOR
SUMMARY JUDGMENT**

No Hearing Scheduled

Courtroom 1, Fourth Floor
Hon. Yvonne Gonzalez Rogers

NOTICE OF MOTION

PLEASE TAKE NOTICE that, 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.

Dated: September 27, 2019

Respectfully submitted,

JOSEPH H. HUNT
Assistant Attorney General

DAVID L. ANDERSON
United States Attorney

ANTHONY J. COPPOLINO
Deputy Branch Director

/s/ Julia A. Heiman
JULIA A. HEIMAN, Bar No. 241415
Senior Counsel
CHRISTOPHER HEALY
Trial Attorney
U.S. Department of Justice
Civil Division, Federal Programs Branch
P.O. Box 883
Washington, D.C. 20044
julia.heiman@usdoj.gov
Attorneys for Defendants

TABLE OF CONTENTS

1		
2		
3	INTRODUCTION	1
4	BACKGROUND	3
5	I. Statutory and Regulatory Background.....	3
6	A. FISA.....	4
7	B. USA FREEDOM Act.....	5
8	II. Factual and Procedural Background	6
9	III. Plaintiff's Claims in the Second Amended Complaint	11
10		
11	LEGAL STANDARD.....	13
12	ARGUMENT	14
13		
14	I. The Restriction on Plaintiff's Speech is Narrowly Tailored to Meet a Compelling State Interest.....	14
15		
16	II. Plaintiff has not Pled a Challenge under <i>Freedman v. Maryland</i> , and that Authority Does Not Apply to Restrictions on Disclosures About National Security Legal Process	18
17		
18	A. The Court Should Decline to Reach a Constitutional Issue Not Pled in the Complaint.	18
19		
20	B. Restrictions on Disclosure of Classified Aggregate Data about Receipt of National Security Process are Not a Censorship or Licensing Scheme Requiring the Procedural Protections of <i>Freedman</i>	20
21		
22	III. The Legislative and Judicial Branches Also Lawfully May Take Steps to Safeguard National Security Information.	22
23		
24	CONCLUSION.....	24
25		
26		
27		
28		

TABLE OF AUTHORITIES

Cases

<i>Al-Haramain Islamic Found., Inc. v. Bush</i> , 507 F.3d 1190 (9th Cir. 2007)	14
<i>Anderson v. Liberty Lobby, Inc.</i> , 477 U.S. 242 (1986).....	13
<i>Celotex Corp. v. Catrett</i> , 477 U.S. 317 (1986).....	13
<i>Dep’t of Navy v. Egan</i> , 484 U.S. 518 (1988).....	15, 22
<i>Dorfmont v. Brown</i> , 913 F.2d 1399 (9th Cir. 1990)	22
<i>Freedman v. Maryland</i> , 380 U.S. 51 (1965).....	<i>passim</i>
<i>Holder v. Humanitarian Law Project</i> , 561 U.S. 1 (2010).....	15
<i>In re Application of USA for an Order Pursuant to 28 U.S.C. § 1651(a)</i> , 2019 WL 4619698 (D.D.C. Aug. 6, 2019)	24
<i>In re Grand Jury Proceedings</i> , 17 F. Supp. 3d 1033 (S.D. Cal. 2013).....	24
<i>In re Grand Jury Proceedings</i> , 417 F.3d 18 (1st Cir. 2005).....	24
<i>In re Nat’l Sec. Letter</i> , 863 F.3d 1110 (9th Cir. 2017)	<i>passim</i>
<i>John Doe, Inc. v. Mukasey</i> , 549 F.3d 861 (2d Cir. 2008).....	5, 18, 20
<i>Lyng v. Nw. Indian Cemetery Protective Ass’n</i> , 485 U.S. 439 (1988).....	19
<i>Reed v. Town of Gilbert</i> , 135 S. Ct. 2218 (2015).....	15

1	<i>Snepp v. United States</i> ,	
2	444 U.S. 507 (1980).....	3, 15, 21
3	<i>Stillman v. CIA</i> ,	
4	517 F. Supp. 2d 32 (D.D.C. 2007).....	14
5	<i>Stillman v. CIA</i> ,	
6	319 F.3d 546 (D.C. Cir 2003).....	7, 14, 21
7	<i>Thomas v. Chicago Park Dist.</i> ,	
8	534 U.S. 316 (2002).....	19
9	<i>United States v. Hanson</i> ,	
10	2019 WL 4051595 (9th Cir. Aug. 28, 2019).....	19, 22
11	<i>United States v. Marchetti</i> ,	
12	466 F.2d 1309 (4th Cir. 1972)	21
13	<i>United States v. Snepp.</i> ,	
14	897 F.2d 138 (4th Cir. 1990)	21
15	Statutes	
16	18 U.S.C. § 792.....	13
17	50 U.S.C. § 1801.....	3
18	50 U.S.C. § 1805.....	4, 23
19	50 U.S.C. § 1824.....	4, 23
20	50 U.S.C. § 1842.....	5, 23
21	50 U.S.C. § 1861.....	5, 23
22	50 U.S.C. § 1874.....	4, 5, 6
23	50 U.S.C. § 1881a.....	4, 23
24		
25		
26		
27		
28		

Other Legislative Materials

H.R. 3361, 113th Cong. (2014)..... 5

S. 2685, 113th Cong. (2014)..... 5

Rules

Fed. R. Civ. P. 56..... 13

Executive Materials

Exec. Order No. 13526 *passim*

Exec. Order No. 12333 3

MEMORANDUM OF POINTS AND AUTHORITIES

INTRODUCTION

Plaintiff Twitter, Inc. seeks to publish in a draft “Transparency Report” precise detail describing the amount and types 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, and to publish analogous data for subsequent periods.¹ See Second Am. Compl., ECF No. 114 (“SAC”) ¶ 4, 86, 91. Plaintiff contends that the First Amendment requires that it be permitted to make such a disclosure. See SAC, Counts I–III. That is not so.

Four different original classification authorities—all of them then serving as Executive Assistant Director (“EAD”) or Acting EAD of the National Security Branch of the Federal Bureau of Investigation (“FBI”)—have examined the information that Plaintiff seeks to publish and determined that disclosure of that information reasonably could be expected to cause serious damage to the national security.² See ECF No. 147-1, ¶¶ 5–8, 29, 39; ECF No. 179-1, ¶ 6; ECF No. 281-2, ¶¶ 19, 22, 25–27; Decl. of EAD Tabb, Ex. 1 hereto (“Tabb Decl.”), ¶¶ 5, 16, 29. Most recently, EAD Tabb considered the information that Plaintiff seeks to publish and determined that such information would provide “highly valuable insights” to international terrorists, terrorist organizations, foreign intelligence services, cyber threat actors, and other persons or entities who pose a threat to the national security (collectively, “adversaries”), giving them a roadmap to the existence or extent of Government surveillance and capabilities associated with Twitter. See Tabb Decl. ¶¶ 5, 7. EAD Tabb’s unclassified declaration describes the information that adversaries could learn from Plaintiff’s proposed disclosures, to the detriment of

¹As with Defendants’ other submissions in this litigation, the discussion herein 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.

² The EAD or Acting EAD of the National Security Branch has official supervision over all of the FBI’s investigations to deter, detect, and disrupt national security threats to the United States, and is responsible for, *inter alia*, overseeing the national security operations of the FBI’s Counterintelligence Division, Counterterrorism Division, High-Value Detainee Interrogation Group, Terrorist Screening Center, and Weapons of Mass Destruction Directorate. See Tabb Decl., ¶ 2.

1 this country's national security. *See id.* ¶¶ 5–8, 16–23. In sum, Plaintiff's proposed disclosures
2 would inform adversaries where and how the United States is or is not deploying its investigative
3 and intelligence resources, and would tend to reveal which communications services may or may
4 not be secure, which types of information may or may not have been collected, and thus whether
5 or to what extent the United States is or is not aware of the activities of its adversaries. *See id.*
6 ¶ 7. Although EAD Tabb cannot address with more specificity, in this unclassified setting,
7 exactly what information adversaries could learn from Plaintiff's proposed disclosures without
8 revealing the very information the Government is seeking to protect, EAD Tabb's classified
9 declaration, submitted solely for the Court's *ex parte*, *in camera* review contains further detail
10 about just why Plaintiff's proposed disclosures would be so harmful.

11 Under any standard of review—whether the correct inquiry is if the Government had
12 “good reason” to classify the information Plaintiff seeks to publish, or whether strict scrutiny
13 applies to the restriction on Plaintiff's speech—the First Amendment does not permit Plaintiff's
14 proposed disclosures. As discussed herein, the protection of information the disclosure of which
15 reasonably could be expected to harm national security is inarguably a compelling state interest,
16 and the restriction on Plaintiff's proposed disclosures about its receipt of national security
17 process is narrowly tailored to meet that interest. Importantly, not all reporting about national
18 security process is prohibited; on the contrary, the Director of National Intelligence (“DNI”) has
19 declassified multiple reporting formats through which Plaintiff may choose to publish detailed
20 information about this topic. *See id.* ¶¶ 13–14. The level of detail that Plaintiff seeks to divulge,
21 however, for the timeframe covered by its draft Transparency Report as well as subsequent
22 periods, would empower adversaries with information that they can use to take operational
23 security measures to conceal their activities, alter their methods of communication to exploit
24 secure channels of communication, or otherwise counter, thwart, or frustrate efforts by the
25 Government to collect foreign intelligence and to detect, obtain information about, or prevent or
26 protect against threats to the national security. *Id.* ¶ 19. More than that, adversaries also could
27 use such information to engage in deceptive tactics or disinformation campaigns that could
28 undermine lawful intelligence operations of the United States, and to carry out hostile actions

1 that would expose Government personnel and their families to the risk of physical harm. *Id.* ¶ 9.
 2 Because the restriction on Plaintiff's speech is narrowly tailored to prevent these serious national
 3 security harms, the determination that Plaintiff may not publish the information at issue is lawful
 4 even under the most exacting strict scrutiny analysis.

5 Furthermore, because all three counts pled in Plaintiff's Second Amended Complaint turn
 6 on whether Plaintiff has a First Amendment right to publish the data at issue, the showing that
 7 the restriction on publication is narrowly tailored to meet these compelling state interests is
 8 dispositive. For all these reasons, explained herein and in the unclassified and classified
 9 declarations of EAD Tabb, summary judgment should be entered for the Government and
 10 Plaintiff's Second Amended Complaint should be dismissed.

11 **BACKGROUND**

12 **I. Statutory and Regulatory Background**

13 The FBI is charged with primary authority for conducting counterintelligence and
 14 counterterrorism investigations in the United States. *See* Exec. Order No. 12333 §§ 1.14(a),
 15 3.4(a), 46 Fed. Reg. 59941 (Dec. 4, 1981). Today, the FBI carries out national security
 16 operations, including counterintelligence, counterterrorism, and other activities to defeat national
 17 security threats directed against the United States through the FBI's National Security Branch,
 18 which is overseen by EAD Tabb. *See* Tabb Decl. ¶ 2.

19 The conduct of national security investigations and the collection, production, and
 20 dissemination of intelligence to support counterterrorism, counterintelligence, and other U.S.
 21 national security objectives requires the FBI to collect, analyze, and disseminate information.
 22 Congress has authorized the FBI to collect such information with a variety of legal tools,
 23 including various authorities under the FISA and pursuant to the supervision of the Foreign
 24 Intelligence Surveillance Court ("FISC"), an Article III court. *See* 50 U.S.C. § 1801 *et seq.*
 25 Because the targets of national security investigations and others who seek to harm the United
 26 States will take countermeasures to avoid detection, secrecy is often essential to protecting
 27 national security while effectively carrying out counterterrorism and counterintelligence
 28 investigations. *See Snapp v. United States*, 444 U.S. 507, 509 n.3 (1980). Recognizing that,

1 Congress has empowered the FISC and the Executive Branch to maintain the confidentiality of
 2 national security legal process. *See, e.g.*, 50 U.S.C. §§ 1805(c)(2)(B), 1881a(i)(1)(A); *see also*
 3 Tabb Decl. ¶ 11. In the Uniting and Strengthening America by Fulfilling Rights and Ensuring
 4 Effective Discipline Over Monitoring Act of 2015 (“USA FREEDOM Act”), Congress likewise
 5 expressed its judgment regarding the manner in which recipients of national security process
 6 may publish information about their receipt of such process, in the aggregate, without imposing
 7 an unacceptable risk of harm to the national security. USA FREEDOM Act § 603, *codified at* 50
 8 U.S.C. § 1874.

9 A. FISA

10 Multiple provisions of FISA provide that the FISC may issue orders that “direct”
 11 recipients to provide certain information “in a manner that will protect the secrecy of the
 12 acquisition.” *See, e.g.*, 50 U.S.C. §§ 1805(c)(2)(B), 1881a(i)(1)(A). For example, Titles I and
 13 VII of FISA provide that FISC orders “shall direct,” and FISA directives issued by the Attorney
 14 General and DNI after FISC approval of an underlying certification “may direct,” recipients to
 15 provide the Government with “all information, facilities, or assistance necessary to accomplish
 16 the acquisition in a manner that will protect the secrecy of the acquisition,” without limitation.
 17 50 U.S.C. § 1881a(i)(1)(A) (Title VII); *see also id.* § 1805(c)(2)(B) (similar language for Title I).
 18 Additionally, the orders “shall direct” and the directives “may direct” that recipients “maintain
 19 under security procedures approved by the Attorney General and the [DNI] any records
 20 concerning the acquisition or the aid furnished” that such recipient maintains. 50 U.S.C.
 21 § 1881a(i)(1)(B) (Title VII); *see also id.* § 1805(c)(2)(C) (similar language for Title I).
 22 Consistent with the Executive Branch’s authority to control classified information, these
 23 provisions explicitly provide for Executive Branch approval of the companies’ procedures for
 24 maintaining the secrecy of records associated with FISA-authorized surveillance.

25 Other FISA titles that provide search or surveillance authorities also provide for secrecy
 26 obligations to be imposed. *See* 50 U.S.C. § 1824(c)(2)(B)–(C) (requiring Title III orders to
 27 require the recipient to assist in the physical search “in such a manner as will protect its secrecy”
 28 and to provide that “any records concerning the search or the aid furnished” that the recipient

retains be maintained under appropriate security procedures); *Id.* § 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); *Id.* § 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, 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 the enactment of the 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 quantity 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.³ See ODNI Memorandum for Distribution (ES 2015-00366), Tabb Decl., Ex. 2. 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 DNI's prior declassification determination on January 27, 2014.

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., ECF No. 147-1, ¶ 22. The report contained data reflecting the specific numbers and types of national security legal process that Twitter had received 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. 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

³ While the DNI confirmed that there is harm to national security associated with the disclosure of the data even reported in these formats, the DNI determined that exceptional circumstances outweighing the need for protection merited a limited declassification of data. See ODNI Memorandum for Distribution (ES-2015-00366), Tabb Decl., Ex. 2.

1 by the passage of the USA FREEDOM Act. *See* ECF No. 85. Subsequently, the Court also
2 dismissed Plaintiff's First Amended Complaint, finding that Plaintiff's constitutional claims
3 were not viable absent a challenge to the classification of information in the draft Transparency
4 Report. Order, ECF No. 113 at 8.

5 Plaintiff then filed the currently-operative complaint, challenging, *inter alia*, whether the
6 information that it seeks to publish is properly classified. *See* SAC; *see also* Section III *infra*
7 (detailing the claims in the currently-operative complaint). Defendants responded by seeking a
8 conference to set a schedule for summary judgment briefing, urging the Court to resolve this case
9 using the procedures set forth in *Stillman v. CIA*, 319 F.3d 546 (D.C. Cir. 2003), which provides
10 that in First Amendment challenges to classification determinations brought by persons subject
11 to non-disclosure requirements, "*in camera* review of affidavits, followed if necessary by further
12 judicial inquiry, will be the norm." *See* ECF No. 116 at 2 (quoting *Stillman*, 319 F.3d at 548–
13 49). The Court denied the Defendants' request, and indicated that a responsive pleading would
14 be required prior to summary judgment briefing. *See* ECF No. 119. Defendants submitted their
15 answer to the Second Amended Complaint on July 5, 2016. *See* Answer, ECF No. 120.

16 Shortly thereafter, Plaintiff moved for a background investigation to permit its counsel to
17 obtain a security clearance, stating that it sought such a clearance so that counsel could review
18 classified information in connection with these proceedings. *See* ECF No. 124. Defendants
19 opposed that motion, explaining that counsel access to classified information in this setting was
20 neither necessary nor appropriate. *See* ECF No. 133. At a subsequent case management
21 conference, Defendants expressed concern about proceeding to submit classified information to
22 the Court with Plaintiff's motion still pending, but the Court directed Defendants to submit their
23 motion for summary judgment, including classified evidence supporting that motion. Oct. 24,
24 2016 Tr., ECF No. 138, 30:14–22, 31:2–24; 32:4–13. Consistent with the Court's Order,
25 Defendants submitted their motion for summary judgment, *see* ECF No. 145, including the
26 Classified Declaration of EAD Steinbach, explaining why publication of the information in
27 Plaintiff's draft Transparency Report reasonably could be expected to harm national security.
28 *See* Notice of Lodging of Classified Declaration, ECF No. 144. Defendants also submitted an

1 unclassified version of that declaration, providing as much information from EAD Steinbach's
 2 classified declaration as possible, consistent with the national security, on the public record. *See*
 3 Unclassified Steinbach Decl., ECF No. 147-1, ¶ 1. On July 6, 2017, the Court denied without
 4 prejudice the Government's summary judgment motion, and granted Plaintiff's motion to initiate
 5 a background investigation of its counsel to determine whether counsel was eligible for a
 6 security clearance. *See* ECF No. 172.⁴ Defendants sought reconsideration based on the Ninth
 7 Circuit's decision in *In re National Security Letter*, 863 F.3d 1110 (9th Cir. 2017) ("*In re NSL*"),
 8 *see* ECF No. 180, and the Court denied Defendants' motion. *See* ECF No. 186.

9 While the Defendants' summary judgment motion was pending, Plaintiff served its
 10 discovery requests, and Defendants responded with their objections. Although Plaintiff's
 11 requests sought classified and unclassified responses, including the Classified Steinbach
 12 Declaration, the parties' February 17, 2017 joint letter brief made clear that Plaintiff was not
 13 seeking to compel access to classified information at that time. *See* Joint Letter Brief, ECF No.
 14 167 at 1 n.2. On August 8, 2017, Defendants submitted a declaration from EAD Carl Ghattas,
 15 who became EAD of FBI's National Security Branch after EAD Steinbach retired, describing the
 16 requirements that must be fulfilled before any individual may access classified information. *See*
 17 ECF No. 175-1, ¶¶ 9–16. EAD Ghattas attested that the FBI had determined that Plaintiff's
 18 counsel do not fulfill those requirements with respect to the classified information at issue in this
 19 case—including the Classified Steinbach Declaration—because the FBI has determined that
 20 counsel lack a "need-to-know" that information, as defined by the operative Executive Order.
 21 *See id.* ¶¶ 17–21. On February 12, 2018, the Court overruled a number of Defendants'
 22 objections to Plaintiff's discovery requests, *see* ECF No. 188, and the parties proceeded with
 23 discovery. *See* ECF No. 244 at 10–13. Defendants, *inter alia*, reviewed for responsiveness and
 24 logged classified materials, including the Classified Steinbach Declaration.

25 At a November 26, 2018 case management conference, Plaintiff requested access to the

26
 27 ⁴ Consistent with the Court's Order, the Government completed a background
 28 investigation of Plaintiff's counsel. That background investigation was favorably adjudicated.
See Fourth Updated Joint Case Management Statement, ECF No. 244 at 7.

1 Classified Steinbach Declaration that Defendants had submitted in support of their first summary
2 judgment motion, *see* Nov. 26, 2018 Tr., ECF No. 251, at 8:20–22, 13:2–5; *see also* ECF No.
3 250). Briefing then followed in which the Defendants urged the Court to deny the request for
4 access and to return to consideration of the merits of Plaintiff’s claims based on the model set
5 forth in *Stillman v. CIA* for persons subject to non-disclosure obligations – *ex parte*, *in camera*
6 review of the Government’s explanation as to why disclosure of the kind of information in
7 Twitter’s Draft Transparency Report would harm national security. *See* ECF No. 256.
8 Defendants also noted that they had initiated the process of considering whether to assert the
9 state secrets privilege to protect the information in the Classified Steinbach Declaration from
10 disclosure but asked that the Court deny Plaintiff’s request on other grounds.

11 On January 2, 2019, the Court entered the Order to Show Cause re: Disclosure of
12 Declaration Submitted in Camera, ordering Defendants to show cause why they should not be
13 compelled to disclose the Classified Steinbach Declaration to Plaintiff’s Counsel. *See* ECF No.
14 261. In briefing submitted in response to the Order to Show Cause, Defendants noted that they
15 were continuing to consider an assertion of the state secrets privilege to protect the classified
16 information in the Classified Steinbach Declaration, but urged the Court to obviate the need for
17 such an assertion by denying the Plaintiff’s request for access on legal grounds. *See* ECF No.
18 264 at 4, 9–14, 18; ECF No. 269 at 2, 15. Because the Plaintiff’s request and the Order to Show
19 Cause remained pending, the Attorney General invoked the state secrets privilege to protect the
20 classified information in the Classified Steinbach Declaration. *See* ECF No. 281.

21 In its submission asserting the state secrets privilege, the Government asked in the first
22 instance that that the Court discharge the Order to Show Cause and deny Plaintiff’s request for
23 access to the Classified Steinbach Declaration and to proceed with the case under *Stillman*-like
24 procedures for judicial review of the merits; the Government sought dismissal of this action on
25 state secrets grounds only in the alternative. *See* ECF No. 281. In support of its privilege
26 assertion, the Government submitted a declaration from the Attorney General, as well as
27 classified and unclassified declarations from Acting EAD McGarrity explaining the harms to
28 national security that reasonably could be expected to result from the disclosure of information

1 contained in the Classified Steinbach Declaration, including to Plaintiff's counsel. See ECF Nos.
 2 281-1, 281-2, 282. Necessarily—because the very purpose of the Classified Steinbach
 3 Declaration, submitted with the Government's first summary judgment motion, was to explain
 4 the harms of disclosing granular data about Plaintiff's receipt of national security process, such
 5 as that contained in the draft Transparency Report—the McGarrity declarations specifically
 6 addressed the information that Plaintiff seeks to publish in its transparency reporting and
 7 explained the harms to national security that could reasonably be expected to result from
 8 disclosure of that information. See ECF No. 281-2, ¶¶ 13, 18, 19, 23, 25–27. Following briefing
 9 directed at Plaintiff's request for access to classified information, the Court issued a separate
 10 Order to Show Cause Why This Court Should Not Reconsider its Order Denying the Govt's Mot.
 11 for Summary Judgment, ECF No. 301 ("June 21, 2019 Order to Show Cause").

12 In that June 21, 2019 Order to Show Cause, the Court noted that it had previously denied
 13 the Government's summary judgment motion without prejudice, and that the classified
 14 declaration of Acting EAD McGarrity (submitted in litigating the question of Plaintiff's access to
 15 classified information) "provide[d] an explanation of the Government's basis for restricting the
 16 information that can be published in the Draft Transparency Report, and the grave and imminent
 17 harm that could reasonably be expected to arise from its disclosure, in far greater detail than the
 18 Government provided previously." *Id.* at 2. The Court noted that it was "inclined to find that the
 19 classified McGarrity Declaration meets the Government's burden under strict scrutiny to justify
 20 classification and restrict disclosure of information in the Draft Transparency Report, based upon
 21 a reasonable expectation that its disclosure would pose grave or imminent harm to national
 22 security, and that no more narrow tailoring of the restrictions can be made." *Id.* The Court
 23 therefore ordered the parties to show cause why the Court should not reconsider its prior Order
 24 Denying the Government's Motion for Summary Judgment Without Prejudice. *Id.* at 1.

25 On August 23, 2019, the parties jointly responded to the June 21, 2019 Order to Show
 26 Cause, and asked that the classified McGarrity declaration itself not be used to inform the
 27 Court's consideration of the Government's motion for summary judgment (since it was
 28 submitted to address a different issue – the disclosure of classified information submitted by the

Government in this litigation, including to Plaintiff's counsel), but instead that Defendants be permitted to submit a new summary judgment motion, supported by a new declaration, which would incorporate, as appropriate, those aspects of the information proffered in the McGarrity declaration germane to the merits of the case. *See* ECF No. 306 at 2–3. The Court granted the parties' request and issued an Order setting a new briefing schedule, permitting cross-motions for summary judgment in this matter. ECF No. 307. Defendants respectfully submit the instant summary judgment motion pursuant to that Order, supported by the classified and unclassified declarations of EAD Tabb, which incorporate those aspects of the information proffered in the declarations of Acting EAD McGarrity that are germane to the merits of the case.

III. 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 in the draft Transparency Report that the Government has determined to be properly classified, as well as similar information covering subsequent time periods, *see id.*, Prayer for Relief. All of Plaintiff's requests for relief, like the three counts of the Second Amended Complaint, turn on whether Plaintiff has a First Amendment right to publish the information at issue; if, as discussed herein, Plaintiff has no First Amendment right to publish such information, then all of its claims must be dismissed.

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, 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 two 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; Plaintiff contends 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

1 declaratory judgment that “the standards set forth in Executive Order 13526 constitute the only
 2 grounds on which the government may rely to prohibit disclosure of the redacted information in
 3 the draft Transparency Report.” *Id.* It appears that this request is based on Plaintiff’s contention
 4 that “[i]f the information that Twitter seeks to publish is not properly classified under Executive
 5 Order 13526, then the government has no other basis for prohibiting its disclosure.” *Id.* ¶ 82.

6 Count II is a duplicative First Amendment claim that mirrors the substance of the claim
 7 and relief sought in Count I, *compare id.* ¶¶ 85–86 with *id.* ¶¶ 90–91, but is asserted through the
 8 waiver of sovereign immunity provided under the Administrative Procedure Act (“APA”), *see id.*
 9 at 21. Like Count I, the essence of Count II is Plaintiff’s allegation that the information redacted
 10 from the draft Transparency Report is not properly classified, and that Plaintiff therefore has a
 11 First Amendment right to publish it. *See id.* ¶¶ 88–89. In Count II, Plaintiff challenges the
 12 “decision to censor Twitter’s transparency report” as a “final agency action” through which it has
 13 suffered a legal wrong, because the agency decision not to allow publication “violates the First
 14 Amendment.” *Id.* ¶ 88–89. Count II does not specifically identify the action to which it refers,
 15 but the SAC refers elsewhere to the September 9, 2014 letter from FBI General Counsel James
 16 A. Baker to counsel for Plaintiff, which advised Plaintiff that “information contained in the
 17 report is classified and cannot be publicly released.” ECF No. 1-5 (“FBI Letter”); SAC ¶ 57
 18 (describing and quoting the FBI Letter). The Second Amended Complaint also refers to the
 19 Government’s production, on November 17, 2014, of a redacted version of the draft
 20 Transparency Report, from which the Government redacted classified national security
 21 information. *See* SAC ¶ 61. In any event, this purported APA claim amounts to another version
 22 of the same challenge to the Government’s determination that information in the draft
 23 Transparency Report is classified, and for which Plaintiff seeks the same relief that it does with
 24 Count I: injunctive relief permitting publication of information that it alleges is not properly
 25 classified and three forms of declaratory relief.⁵ *Compare id.* ¶¶ 85–86 with *id.* ¶¶ 90–91.

26 ⁵ Specifically, Plaintiff seeks: 1) a declaration that Executive Order 13526 is the only
 27 basis on which the Government can restrict publication of the information redacted from the
 28 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

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.⁶ See *id.* ¶¶ 92–96. Plaintiff avers that it has a “reasonable concern” that it would face prosecution if it 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 disclosure of the information redacted from the draft Transparency Report, and analogous information for subsequent time periods, 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 is the focus of all three of the Counts in the Second Amended Complaint. 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).

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.

⁶ 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. § 792, *et seq.*

1 In cases where the central dispute is whether information is properly classified, summary
 2 judgment is proper if the Court is able to reach such a determination based upon materials
 3 submitted by the Government, including through *in camera* and *ex parte* review. *See, e.g.,*
 4 *Stillman v. CIA*, 517 F. Supp. 2d 32 (D.D.C. 2007) (granting summary judgment upon remand).

5 ARGUMENT

6 **I. The Restriction on Plaintiff's Speech is Narrowly Tailored to Meet a Compelling State Interest.**

7 In *In re NSL*, 863 F.3d 1110 (9th Cir. 2017), the Court of Appeals held that a prohibition
 8 on the disclosure of “the bare fact of receiving” an NSL is a content-based restriction to which
 9 the Supreme Court’s strict scrutiny test applies. *Id.* at 1124. Although much more than the bare
 10 fact of receiving national security process would be revealed by the information that Plaintiff
 11 seeks to disclose here, *see infra* at 17–18, this Court, too, has held that strict scrutiny applies to
 12 the Government’s determination that the information at issue in this case may not be published.
 13 *See* ECF No. 172 at 15; ECF No. 186 at 3–4. In its recent Order to Show Cause, the Court again
 14 referred to “the Government’s burden under strict scrutiny to justify classification and restrict
 15 disclosure of information in the Draft Transparency Report.” ECF No. 301 at 1.

16 For the reasons explained in the Defendants’ prior motion for summary judgment, *see*
 17 ECF No. 145 at 11–15, 18–19, Defendants respectfully disagree that a challenge to a
 18 nondisclosure requirement imposed on the recipient of national security legal process—or the
 19 Government determination that a party subject to a nondisclosure obligation may not publish
 20 information because it is classified—must satisfy strict scrutiny as a content-based restriction on
 21 speech. *See, e.g., Stillman*, 319 F.3d at 548 (party under nondisclosure obligations had no First
 22 Amendment right to publish classified information); *Al-Haramain Islamic Found., Inc. v. Bush*,
 23 507 F.3d 1190, 1203 (9th Cir. 2007) (“acknowledg[ing] the need to defer to the Executive on
 24 matters of . . . national security”). However, while Defendants reserve the right to argue on a
 25 subsequent appeal that a different standard should apply, for purposes of this motion, Defendants
 26 address the analysis in *In re NSL* as presently controlling, as well as the standard that this Court
 27 previously found applicable. But even if strict scrutiny applies to the Government’s
 28 determination in this setting, that test is satisfied here: the restriction on the publication of the

classified data in the draft Transparency Report, and analogous data for subsequent periods, is “narrowly tailored to serve a compelling state interest.” *In re NSL*, 863 F.3d at 1123 (quoting *Reed v. Town of Gilbert*, 135 S. Ct. 2218, 2226 (2015)).

First, as the Court of Appeals “readily conclude[d],” the national security constitutes a compelling Government interest. *Id.* (noting that the Supreme Court “has recognized that ‘[e]veryone agrees that the Government’s interest in combating terrorism is an urgent objective of the highest order’”) (quoting *Holder v. Humanitarian Law Project*, 561 U.S. 1, 28 (2010)). More specifically, the Court of Appeals recognized that “keeping sensitive information confidential in order to protect national security is a compelling government interest.” *Id.* In so holding, the Court of Appeals relied on the Supreme Court’s reasoning that the Government has a compelling interest “in withholding national security information from unauthorized persons in the course of executive business,” *id.* (quoting *Dep’t of Navy v. Egan*, 484 U.S. 518, 527 (1988)), and in “protecting both the secrecy of information important to our national security and the appearance of confidentiality so essential to the effective operation of our foreign intelligence service,” *id.* at 1124 (quoting *Snepp v. United States*, 444 U.S. 507, 509 n.3 (1980)).

The declarations of EAD Tabb explain why the determination at issue here—that Plaintiff may not publish the information redacted from the draft Transparency Report or analogous data for subsequent timeframes—is narrowly tailored to meet these compelling interests. The classified declaration of EAD Tabb details what the Court has recognized as “the grave and imminent harm that could reasonably be expected to arise from [the] disclosure” of such information.⁷ ECF No. 301 at 2. The Court further recognized, based on that detailed classified explanation “that no more narrow tailoring of the restrictions [on Twitter’s publication of the

⁷ As noted above, *see supra* at 10–11, the explanation to which the Court was referring was offered in an earlier declaration, in which Acting EAD McGarrity explained the harm of disclosure of classified information, including to Plaintiff’s counsel, contained in materials the Government had submitted solely for the Court’s *ex parte*, *in camera* review – a discussion that necessarily addressed the harm of disclosing the classified information in Plaintiff’s draft Transparency Report. In the classified declaration submitted in support of the instant renewed summary judgment motion, EAD Tabb has included those facets of Acting EAD McGarrity’s explanation, *i.e.* the detailed explanation of the harms of disclosing the information that Plaintiff seeks to publish.

information at issue] can be made.” *Id.* While it is not possible for EAD Tabb to explain in an unclassified setting with the same level of specificity the harm that reasonably could be expected to result from disclosure, his unclassified declaration discusses the harms of disclosure and the reasons for classification to the extent possible consistent with national security.

EAD Tabb explains that disclosure of the information at issue here would provide adversaries with a roadmap to the existence or extent of Government surveillance at Twitter, giving them highly valuable insights into where and how the United States is or is not deploying its investigative and intelligence resources, revealing the extent, scope, and reach of the Government’s national security collection capabilities and investigative interests. Tabb Decl. ¶¶ 5, 16. Such information would give adversaries insight into the Government’s counterterrorism and counterintelligence efforts and capabilities—or, significantly, the lack thereof—and into particular sources, methods, and techniques. *Id.* ¶ 16. Specifically, the data that Plaintiff seeks to disclose would reveal such information as: (i) incremental increases or decreases in collection over time, which would show whether the Government has a significant presence or investigative focus on a particular platform, reflecting the extent to which the platform becomes more or less “safe” over time; (ii) the collection of content or non-content information, which would show whether and to what extent the Government is collecting certain types of information on the platform; and (iii) the fact of whether or when the recipient received a particular type of process at all, which may reflect different collection capabilities and focus on that platform, different types of information collection, and locations of FBI targets. *Id.* ¶¶ 16, 17, 18, 21.⁸

Armed with such information, adversaries reasonably can be expected to exploit it. As EAD Tabb explained, the FBI has long known that adversaries gather publicly available information to learn sources, methods, and techniques of U.S. intelligence and law enforcement

⁸ It is important to note that these revelations would not be limited to national security process served on Twitter. Tabb Decl. ¶¶ 8, 20. If the Court were to permit the disclosure that Plaintiff seeks to make here, other electronic communication service providers would seek to make similarly detailed disclosures, ultimately yielding for adversaries a comprehensive picture of the Government’s use of national security process that they could use to evaluate the Government’s collection capabilities and vulnerabilities, and which they could then use to the detriment of our national security. *Id.*; see also *infra* at 18.

1 agencies, in order to take countermeasures to attempt to limit the effectiveness of or thwart these
 2 sources, methods, and techniques. *Id.* ¶¶ 24–26. Based on this knowledge and experience, EAD
 3 Tabb has concluded that “we must expect our adversaries to obtain and exploit information
 4 regarding national security process contained within transparency reporting.” *Id.* ¶ 25. That is,
 5 we must expect that adversaries will take action based on the information that Plaintiff seeks to
 6 disclose. *Id.* In particular, EAD Tabb sets forth a number of ways in which adversaries
 7 reasonably could be expected to use the information that Plaintiff seeks to publish: based on
 8 such information, adversaries can be expected to take operational security measures to conceal
 9 their activities, alter their methods of communication to exploit secure channels of
 10 communication, or otherwise counter, thwart or frustrate efforts by the Government to obtain
 11 foreign intelligence and to detect, obtain information about, or prevent or protect against threats
 12 to the national security. *Id.* ¶ 19. Moreover, adversaries could use such information to engage in
 13 deceptive tactics or disinformation campaigns that could undermine lawful intelligence
 14 operations of the United States, and to carry out hostile actions that would expose Government
 15 personnel and their families to the risk of physical harm. *Id.* ¶ 9.

16 Although EAD Tabb made clear that the above-discussed effects would apply to a broad
 17 variety of adversaries, he highlighted, in particular, the potential harm to the Government’s
 18 counterterrorism efforts that reasonably could be expected from the disclosures that Plaintiff
 19 proposes. *See id.* ¶¶ 22–23. EAD Tabb noted that his determination regarding the potential
 20 harm of disclosing the information at issue is informed by the use of social media, including
 21 Twitter, by terrorist organizations such as the Islamic State of Iraq and Syria (“ISIS”). *Id.* ¶ 22.
 22 Especially given the use of social media like Twitter by terrorist adversaries, it is imperative that
 23 the Government maintain the capability to monitor communications platforms, as authorized,
 24 without disclosures related to national security legal process that would reveal the extent and
 25 nature of such surveillance and capabilities, *id.* ¶ 23, and which would thus empower those
 26 terrorist adversaries to avoid detection or to carry out hostile actions.

27 For all these reasons, the determination that Plaintiff cannot publish the information at
 28 issue here is narrowly tailored to serve the compelling interest of national security. As noted

above, the classified declaration of EAD Tabb provides further detail regarding exactly why no further narrow tailoring is possible, and why Plaintiff may not disclose the information that it seeks to publish without risking serious harm to the national security. The same analysis of the harm that reasonably could be expected to arise from disclosure of this information also fulfills the requirement, noted by the Court, that the Government justify classification, *see* ECF No. 301 at 2, and EAD Tabb's declaration explains why the information at issue fulfills the other requirements for classification under Executive Order 13526. *See* Tabb Decl. ¶¶ 27–31. Based on the Government's detailed showing, justifying classification and explaining the serious national security harm that reasonably could be expected to result from Plaintiff's proposed disclosure, the Court should find that this restriction on publication comports with strict scrutiny, and thus that Plaintiff has no First Amendment right to publish the data in its draft Transparency Report or analogous data for subsequent periods.

II. Plaintiff has not Pled a Challenge under *Freedman v. Maryland*, and that Authority Does Not Apply to Restrictions on Disclosures About National Security Legal Process.

In the decision on the Government's prior motion for summary judgment, the Court went beyond the application of strict scrutiny to the Government determination that Plaintiff may not publish the information at issue, and considered the application of *Freedman v. Maryland*, 380 U.S. 51 (1965), to the instant case. *See* ECF No. 172 at 18. The Court should decline to do so again. As discussed below, Plaintiff has not pled a challenge under *Freedman* in the Second Amended Complaint, and Constitutional avoidance principles counsel against addressing this theory. But if the Court were to reach the issue, it should find, based on the guidance of the Ninth Circuit in *In re NSL* and the reasoning of the Second Circuit in *Doe v. Mukasey*, that the present circumstances are not a setting in which the *Freedman* framework applies. Finally, if such protections were applicable here, the requirements of *Freedman* would be satisfied.

A. The Court Should Decline to Reach a Constitutional Issue Not Pled in the Complaint.

“A fundamental and longstanding principle of judicial restraint requires that courts avoid reaching constitutional questions in advance of the necessity of deciding them.” *United States v.*

1 *Hanson*, --- F.3d ---, 2019 WL 4051595, at *9 n.10 (9th Cir. Aug. 28, 2019) (quoting *Lyng v.*
 2 *Nw. Indian Cemetery Protective Ass’n*, 485 U.S. 439, 445 (1988)). Here, the Court should not
 3 decide whether the procedural requirements of *Freedman v. Maryland* are satisfied—or apply in
 4 the first instance—because Plaintiff has pled no such challenge in its complaint.

5 In *Freedman v. Maryland*, the Supreme Court set forth three requirements designed to
 6 ensure that the judicial review of a licensing body’s decisions happens swiftly enough to protect
 7 would-be speakers’ First Amendment rights:

8 (1) any restraint prior to judicial review can be imposed only for a specified brief
 9 period during which the status quo must be maintained; (2) expeditious judicial
 10 review of that decision must be available; and (3) the censor must bear the burden
 of going to court to suppress the speech and must bear the burden of proof once in
 court.

11 *Thomas v. Chicago Park Dist.*, 534 U.S. 316, 321 (2002) (discussing *Freedman*). The very heart
 12 of the decision in *Freedman*, evident in all three of its procedural safeguards, is facilitating
 13 judicial review. *See id.* The crux of the argument in that case was that the judicial review
 14 previously available to challenge the licensing body’s decisions had been “too little and too late.”
 15 *Freedman*, 380 U.S. at 57. Thus, the Supreme Court set forth three safeguards all designed to
 16 ensure that a party subject to a licensing scheme would have access to timely judicial review of
 17 any restriction on its speech: the first safeguard limits the length of a restriction on speech only
 18 “prior to judicial review”; the second safeguard expressly requires the availability of
 19 “expeditious judicial review”; and the third safeguard requires the Government to bear the
 20 burden of “going to court,” *i.e.* obtaining judicial review. *Thomas*, 534 U.S. at 321. In sum, the
 21 *Freedman* safeguards, where applicable, are aimed at ensuring that judicial review of a censor’s
 22 restriction on speech is neither too slow nor too cumbersome to provide for meaningful
 23 protection of a party’s First Amendment rights.

24 In the instant case, Plaintiff has pled no such challenge. Rather, Plaintiff alleges that, as a
 25 substantive matter, the information that it seeks to publish is not properly classified, and that
 26 there are no lawful grounds on which the Government may restrict its publication. *See supra* at
 27 12–14 (detailing the three Counts in the Second Amended Complaint). For this reason alone, the
 28 Court should decline to reach the question of whether the *Freedman* safeguards apply here.

B. Restrictions on Disclosure of Classified Aggregate Data about Receipt of National Security Process are Not a Censorship or Licensing Scheme Requiring the Procedural Protections of *Freedman*.

Even if the Court were to consider the *Freedman* framework, it should find that it has no application here. The sharp contrast between the instant setting and the circumstances in *Freedman*, as well as the reasoning of the Ninth Circuit and the Second Circuit in cases addressing nondisclosure requirements applicable to NSLs, all support this conclusion.

First, *Freedman* itself focused on purely executive restrictions on speech—a requirement that films be submitted to a state board of censors—and did not implicate any statutorily or judicially-imposed nondisclosure obligations analogous to any NSLs or FISC process the Plaintiff may have received here. *See Freedman*, 380 U.S. at 52. Indeed, the Ninth Circuit has recognized the significant difference between the nondisclosure requirements stemming from the statutory framework applicable to NSLs and those settings in which the Supreme Court has found the *Freedman* framework applicable. *See In re NSL*, 863 F.3d at 1128. Although there was no need in that case for the Ninth Circuit to reach the constitutional question of whether the *Freedman* framework applied to the NSL statutes, *see id.* at 1129, the Court of Appeals at great length discussed that “the NSL law does not resemble [the] government censorship and licensing schemes” in which procedural safeguards have been found to be required. *Id.* at 1128. The Ninth Circuit looked to the reasoning of the Second Circuit in *Doe v. Mukasey*, noting that “[u]nlike an exhibitor of movies,’ the recipient of a nondisclosure requirement ‘did not intend to speak and was not subject to any administrative restraint on speaking *prior to* the Government’s issuance of an NSL.’” *Id.* at 1128 (quoting *Doe*, 549 F.3d at 880) (emphasis the Ninth Circuit’s). The Court reasoned that “[r]ather than resembling a censorship or licensing scheme, the NSL law is more similar to governmental confidentiality requirements that have been upheld by the courts.” *Id.* at 1129 (analogizing to restrictions in grand jury proceedings). Here, as in *In re NSL*, Plaintiff was not subject to nondisclosure restrictions prior to the Government’s issuance of process to the Plaintiff. As the Ninth Circuit pointed out in reviewing the NSL law, “the [Supreme] Court has not held that these sorts of government confidentiality restrictions must have the sorts of procedural safeguards required for censorship and licensing schemes.” *Id.*

1 Indeed, application of these factors would make little sense where the data regarding
 2 national security legal process itself arises from either NSLs, which already are accompanied by
 3 procedural safeguards comporting with the *Freedman* framework, *see In re NSL*, 863 F.3d at
 4 1129, or from FISA process, which begins with a Court order or a directive issued in connection
 5 with judicially-reviewed process. *See supra* at 5–6 (discussing various forms of FISA process).
 6 In this setting, if the *Freedman* framework were applied, it would be satisfied: as to the first
 7 *Freedman* requirement, there is no restraint on speech prior to judicial review, because FISA
 8 process emanates from FISC orders or process overseen by that court. As to the second factor,
 9 because of the FISC’s involvement in and supervision of process issued under FISA, judicial
 10 review is available, not just “expeditious[ly],” but from the very outset. And, finally, with
 11 respect to the third factor, the burden of “going to court” necessarily rests with the Government,
 12 which initiates FISC process. Thus, far from constituting a licensing scheme subject to
 13 *Freedman*, restrictions on the disclosure of aggregate data on national security legal process
 14 already emanate from non-disclosure obligations subject to the judicial process.

15 More generally, no case of which Defendants are aware obligates the Government to
 16 initiate judicial review on an expedited basis in order to protect classified information entrusted
 17 to persons subject to non-disclosure obligations whenever they claim a First Amendment right to
 18 disclose it. *See United States v. Snapp*, 897 F.2d 138, 141–43 (4th Cir. 1990) (rejecting the
 19 argument that the CIA should be required to initiate judicial review to protect classified
 20 information in prepublication review context); *United States v. Marchetti*, 466 F.2d 1309, 1317
 21 (4th Cir. 1972) (rejecting same argument, reasoning “[b]ecause of the sensitivity of the area and
 22 confidentiality of the relationship in which the information was obtained . . . we find no reason to
 23 impose the burden of obtaining judicial review upon the CIA”). Such a requirement could lead
 24 to constant emergency efforts by the Government to enlist courts to prevent disclosures that
 25 would jeopardize national security. Indeed, the law is clear that persons subject to nondisclosure
 26 obligations have no First Amendment right to disclose classified information, *see Snapp*, 444
 27 U.S. at 509–510 & n.3, but that such persons have a remedy to obtain judicial review of
 28 restrictions in particular cases, *see, e.g., Stillman*, 319 F.3d at 548–549.

III. 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 reach these questions; if the Court finds that the Government’s determination that Plaintiff may not publish the information at issue is narrowly tailored to meet the Government’s compelling interest in national security, then Plaintiff has no First Amendment right to publish it. *See Hanson*, --- F.3d ---, 2019 WL 4051595, at *9 n.10 (reiterating that courts should “avoid reaching constitutional questions in advance of the necessity of deciding them”).

In any event, if the Court were to consider these 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. As Defendants have explained in prior briefing, the Constitution confers on the Executive the exclusive responsibility for the protection and control of national security information, *see Egan*, 484 U.S. at 527; *Dorfmont v. Brown*, 913 F.2d 1399, 1401 (9th Cir. 1990), and Executive Order 13526, which sets forth the framework for classification, was promulgated pursuant to that constitutional authority. *See* ECF No. 145 at 12–13. 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.

Plaintiff’s contention that FISA nondisclosure provisions would not protect aggregate data from disclosure is contrary to the text of the statute and lacks common sense. 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(i)(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 (emphasis added). Instead, 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 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 number of FISC orders, by the plain meaning of the terms, would disclose “the existence” of those 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].” 50 U.S.C. § 1861(d)(1). Once again, protection for aggregate data falls well 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. *Id.* 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. Whether the specific terms of any order have been violated may entail further examination by the Government and the issuing

1 court, depending on what information is disclosed. But Plaintiff's contention that no other
 2 authority would apply to protect the information at issue is meritless on its face.

3 Indeed, Section 603 of the USA FREEDOM Act reinforces that Congress understands
 4 aggregate data regarding receipt of national security process to be protected from disclosure. In
 5 Section 603, Congress introduced the permissible bounds of disclosure by explaining: "A person
 6 subject to a nondisclosure requirement accompanying [process] under [FISA] or a national
 7 security letter may, with respect to such order, directive, or national security letter, publicly
 8 report the following information using one of the following structures." Section 603(a). While
 9 Section 603(c) clarifies that the Government may, in its discretion, permit other forms of
 10 reporting, the quoted language from Section 603(a) reflects that Congress understood other
 11 formats of reporting aggregate data as being prohibited unless the Government took such actions.

12 Furthermore, apart from the statutory protections that shield the data in question from
 13 disclosure, nothing prevents an Article III court from reinforcing with a court order other
 14 protections against disclosure. *Cf. In re Grand Jury Proceedings*, 417 F.3d 18, 26 (1st Cir. 2005)
 15 ("Absent restriction, courts have inherent power, subject to the Constitution and federal statutes,
 16 to impose secrecy orders incident to matters occurring before them."); *In re Application of USA*
 17 *for an Order Pursuant to 28 U.S.C. § 1651(a)*, --- F. Supp. 3d ---, 2019 WL 4619698 (D.D.C.
 18 Aug. 6, 2019); *In re Grand Jury Proceedings*, 17 F. Supp. 3d 1033, 1035-36 (S.D. Cal. 2013).
 19 Plaintiff cites no contrary authority; indeed, if there were a rule that prevented courts from
 20 issuing such orders, the provisions of FISA that authorize FISC nondisclosure orders all would
 21 amount to a nullity. Indeed, there is nothing anomalous about the presence of multiple legal
 22 nondisclosure requirements overlapping to protect sensitive national security information.

23 Thus, Plaintiff's challenges to statutory or judicially-imposed nondisclosure obligations,
 24 if any, prohibiting the disclosure of classified aggregate data, fail as a matter of law.

25 CONCLUSION

26 For the foregoing reasons, and the reasons set forth in EAD Tabb's classified and
 27 unclassified declarations, the Court should grant Defendants' renewed motion for summary
 28 judgment and dismiss Plaintiff's Second Amended Complaint.

1 Dated: September 27, 2019

Respectfully submitted,

2
3 JOSEPH H. HUNT
Assistant Attorney General

4 DAVID L. ANDERSON
5 United States Attorney

6 ANTHONY J. COPPOLINO
7 Deputy Branch Director

8 /s/ Julia A. Heiman
9 JULIA A. HEIMAN, Bar No. 241415
Senior Counsel
10 CHRISTOPHER HEALY
Trial Attorney
11 U.S. Department of Justice
12 Civil Division, Federal Programs Branch
P.O. Box 883
13 Washington, D.C. 20044
julia.heiman@usdoj.gov
14 *Attorneys for Defendants*

Exhibit 1

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

_____	)	
TWITTER, INC.,	)	
	)	
Plaintiff,	)	
	)	Case No. 14-cv-4480-YGR
v.	)	
	)	
WILLIAM P. BARR, Attorney General	)	
of the United States, <i>et al.</i> ,	)	
	)	UNCLASSIFIED DECLARATION
Defendants.	)	OF JAY S. TABB, JR.
_____	)	

I, Jay S. Tabb, Jr., hereby declare as follows, pursuant to 28 U.S.C. § 1746:

I. INTRODUCTION

1. I am the Executive Assistant Director (“EAD”) of the National Security Branch of the Federal Bureau of Investigation (“FBI”), United States Department of Justice. The purpose of this declaration is to support the Government’s renewed motion for summary judgment in the above-captioned case by explaining, in unclassified terms, the national security harms that reasonably could be expected to result from the disclosure of data reflecting the Government’s use of national security process contained in a draft 2014 Transparency Report, and analogous data for later periods, that Twitter, Inc. (“Twitter”) seeks to publish and that I understand to be the subject of this litigation. A redacted, unclassified copy of the draft Transparency Report is attached hereto as Exhibit 1.¹

2. As the EAD of the FBI’s National Security Branch, I am responsible for, among other things, overseeing the national security operations of the FBI’s Counterintelligence

¹ In a separate, classified declaration, I have set forth a more thorough explanation of the reasons that support the Government’s renewed motion for summary judgment. It is my understanding that counsel for Defendants will make the classified declaration available to the Court solely for its *ex parte* and *in camera* review by lodging that declaration with the Court Information Security Officer. The FBI does not consent to its disclosure beyond the presiding judge.

Division, Counterterrorism Division, High-Value Detainee Interrogation Group, Terrorist Screening Center, and Weapons of Mass Destruction Directorate. The FBI's National Security Branch also guides the functions carried out by other FBI divisions that support the FBI's national security missions, such as training, technology, human resources, and any other operations that further the FBI's mission to defeat national security threats directed against the United States. In this role, I have official supervision over all of the FBI's investigations to deter, detect, and disrupt national security threats to the United States.

3. As the EAD of the National Security Branch, I have also been delegated original classification authority by the Director of the FBI. *See* Executive Order 13526, 75 F.R. 707 (Dec. 29, 2009), § 1.3(c). As a result, I am responsible for the protection of classified national security information within the National Security Branch of the FBI and in matters affecting the national security mission of the FBI, including the sources, methods, and techniques used by the FBI in the collection of national security and criminal information for national security investigations. To that end, the Director of the FBI has authorized me to execute declarations and affidavits to protect such information.

4. The statements in this declaration are based on my personal knowledge, my review and consideration of documents and information, including Twitter's draft Transparency Report, made available to me in my official capacity, and on information obtained from Special Agents and other FBI employees. I have reached my stated conclusions in accordance with this information.

II. SUMMARY

5. I have determined that the information about Twitter's receipt of national security process that was redacted from Twitter's draft Transparency Report is properly classified, and that its unauthorized disclosure reasonably could be expected to result in serious damage to the national security. As explained further below, and in greater detail in my classified declaration, disclosure of the information at issue here would provide international terrorists, terrorist organizations, foreign intelligence services, cyber threat actors, and other persons or entities who pose a threat to the national security—including not only targets of investigation but also those

yet undetected by the Government—(collectively, “adversaries”) with a roadmap to the existence or extent of Government surveillance and capabilities associated with Twitter.

6. In addition, I have reviewed the unclassified and classified declarations of former EAD Michael Steinbach and Acting EAD Michael C. McGarrity that I understand to have been previously submitted to the Court in this case, and I agree with the assessments and conclusions set forth therein.

7. Disclosure of the information Twitter seeks to publish would provide highly valuable insights into where and how the United States is or is not deploying its investigative and intelligence resources, and would tend to reveal which communications services may or may not be secure, which types of information may or may not have been collected, and thus whether or to what extent the United States is or is not aware of the activities of these adversaries. Moreover, as such information is disclosed in subsequent transparency reports, our adversaries would derive a clear picture not only of where the Government’s surveillance efforts are directed, including its current ability (or inability) to conduct surveillance on particular electronic communication service providers or platforms, but also of how its surveillance activities change over time, including when the Government initiates or expands surveillance capabilities or efforts involving providers or services that adversaries previously considered “safe.”

8. Furthermore, when other companies follow suit and disclose similarly detailed information about their receipt of national security process, that roadmap will expand to Government surveillance and capabilities as to other providers or platforms as well.²

9. Foreign governments and adversaries, including terrorist organizations, actively gather information to assess the Government’s capabilities and seek to exploit any such information that they obtain. For example, if adversaries learn from which platforms and what types of information the Government seeks to collect, they can take steps to avoid collection. Additionally, they can use such information to engage in deceptive tactics or disinformation

² If Twitter were permitted to disclose the granular aggregate data at issue here, the harm to national security would be compounded by the fact that other companies would almost certainly seek to make similar disclosures. As a result, our adversaries could soon obtain a comprehensive picture of the Government’s use of national security process.

campaigns that could undermine lawful intelligence operations of the United States, and to carry out hostile actions that expose Government personnel and their families to the risk of physical harm. In sum, and as explained further below, Twitter's proposed disclosure of specific information about the United States' use of national security legal process would assist adversaries in avoiding detection by and in carrying out hostile actions against the United States and its interests.

III. BACKGROUND

A. National Security Legal Process

10. Several federal statutes authorize the FBI to obtain information from individuals or private entities, including electronic communication service providers ("providers"), in furtherance of investigations conducted to protect the national security of the United States. Under 18 U.S.C. § 2709, 12 U.S.C. § 3414, and 15 U.S.C. §§ 1681u, 1681v, the FBI may issue National Security Letters ("NSLs"). The Foreign Intelligence Surveillance Act ("FISA") provides different mechanisms for the Government to obtain foreign intelligence information in support of its national security investigations, including: Title I, authorizing electronic surveillance within the United States; Title III, allowing physical searches in the United States; Title IV, permitting the installation of pen registers and trap and trace devices; Title V, for access to certain "tangible things"; and Title VII, permitting the acquisition of foreign intelligence information concerning subjects outside the United States. *See* 50 U.S.C. §§ 1801, *et seq.*

11. This declaration refers at times collectively to NSLs and FISA orders and directives as "national security process" or "national security legal process." In some circumstances, data reflecting the Government's use of such process, including qualitative and quantitative information about the national security process received by a particular individual or entity, is classified and subject to nondisclosure requirements imposed by statute or court order or both. These protections and restrictions reflect a recognition that often - and in the case of FISA process, always - secrecy is essential to the effectiveness of these critical tools to protect national security.

B. Provider Reporting Regarding Receipt of National Security Process

12. Following unauthorized disclosures by Edward Snowden of documents that purportedly contained classified national security information, multiple providers sought to disclose data regarding their receipt of national security process to correct perceived inaccuracies in the press and to address public speculation about the nature and scope of their cooperation with the Government.

13. Citing exceptional circumstances, including the need to facilitate transparency and the impact of secrecy on providers, in 2014 and 2015, the Director of National Intelligence (“DNI”) declassified certain categories of data reflecting the Government’s use of national security process, permitting disclosure of such data by recipients of national security process if reported in one of a number of specified formats. The categories of data reflecting the Government’s use of national security process declassified by the DNI in 2015 that providers and others may choose to publicly report are set forth in Section 603 of the USA FREEDOM Act and codified at 18 U.S.C. § 1874.³

14. The reporting framework reflected in the 2015 DNI declassification and the USA FREEDOM Act allows providers to report aggregate data regarding their receipt of national security process with more granularity than had ever been permitted before. Under each of the permissible reporting formats recognized by Congress: (1) if a recipient of national security process chooses to publicly report quantitative information revealing that it received *any* national security process, it must report statistics regarding process received in *every* category of authorities, even if that provider received no process pursuant to a particular category; (2) the allowable methods of reporting are all structured as defined aggregate quantities of national security process, varying in scale depending on defined categories of national security process

³ Although the DNI concluded that the aggregate quantities of data reflected in the USA FREEDOM Act were properly classified because disclosure reasonably could be expected to harm national security, he exercised his discretion to declassify that information in the interests of transparency and in light of the impact of secrecy on providers. See ODNI Memorandum for Distribution (ES-2015-00366), attached hereto as Exhibit 2.

(“bands”); and (3) each category of reporting bands begins at “0.” *See* 18 U.S.C. § 1874 (emphases added).

15. The currently-operative reporting framework allows electronic communication service providers and others who are subject to national security process, and the secrecy requirements that accompany such process, latitude to describe the process that they have received without unduly compromising national security interests. Information at a more granular level than described in the USA FREEDOM Act remains classified, because it would provide a roadmap to adversaries revealing the existence of or extent to which Government surveillance may be occurring at Twitter or providers like Twitter.

IV. HARM OF DISCLOSURE OF CLASSIFIED INFORMATION IN TWITTER’S DRAFT TRANSPARENCY REPORT

16. Disclosure of the classified information redacted from Twitter’s draft Transparency Report reasonably could be expected to cause serious harm to national security. Such data would reveal or tend to reveal information about the extent, scope, and reach of the Government’s national security collection capabilities and investigative interests, not only at Twitter but more broadly. The disclosure of such information would allow adversaries of the United States, including current and future targets of FBI national security investigations, significant insight into the U.S. Government’s counterterrorism and counterintelligence efforts and capabilities, or, significantly, the lack thereof, and into particular intelligence sources and methods.

A. The Disclosures Twitter Seeks Would Provide Invaluable Insights into U.S. Intelligence Collection Activities.

17. As noted, the Director of National Intelligence declassified certain aggregate quantities of data reflecting the Government’s use of national security legal process to permit public reporting by recipients of such process, if reported in one of the formats specified by the Government in accord with the USA FREEDOM Act. Those formats were designed specifically to minimize the harms that could reasonably be expected to result from disclosure of this data if publicly reported as specific quantities and types of process or in smaller aggregate quantities. Disclosure of the kind of granular data regarding the national security legal process received by

Twitter, as set forth in its draft Transparency Report, would reveal such information as:

(i) incremental increases or decreases in collection over time, which would show whether the Government has a significant presence or investigative focus on a particular platform; (ii) the collection of content or non-content information, which would show whether and to what extent the Government is collecting certain types of information on that platform; and (iii) the fact of whether or when the recipient received a particular type of process at all, which may reflect different collection capabilities and focus on that platform, different types of information collected, and locations of FBI targets.

18. More specifically, by detailing the amount, if any, of each particular type of process Twitter had received during a particular period, and over time, this data would reveal the extent to which Twitter was or was not a safe channel of communication for our adversaries. It is reasonable to expect that our adversaries will take action based on such information. Even historical data would be alerting to adversaries by tending to reveal collection capabilities and investigative interests.

19. Armed with the kind of detailed information about Twitter's receipt of national security process contained in Twitter's draft Transparency Report, adversaries reasonably can be expected to take operational security measures to conceal their activities, alter their methods of communication to exploit secure channels of communication, or otherwise counter, thwart or frustrate efforts by the Government to collect foreign intelligence and to detect, obtain information about, or prevent or protect against threats to the national security. Moreover, adversaries would be able to use transparency reporting not only to ascertain the direction and focus of past national security investigations, but also to proactively exploit transparency reporting to detect and thwart current and future surveillance by the Government.

20. Furthermore, and as noted previously, the harms from such disclosures would be compounded if other electronic communication service providers were permitted to make similar detailed disclosures regarding their receipt of national security process in the manner that Twitter seeks to make. If the Court were to grant Twitter the relief it seeks in this case, other providers would almost certainly seek to make the same types of disaggregated, granular disclosures

regarding their receipt of national security process. These disclosures would provide a comprehensive picture of the Government's use of national security process that adversaries would use to evaluate the Government's collection capabilities and vulnerabilities, as well as its investigative practices, and enable them to take operational security measures to avoid and thwart continued and future investigation and to seek more secure means of communication.

21. The granularity of the data that Twitter seeks to publish would reveal or tend to reveal information about the extent, scope, and reach of the Government's national security collection capabilities and investigative interests—including its limitations and vulnerabilities. The disclosure of such data would tend to reveal whether the Government does or does not have a significant presence and investigative focus on communications occurring on Twitter, and changes in those numbers over time would tend to reveal an increase or decrease in collection, signaling that the platform is a more or less safe channel of communication. Also, reporting that differentiates between types of collections—content or non-content—tends to reveal sources and methods regarding whether and to what extent the Government is or is not collecting certain types of information on that platform. And, again, future reporting would reveal contrasts with prior activities that may show additional or different types of information collection, or that certain types of information are no longer being collected.

22. My determination that the detailed disclosures Twitter seeks to make reasonably could be expected to harm national security is informed by the use of social media, including Twitter, by terrorist organizations and other adversaries of the United States to further their illicit aims and efforts to harm the United States. Social media and the Internet have been used by adversaries for communication among operatives to facilitate and plan terrorist attacks, espionage, and other conduct which threatens the national security. For example, with respect to Twitter in particular, the Islamic State of Iraq and Syria ("ISIS") has used Twitter extensively to broadcast videos of beheadings of Western hostages and others. In fact, when Twitter removed such videos from its platforms, ISIS threatened to retaliate by murdering Twitter employees. *See, e.g.,* Lizzie Dearden, "Islamic State: ISIS fanatics threaten terrorist attacks on Twitter employees for shutting accounts down," *The Independent* (Sept. 10, 2014), available at

<http://www.independent.co.uk./news/world/middle-east/islamic-state-isis-fanatics-threaten-terrorist-attacks-on-twitter-employees-for-shutting-accounts-down-9722845.html>.

23. Given the use and exploitation of social media by terrorist adversaries, it is imperative that the Government maintain the capability to monitor communications platforms, as authorized, without disclosures related to national security legal process that would reveal the extent and nature of such surveillance and capabilities.

B. Adversaries Are Likely to Use the Information Twitter Seeks to Disclose.

24. My determination that the detailed disclosures Twitter seeks to make reasonably could be expected to harm national security is also informed by efforts that terrorists, hostile foreign intelligence services, and other adversaries undertake to thwart surveillance and detection by the United States. The FBI has long known that adversaries gather publicly available information to learn about the sources, methods, and techniques of U.S. intelligence and law enforcement agencies, in order to take countermeasures to attempt to limit the effectiveness of or thwart these sources, methods, and techniques. Numerous open sources have reported regarding extensive use and exploitation of the internet by terrorist organizations. In 2003, for example, then Secretary of Defense Donald Rumsfeld reported that an Al Qaeda training manual recovered in Afghanistan instructed that, “[u]sing public sources openly and without resorting to illegal means, it is possible to gather at least 80 percent of all information required about the enemy.” *See, e.g.,* Gabriel Weimann, “Al-Qa’ida’s Extensive Use of the Internet,” (Jan. 15, 2008), *available at* <https://ctc.usma.edu/al-qaidas-extensive-use-of-the-internet/>; Timothy L. Thomas, “Al Qaeda and the Internet: The Danger of ‘Cyberplanning,’” (Spring 2003), *available at* <https://www.ncjrs.gov/App/publications/Abstract.aspx?id=199581>.

25. In addition, among other documents that U.S. Government personnel found at Usama Bin Laden’s compound in Pakistan in May 2011 were publicly available criminal complaints filed against several FBI subjects, and a 2010 letter from Bin Laden directing that certain classified cables made public by Wikileaks concerning Pentagon policy be downloaded from the Internet so that he could analyze the materials. *See* “Bin Laden’s Bookshelf,” *available at* <https://www.dni.gov/index.php/features/bin-laden-s-bookshelf>. Just as those documents were

accessed in an effort to exploit information for use against the United States, we must expect our adversaries to obtain and exploit information regarding national security process contained within transparency reporting, including the draft Transparency Report that Twitter seeks to publish here.

26. For these reasons, and as explained further in my classified declaration, Twitter's proposed disclosure of the information redacted from its draft Transparency Report reasonably could be expected to cause serious harm to national security by revealing details regarding the Government's technical capabilities and investigative interests, or limitations and lack of investigative focus, thereby providing adversaries valuable information that they will seek to exploit.

V. THE INFORMATION THAT TWITTER SEEKS TO PUBLISH REMAINS CURRENTLY AND PROPERLY CLASSIFIED.

27. In light of the harm that reasonably could be expected to result from the disclosure of the information redacted from Twitter's draft Transparency Report, I find that that information contained within it meets the standards for classification under Executive Order 13526.

28. Section 1.1 of Executive Order 13526 provides that information may be originally classified if: (1) an original classification authority is classifying the information; (2) the information is owned by, produced by or for, or is under the control of the Government; (3) the information falls within one or more of the categories of information listed in Section 1.4 of the Executive Order; and (4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, and the original classification authority is able to identify or describe the damage.

29. As an original classification authority, I have determined that the information that Twitter seeks to publish meets these criteria. Exec. Order 13526, § 1.1(1). Section IV above explains, to the extent possible in unclassified terms, the serious national security harm that reasonably could be expected to result from disclosure of this information, and, therefore, sets

forth why this information meets the fourth factor required by Executive Order 13526. Exec. Order 13526, § 1.1(4).

30. The information that Twitter seeks to publish meets the remaining criteria for classification as well. Specifically, information concerning national security legal process served on Twitter was produced by and for the United States Government during the course of and in furtherance of national security investigations, and is under the control of the Government. Exec. Order 13526, § 1.1(2). Additionally, disclosure of this information reasonably could be expected to result in damage to the national security, and it pertains to intelligence activities, Exec. Order 13526, § 1.4(c); foreign relations or foreign activities of the United States, Exec. Order 13526, § 1.4(d); and vulnerabilities or capabilities of systems, installations, infrastructures, project, plans, or protection services relating to the national security, Exec. Order 13526, § 1.4(g).

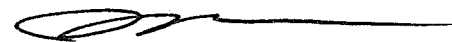
31. Accordingly, and as an original classification authority, I have determined that the information that Twitter seeks to publish was properly classified at the time that Twitter's draft Transparency Report was received by the FBI in 2014 and continues to be properly classified at this time.

VI. CONCLUSION

32. In sum, for the reasons explained herein and in my classified declaration, I have determined that the disclosure of the classified data in Twitter's draft Transparency Report and disclosure of analogous data for subsequent periods reasonably could be expected to cause serious damage to the national security.

I declare under penalty of perjury that the foregoing is true and correct.

Dated: September 25, 2019



Jay S. Tabb, Jr.
Executive Assistant Director

National Security Branch
Federal Bureau of Investigation
Washington, D.C.

(U) Exhibit 1

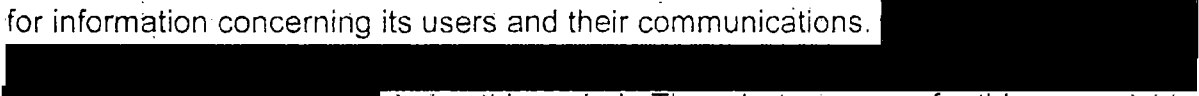


Empowering users with more #transparency on national security surveillance

[Date] __, 2014 | By _____ [title] [time]

Twitter is a unique global platform. It provides a public voice to people all over the world—people who inform and educate others, express their individuality, and seek positive change. Because we are committed to free expression, we vigilantly protect our users' right to know when others threaten their privacy and their freedom to communicate by trying to unmask them or seeking other information about them. Like all companies, Twitter can be compelled by court orders and other means to release user information to the government. Unless our users understand how much, how often, and what kinds of information Twitter is forced to disclose, our users cannot make informed decisions when posting their often courageous Tweets. Therefore, it is vital that Twitter be transparent with its users and be able to communicate this information in a manner that is relevant, understandable and useful.

For the past two years, Twitter has published a Transparency Report, which includes aggregate numbers of requests for account information received from the U.S. government and from other governments around the world. However, our reporting has not included U.S. national security requests such as National Security Letters ("NSLs") or court orders issued pursuant to the Foreign Intelligence Surveillance Act ("FISA"). The truth is that from January 1, 2012, to December 31, 2013, the U.S. government issued a relatively small number of national security requests to Twitter for information concerning its users and their communications.



_____ during this period. The primary reason for this volume is that Twitter's platform is inherently open, and almost all communications are broadcast publicly for everyone to see. (In fact, only a small number of "protected" Tweets and direct messages are not publicly available for all to see.) In this way, Twitter's situation is quite different from that of other communications providers, such as Web-based email services, where most communications are private.

Recently, in order to settle a lawsuit brought before the secret FISA court, the government agreed that companies could disclose their receipt of NSLs and FISA orders separately, for six-month periods, in nonsensical ranges of 0-999 and, if NSLs are lumped together with FISA orders, in ranges of 0-249. Notably, this agreement does not even permit a company to state truthfully that it has not received *any* national security requests, or any of a particular kind of national security request, when none have been issued to it.



[REDACTED]

Given the recent disclosures regarding U.S. government surveillance, as well as our government's related statements and selective declassifications, Twitter needs to be in a position to dispel our users' fears and provide meaningful information about the limited scope of U.S. surveillance on its platform. The current government policy forbids us from responding to one-sided government speech and forces us to mislead our users by reporting overly broad ranges of requests. Forcing Twitter to use only government-sanctioned speech is wrong and unlawful. It is harmful to the public's trust in Twitter, and it violates Twitter's First Amendment right to free speech.

We want everyone to know that the U.S. government's surveillance of Twitter users through NSLs and FISA orders is quite limited. The number of national security requests Twitter receives has increased over time, but even during the last six months of 2013, the combined number of NSLs and FISA orders that Twitter received was [REDACTED] of the 249 combined requests that the government would have Twitter suggest [REDACTED]

[REDACTED] If Twitter decided to report its receipt of national security requests in ranges, we would use ranges that are more proportional to what we receive—e.g., [REDACTED] of the scale that the other providers are using—and report [REDACTED] total NSLs and FISA orders received in that period (July 1 – December 31, 2013); that is, [REDACTED]

NSLs and [REDACTED] FISA orders. More precisely, Twitter received just [REDACTED] NSLs and [REDACTED] FISA orders over this six-month period. These [REDACTED] requests affected a total of [REDACTED] users, out of approximately 240 million active user accounts. (That's just [REDACTED] millionths of one percent of our users.) In addition, [REDACTED]

These are small numbers, whether considered individually, in the aggregate, or as a percentage of Twitter's total number of active users. Therefore, it is important that we be able to share *our* version of the surveillance story that so many others are trying to tell now. We intend to make this kind of report on a regular basis and hope that, in doing so, we can continue to give our users valuable information that will help them trust in the safety of their communications as they use Twitter to voice their opinions, views, and ideas.

###

[REDACTED]

(U) Exhibit 2

UNCLASSIFIED

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

ES 2015-00366

MEMORANDUM FOR: Distribution

SUBJECT: Declassification: Certain Data Related to Requests by the United States to Telecommunications Companies for Customer Information under Orders Issued Pursuant to the Foreign Intelligence Surveillance Act and under National Security Letters

REFERENCES: A. National Security Act of 1949
B. Executive Order 12,333, as amended, *United States Intelligence Activities*
C. Executive Order 13,526, *Classified National Security Information*

Pursuant to References B and C and consistent with my statutory obligation to protect intelligence sources and methods (Reference A), I am authorizing the declassification of certain data related to requests by the United States to communication providers for customer information under orders issued pursuant to the Foreign Intelligence Surveillance Act (FISA) and under national security letters. As described in more detail below, data publicly reported in a manner consistent with the provisions of Section 604 of the FISA, as added by Section 603 of the USA Freedom Act of 2015 (Attachment 1), to the extent currently classified, is hereby declassified.

Some of the data covered by Section 603 of the USA Freedom Act was previously declassified on 27 January 2014 (Attachment 2), but my declassification today covers additional data. While the newly declassified data had been properly classified and indeed continues to meet the classification requirements of Executive Order 13526 for ongoing protection, I have determined that this data presents an exceptional circumstance that outweighs the need for protection. This declassification reflects the Executive Branch's continuing commitment to making information about the Government's intelligence activities publicly available where appropriate and consistent with ensuring the protection of the national security of the United States.

The data described below is declassified when a communication provider subject to a nondisclosure requirement accompanying a FISA order or directive, or a national security letter, publicly reports the data using one of the following four structures:

UNCLASSIFIED

UNCLASSIFIED

SUBJECT: Declassification: Certain Data Related to Requests by the United States to Telecommunications Companies for Customer Information under Orders Issued Pursuant to the Foreign Intelligence Surveillance Act and under National Security Letters

Structure 1

- A. The number of national security letters received, reported in bands of 1,000 starting with 0-999;
- B. The number of customer selectors targeted by national security letters, reported in bands of 1,000 starting with 0-999;
- C. The combined number of FISA orders or directives received for contents, reported in bands of 1,000 starting with 0-999;
- D. The combined number of customer selectors targeted under FISA orders or directives received for contents, reported in bands of 1,000 starting with 0-999;
- E. The number of FISA orders received for non-content, reported in bands of 1,000 starting with 0-999; and
- F. The number of customer selectors targeted under FISA orders for non-content, reported in bands of 1,000 starting with 0-999

This data may only be reported in six month intervals. The data set forth above relating to FISA orders and directives is declassified only when released after a 180-day delay between the release date and the period covered by the release, except that with respect to a platform, product, or service for which a provider did not previously receive a FISA order or directive (not including an enhancement to or iteration of an existing publicly available platform, product, or service) such report shall not include any information relating to such new order or directive until 540 days after the date on which such new order or directive is received. The data set forth above relating to national security letters is declassified only when the release date is less than 180 days from the receipt of the national security letter.

Structure 2

- A. The number of national security letters received, reported in bands of 500 starting with 0-499;
- B. The number of customer selectors targeted by national security letters, reported in bands of 500 starting with 0-499;
- C. The combined number of FISA orders or directives received for content, reported in bands of 500 starting with 0-499;

UNCLASSIFIED

UNCLASSIFIED

SUBJECT: Declassification: Certain Data Related to Requests by the United States to Telecommunications Companies for Customer Information under Orders Issued Pursuant to the Foreign Intelligence Surveillance Act and under National Security Letters

- D. The combined number of customer selectors targeted under FISA orders or directives received, reported in bands of 500 starting with 0-499;
- E. The number of FISA orders received for non-content, reported in bands of 500 starting with 0-499; and
- F. The number of customer selectors targeted under FISA orders received for non-content, reported in bands of 500 starting with 0-499.

This data may only be reported in six-month intervals. The data set forth above relating to FISA orders and directives is declassified only when released after a 180-day delay between the release date and the period covered by the release, except that with respect to a platform, product, or service for which a provider did not previously receive a FISA order or directive (not including an enhancement to or iteration of an existing publicly available platform, product, or service) such report shall not include any information relating to such new order or directive until 540 days after the date on which such new order or directive is received. The data set forth above relating to national security letters is declassified only when the release date is less than 180 days from the receipt of the national security letter.

Structure 3

- A. The total number of all national security process received, including all national security letters, and FISA orders and directives, reported in bands of 250 starting with 0-249; and
- B. The total number of customer selectors targeted under all national security process received, including all national security letters, and FISA orders and directives, reported in bands of 250 starting with 0-249.

This data may only be reported in six-month intervals. The data set forth above is declassified only when the release date is less than 180 days from the receipt of the national security letter.

Structure 4

- A. The total number of all national security process received, including all national security letters, and FISA orders and directives, reported in bands of 100 starting with 0-99; and
- B. The total number of customer selectors targeted under all national security process received, including all national security letters, and FISA orders and directives, reported in bands of 100 starting with 0-99.

UNCLASSIFIED

UNCLASSIFIED

SUBJECT: Declassification: Certain Data Related to Requests by the United States to Telecommunications Companies for Customer Information under Orders Issued Pursuant to the Foreign Intelligence Surveillance Act and under National Security Letters

This data may only be reported in one-year intervals. The data set forth above is declassified only when released after a one-year delay between the release date and the period covered by the release.

Departments and agencies shall ensure individual agency or program classification guides that may be affected are updated accordingly.

Please contact Ms. Jennifer Hudson, Director of Information Management, at (703) 874-8085 or via email at Jennifer.Hudson@dni.gov, with any questions.


James R. Clapper

2 Jul 2015
Date

Attachments:

1. USA Freedom Act of 2015, Section 603
2. Director of National Intelligence Declassification Memo, E/S 2014-0052, *Declassification: Certain Data Related to Requests by the United States to Telecommunications Companies for Customer Information under Orders from the Foreign Intelligence Surveillance Act and with National Security Letters*

UNCLASSIFIED

UNCLASSIFIED

**SUBJECT: Declassification: Certain Data Related to Requests by the United States to
Telecommunications Companies for Customer Information under Orders Issued Pursuant
to the Foreign Intelligence Surveillance Act and under National Security Letters**

Distribution:

National Security Council Staff
Director, Central Intelligence Agency
Director, Defense Intelligence Agency
Director, National Geospatial Intelligence Agency
Director, National Reconnaissance Office
Director, National Security Agency
Under Secretary of Defense for Intelligence
Assistant Secretary for Intelligence and Research, Department of State
Under Secretary for Intelligence and Analysis, Department of Homeland Security
Executive Assistant Director, National Security Branch, Federal Bureau of Investigation
Director, Office of Intelligence and Counterintelligence, Department of Energy
Chief of Intelligence/Senior Officer, Drug Enforcement Agency
Assistant Secretary for Intelligence and Analysis, Department of the Treasury Deputy
Chief of Staff, G2 US Army
Director of Naval Intelligence, US Navy
Director of Intelligence, Headquarters US Marine Corps
Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance, US Air Force
Assistant Commandant for Intelligence and Criminal Investigations, US Coast Guard
Assistant Attorney General for National Security, Department of Justice

UNCLASSIFIED

JOSEPH H. HUNT
Assistant Attorney General
DAVID L. ANDERSON
United States Attorney
ANTHONY J. COPPOLINO
Deputy Branch Director
JULIA A. HEIMAN
Senior Counsel
CHRISTOPHER HEALY
Trial Attorney
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.heiman@usdoj.gov

Attorneys for Defendants

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA**

TWITTER, INC.,

Plaintiff,

v.

WILLIAM P. BARR, United States
Attorney General, *et al.*,

Defendants.

Case No. 14-cv-4480-YGR

**DEFENDANTS'
SEPARATE STATEMENT
OF UNDISPUTED FACTS**

No Hearing Scheduled

Hon. Yvonne Gonzalez Rogers