

1 MAYER BROWN LLP
2 ANDREW JOHN PINCUS (*Pro Hac Vice*)
3 apincus@mayerbrown.com
4 1999 K Street, NW
Washington, DC 20006
Tel: (202) 263-3220 / Fax: (202) 263-3300

5 MAYER BROWN LLP
6 LEE H. RUBIN (SBN 141331)
7 lrubin@mayerbrown.com
8 Two Palo Alto Square, Suite 300
3000 El Camino Real
Palo Alto, CA 94306-2112
Tel: (650) 331-2000 / Fax: (650) 331-2060

9 PERKINS COIE LLP
10 MICHAEL A SUSSMANN (*Pro Hac Vice*)
MSussmann@perkinscoie.com
11 700 Thirteenth Street, NW, Suite 600
Washington, DC 20005-3960
Tel: 202-654-6333 / Fax: 202-654-9127

12 *Attorneys for Plaintiff Twitter, Inc.*

13
14 **UNITED STATES DISTRICT COURT**
15 **NORTHERN DISTRICT OF CALIFORNIA**
16 **OAKLAND DIVISION**

17 TWITTER, INC.,

18 Plaintiff,

19 v.

20 LORETTA LYNCH, Attorney General of the
21 United States,

22 THE UNITED STATES DEPARTMENT OF
JUSTICE,

23 JAMES COMEY, Director of the Federal
24 Bureau of Investigation, and THE FEDERAL
BUREAU OF INVESTIGATION,

25 Defendants.

Case No. 14-cv-4480-YGR

**SECOND AMENDED COMPLAINT FOR
DECLARATORY JUDGMENT AND
INJUNCTIVE RELIEF PURSUANT TO
28 U.S.C. §§ 2201 and 2202**

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

I. NATURE OF THE ACTION

1. Twitter, Inc. (“Twitter”) brings this action for a declaratory judgment and permanent injunction pursuant to 28 U.S.C. §§ 2201 and 2202, requesting relief from prohibitions on its speech in violation of the First Amendment.

2. The U.S. government engages in extensive but incomplete speech about the scope of its national security surveillance activities as they pertain to U.S. communications providers, such as Twitter. At the same time, those communications providers are tightly constrained in providing information regarding the scope (*i.e.*, amount) of national security surveillance-related requests they receive.

3. Twitter is firmly committed to providing meaningful transparency to its users and the public. Since 2012, Twitter has published a biannual transparency report that sets forth numbers of requests it receives for user information from governments across the globe, including the U.S. government.

4. Twitter seeks to publish information contained in a draft Transparency Report that describes the *amount* of national security legal process that it received, if any, for the period July 1 to December 31, 2013, from the Foreign Intelligence Surveillance Court (“FISC”). In this Transparency Report, Twitter does not seek to disclose any information or details concerning any specific order from the FISC that it may have received. Twitter’s draft Transparency Report instead reveals the actual aggregate number of Foreign Intelligence Surveillance Act (“FISA”) orders received (if any), the volume of FISA orders received by comparison to government-approved reporting structures, and similar information. Twitter also seeks to disclose that it received “zero” FISA orders, or “zero” of a specific *kind* of FISA order, for that period, if either of those circumstances is true.

5. Twitter submitted its draft Transparency Report to Defendants for review on April 1, 2014. Five months later, Defendants informed Twitter that “information contained in the [transparency] report is classified and cannot be publicly released” because it does not comply with the government’s pre-approved framework for reporting data about government requests in national security investigations.

1 6. Defendants' response means that Twitter cannot speak about the volume of
2 national security legal process it has received except in ways that have been pre-approved by
3 government officials. Defendants initially took the position that communications providers like
4 Twitter are prohibited even from saying that they have received zero national security requests,
5 or zero of a particular kind of national security request, although Defendants later conceded that
6 providers who received zero national security requests for a six-month period can say so, as such
7 information could not be classified. (In addition, a number of providers who, presumably, have
8 received some orders from the FISC have disclosed publicly that they received zero of a
9 particular *kind* of FISA order, and Twitter is unaware of any comment or action by Defendants to
10 indicate such disclosures are unlawful). Twitter's ability to respond to government statements
11 about the scope of its national security surveillance activities generally and to speak about the
12 scope of those activities with respect to Twitter users specifically is being unconstitutionally
13 restricted by Defendants' interpretation of statutes as prohibiting and even criminalizing a
14 provider's mere disclosure of the *number* of FISA orders that it has received, if any.

15 7. Twitter either has received a FISA order in the past or has a reasonable
16 expectation of receiving one in the future. Twitter recognizes that genuine national security
17 concerns require that certain details about such orders, such as the specific target of surveillance,
18 be kept secret. Twitter does not seek through this Complaint to disclose the contents of any FISA
19 orders it may have or will receive.

20 8. Disclosure of the number of the different types of orders that Twitter has or may
21 have received reveals nothing about the content or subjects of such orders, particularly given
22 Twitter's more than 310 million active members.

23 9. In addition, the government's legitimate interest in secrecy cannot last forever,
24 and at some point, release of information about those orders will no longer harm national
25 security. Despite this fact and in spite of its stated legal obligations, Defendants have refused to
26 indicate when, if ever, they will allow Twitter to release *any* information on the volume of
27 national security legal process it has received that goes beyond the pre-approved categories they
28 have heretofore allowed.

1 trap and trace devices to obtain dialing, routing, addressing, and signaling information); Title V
2 (disclosure of certain “business records”) (also referred to as “Section 215 of the USA PATRIOT
3 Act”); and Title VII (surveillance of non-U.S. persons located beyond U.S. borders). In the case
4 of orders issued pursuant to Titles I, III, IV and V, surveillance of the specified target is
5 approved by the FISC; under Title VII, the FISC annually approves procedures for surveillance,
6 but the government selects targets of surveillance without court supervision.

7 20. Each of these Titles of FISA contains a restriction that limits a provider’s ability
8 to disclose information relating to a specific FISA request. Several provisions require the FISC
9 to direct the recipient of a FISA request to comply in such a manner as will protect the secrecy of
10 the court-ordered electronic surveillance, physical search, or installation of a pen register or trap
11 and trace device, or the acquisition of foreign intelligence information, 50 U.S.C. §§
12 1805(c)(2)(B) (Title I); 1824(c)(2)(B) (Title III); 1842(d)(2)(B) (Title IV); 1881a(h)(1)(A) (Title
13 VII). FISA also contains provisions that directly instruct the recipient of a FISA order that it may
14 not disclose the existence of a pen register or trap and trace device “unless or until ordered by the
15 court,” 50 U.S.C. §§ 1842(d)(2)(B) (Title IV), and that it may not “disclose to any other person”
16 the existence of a business records order, 50 U.S.C. § 1861(d)(1) (Title V).

17 21. No provision in FISA prohibits or directs the FISC to prohibit the disclosure of
18 *aggregate numbers* of FISA orders received.

19 22. Defendants have taken the position that the aggregate number of FISA orders
20 received by a particular ECS may only be disclosed in accordance with the pre-approved
21 categories established by the Uniting and Strengthening America by Fulfilling Rights and
22 Ensuring Effective Discipline Over Monitoring Act of 2015, Pub. L. No. 114-23, 129 Stat. 268
23 (2015), codified in relevant part at 50 U.S.C. § 1874 (“USA FREEDOM Act” or “USAFA”).
24 (Dkt. No. 83.) Defendants contend that because the Twitter draft Transparency Report includes
25 aggregate data that is different and more detailed than the categories permitted by the Act, the
26 publication of the draft Transparency Report would constitute an unauthorized disclosure of
27 classified information.

28

1 23. Defendants have not disclosed the basis for their claimed determination that
2 Twitter’s draft Transparency Report contains classified information. For example, in the FBI’s
3 letter to Twitter denying Twitter’s request to publish the draft Transparency Report, the FBI
4 neither identified the classifying authority who made the determination, the date until which the
5 information allegedly classified may not be disclosed, or the reasons for the claimed
6 classification decision. See Letter from James A. Baker, Gen. Counsel, FBI, to Michael A.
7 Sussmann (Sept. 9, 2014) (Dkt. No. 1, Ex. 5.); see ¶ 57 *infra*.

8 **B. Classified National Security Information**

9 24. On December 29, 2009, President Obama issued Executive Order No. 13526,
10 which sets forth the federal government’s policies and procedures for “classifying, safeguarding,
11 and declassifying national security information.” The Executive Order is predicated upon a
12 “commitment to open Government through accurate and accountable application of classification
13 standards and routine, secure, and effective declassification” Exec. Order No. 13526,
14 Preface.

15 25. Executive Order No. 13526 modified regulations codified at 32 C.F.R. Part 2001
16 “Classified National Security Information.”

17 26. Executive Order No. 13526 distinguishes between two basic methods of
18 classifying information—“original classification” and “derivative classification.” “‘Original
19 classification’ means an initial determination that information requires, in the interest of the
20 national security, protection against unauthorized disclosure.” Exec. Order No. 13526 § 6.1(ff).
21 By contrast, “[d]erivative classification” means the “incorporating, paraphrasing, restating, or
22 generating in new form information that is already classified, and marking the newly developed
23 material consistent with the classification markings that apply to the source information.” *Id.* §
24 6.1(o).

25 27. Individuals who “reproduce, extract, or summarize classified information” are
26 bound to “observe and respect original classification decisions.” *Id.* § 2.1.

27 28. Information may be originally classified only if it meets several requirements: (1)
28 it must be classified by an “original classification authority”—officials who are identified in

1 section 1.3 of the Executive Order; (2) the information must be “owned by, produced by or for,
2 or is under the control of the United States Government;” (3) “the information falls within one or
3 more of the categories of information listed in section 1.4 of th[e] order;” and (4) “the original
4 classification authority determines that the unauthorized disclosure of the information reasonably
5 could be expected to result in damage to the national security, which includes defense against
6 transnational terrorism, and the original classification authority is able to identify or describe the
7 damage.” *Id.* § 1.1(a).

8 29. While there is no *ex ante* requirement to provide a justification for a classification,
9 “the original classification authority must be able to support the decision in writing, including
10 identifying or describing the damage, should the classification decision become the subject of a
11 challenge.” 32 C.F.R. § 2001.10.

12 30. There is no distinct standard for derivative classification because all material that
13 is “derivatively” classified has already received an original classification.

14 31. Executive Order No. 13526 delineates three levels of classification:
15 “Confidential,” “Secret,” and “Top Secret.” Exec. Order No. 13526 § 1.2.

16 32. “Confidential” material is information, “the unauthorized disclosure of which
17 reasonably could be expected to cause damage to the national security.” *Id.*

18 33. “‘Secret’ shall be applied to information, the unauthorized disclosure of which
19 reasonably could be expected to cause *serious* damage to the national security.” *Id.* (emphasis
20 added).

21 34. “‘Top Secret’ shall be applied to information, the unauthorized disclosure of
22 which reasonably could be expected to cause *exceptionally grave* damage to the national
23 security.” *Id.* (emphasis added).

24 35. At each classification level, the original classification authority must be able to
25 “identify or describe” the threatened damage. *Id.*

26 36. When information is originally classified “the original classification authority
27 shall establish a *specific date or event* for declassification Upon reaching the date or event,
28 the information shall be automatically declassified.” *Id.* § 1.5 (emphasis added).

1 37. “If the original classification authority cannot determine an earlier specific date
2 event for declassification,” then classified information shall by default be marked for
3 declassification after 10 years, “unless the original classification authority otherwise determines
4 that the sensitivity of the information requires that it be marked for declassification for up to 25
5 years from the date of the original decision.” *Id.*

6 38. Only information that would “clearly and demonstrably be expected to reveal the
7 identity of a confidential human source or a human intelligence source or key design concepts of
8 weapons of mass destruction” is excluded from this eventual declassification requirement. *Id.*
9 Derivative documents containing classified information are also bound to this requirement. *Id.* §
10 2.2(f).

11 39. Executive Order No. 13526 places several limitations on the duration and extent
12 of classification. Most notably, it clarifies that: “No information may remain classified
13 indefinitely.” *Id.* It also prohibits classification that is intended to serve an unacceptable purpose.
14 For example, information may not be classified in order to “prevent embarrassment to a person,
15 organization, or agency,” to “restrain competition,” or to “prevent or delay the release of
16 information that does not require protection in the interest of the national security.” *Id.* § 1.7.
17 Additionally, the Executive Order affirmatively states that “[i]nformation *shall* be declassified as
18 soon as it no longer meets the standards for classification.” *Id.* § 3.1 (emphasis added).

19 40. Executive Order No. 13526 superseded and revoked other Executive Orders
20 governing classification standards including Executive Order No. 12958 of April 1995 and
21 Executive Order No. 13292 of March 25, 2003. *Id.* § 6.2.

22 **C. The Espionage Act**

23 41. The Espionage Act criminalizes a number of actions involving the disclosure or
24 improper handling of information “relating to the national defense.” 18 U.S.C. § 793. Subsection
25 (d) of the Espionage Act criminalizes the willful communication or delivery of any information
26 relating to the national defense that “could be used to the injury of the United States or to the
27 advantage of any foreign nation,” by someone who has lawful possession of same, to any person
28

1 not entitled to receive it. *Id.* § 793(d). Penalties for violations of the Espionage Act include fines
2 and imprisonment. *Id.*

3 42. Twitter is informed and believes and is concerned that if it were to publicly
4 disclose the actual aggregate number of FISA orders or directives it may have received—which
5 would constitute more detailed reporting than permitted under the options provided in the
6 USAFA—or if Twitter were to publicly disclose its unredacted draft Transparency Report,
7 Defendant DOJ may seek to prosecute Twitter and impose the applicable penalties under the
8 Espionage Act.

9 **D. The Government’s Restrictions on Other Communications Providers’ Ability to**
10 **Discuss Their Receipt of National Security Legal Process**

11 43. On June 5, 2013, the British newspaper *The Guardian* reported the first of several
12 leaks of classified material from Edward Snowden, a former U.S. government contractor, which
13 have revealed—and continue to reveal—multiple U.S. government intelligence collection and
14 surveillance programs.

15 44. The Snowden disclosures deepened public concern regarding the scope of
16 governmental national security surveillance. This concern has been shared by members of
17 Congress, industry leaders, world leaders, and the media. In response to this concern, the
18 government has selectively declassified surveillance-related information for public
19 dissemination, a number of executive branch officials have made public statements
20 characterizing and revealing select details of specific U.S. surveillance programs—including the
21 nature and extent of involvement of U.S. communications providers—and the government has
22 engaged in a programmatic review of classification determinations with a stated goal of
23 declassifying more information.

24 45. While engaging in their own carefully crafted speech, U.S. government officials
25 have relied on statutory and other purported legal authority to preclude communications
26 providers from responding to leaks and inaccurate information reported in the media and by
27 public officials, and from addressing related public concerns regarding the providers’
28 involvement with and exposure to U.S. surveillance efforts. These authorities—and the

1 government's interpretation of and reliance on them—constitute facial and as-applied violations
2 of the First Amendment right to engage in speech regarding a matter of extensively debated and
3 significant public interest.

4 46. In response to these restrictions on speech, on June 18, 2013, Google filed in the
5 FISC a Motion for Declaratory Judgment of Google's First Amendment Right to Publish
6 Aggregate Data About FISA Orders. Google then filed an Amended Motion on September 9,
7 2013. Google's Amended Motion sought a declaratory judgment that it had a right under the
8 First Amendment to publish, and that no applicable law or regulation prohibited it from
9 publishing, (1) the total number of requests it receives under various national security authorities,
10 if any, and (2) the total number of users or accounts encompassed within such requests. Similar
11 motions were subsequently filed by four other U.S. communications providers: Microsoft (June
12 19, 2013), Facebook (September 9, 2013), Yahoo! (September 9, 2013), and LinkedIn
13 (September 17, 2013). Apple also submitted an amicus brief in support of the motions
14 (November 5, 2013).

15 47. In January 2014, the DOJ and the five petitioner companies reached an agreement
16 that the companies would dismiss the FISC actions without prejudice in return for the DOJ's
17 agreement that the companies could publish information about U.S. government surveillance of
18 their networks in one of two preapproved disclosure formats. (Two more general reporting
19 options had been approved in the summer of 2013.) President Obama previewed this agreement
20 in a public speech that he delivered on January 17, 2014, saying, "We will also enable
21 communications providers to make public more information than ever before about the orders
22 that they have received to provide data to the government." President Barack Obama, Remarks
23 by the President on Review of Signals Intelligence, White House Office of Press Secretary (Jan.
24 17, 2014, 11:15 AM), [http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-](http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence)
25 [president-review-signals-intelligence](http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence).

26 48. The two pre-approved disclosure formats were set forth in a letter dated January
27 27, 2014, from Deputy Attorney General James M. Cole to the General Counsels for Facebook,
28 Google, LinkedIn, Microsoft and Yahoo! (the "DAG Letter"). (Dkt. No. 1, Ex. 1.) (The DAG

1 Letter also included the two other preapproved disclosure formats from the summer of 2013.)
2 These four preapproved disclosure formats generally permit disclosures of the volume of legal
3 process received in wide reporting bands, with slightly more granularity allowed if aggregate
4 FISA orders are reported in combination with aggregate National Security Letters (“NSLs”)
5 received.

6 49. In a Notice filed with the FISC simultaneously with transmission of the DAG
7 Letter, the DOJ informed the court of the agreement, the new disclosure options detailed in the
8 DAG Letter, and the stipulated dismissal of the FISC action by all parties. (Dkt. No. 1, Ex. 2.)
9 The Notice concluded by stating: “It is the Government’s position that the terms outlined in the
10 Deputy Attorney General’s letter define the limits of permissible reporting for the parties and
11 other similarly situated companies.” (Dkt. No. 1, Ex. 2 at 2.) In other words, according to the
12 DOJ, the negotiated agreement reached to end litigation by five petitioner companies was not
13 limited to the five petitioner companies as a settlement of private litigation, but instead served as
14 a disclosure format imposed on a much broader—yet undefined—group of companies. No
15 further guidance was offered by the DOJ regarding what it considered to be a “similarly situated”
16 company. Further, the Notice cited no authority for extending these restrictions on speech to
17 companies that were not party to the negotiated agreement.

18 **E. The DOJ and FBI Deny Twitter’s Request to Be More Transparent**

19 50. Twitter is a unique service built on trust and transparency. Twitter is used by
20 world leaders, political activists, journalists, and millions of other people to disseminate
21 information and ideas, engage in public debate about matters of national and global concern,
22 seek justice, and reveal government corruption and other wrongdoing. Twitter users are
23 permitted to post under their real names or pseudonymously, and the ability of Twitter users to
24 share information depends, in part, on their ability to do so without undue fear of government
25 surveillance. Therefore, the ability to engage in speech concerning the nature and extent of
26 government surveillance of Twitter users’ activities is critical to Twitter.

27 51. In July 2012, Twitter released its first Transparency Report. Release of this
28 Transparency Report was motivated by Twitter’s recognition that citizens must “hold

1 governments accountable, especially on behalf of those who may not have a chance to do so
2 themselves.” Jeremy Kessel, Twitter Transparency Report, Twitter Blog (July 2, 2012, 20:17
3 UTC), <https://blog.twitter.com/2012/twitter-transparency-report>. The Transparency Report
4 addressed the volume of civil and criminal government requests for account information and
5 content removal, broken down by country, and takedown notices pursuant to the Digital
6 Millennium Copyright Act received from third parties and the number of instances when Twitter
7 responded to these requests. The report did not contain information regarding government
8 national security requests Twitter may have received. Subsequent biannual transparency reports
9 have been released since then, including the most recent on February 19, 2016.

10 52. At Twitter’s request, on January 29, 2014, representatives of the DOJ, FBI, and
11 Twitter met at the Department of Justice to discuss Twitter’s desire to provide greater
12 transparency regarding the extent of U.S. government surveillance of Twitter’s users through
13 NSLs and FISA court orders. Twitter explained why the DAG Letter should not apply to Twitter,
14 which was not a party to the proceedings that resulted in the DAG Letter. In response, the DOJ
15 and FBI told Twitter that the DAG Letter set forth the limits of permissible transparency-related
16 speech for Twitter and that the letter would not be amended or supplemented with additional
17 options of preapproved speech.

18 53. In February 2014, Twitter released its Transparency Report for the second half of
19 2013, which included two years of data covering global government requests for account
20 information. In light of the government’s admonition regarding more expansive transparency
21 reporting than that set forth in the DAG Letter, Twitter’s February 2014 Transparency Report did
22 not include quantitative information at the level of granularity Twitter felt provided an accurate
23 and representative view of its receipt of and response to U.S. national security requests and had
24 sought approval from Defendants to disclose.

25 54. In a blog post, Twitter explained the importance of reporting more specific
26 quantitative information to users about government surveillance. Twitter also explained how the
27 U.S. government was unconstitutionally prohibiting Twitter from providing a meaningful level
28

1 of quantitative detail regarding U.S. government national security requests Twitter had or may
2 have received:

3 We think the government’s restriction on our speech not only
4 unfairly impacts our users’ privacy, but also violates our First
5 Amendment right to free expression and open discussion of
6 government affairs. We believe there are far less restrictive ways
7 to permit discussion in this area while also respecting national
8 security concerns. Therefore, we have pressed the U.S. Department
9 of Justice to allow greater transparency, and proposed future
10 disclosures concerning national security requests that would be
11 more meaningful to Twitter’s users.

12 Jeremy Kessel, *Fighting for more #transparency*, Twitter Blog (Feb. 6, 2014, 14:58 UTC),
13 <https://blog.twitter.com/2014/fighting-for-more-transparency>.

14 55. On or about April 1, 2014, Twitter submitted a draft July 2014 Transparency
15 Report to the FBI, explaining:

16 We are sending this to you so that Twitter may receive a
17 determination as to exactly which, if any, parts of its Transparency
18 Report are classified or, in the Department’s view, otherwise may
19 not lawfully be published online.

20 A copy of Twitter’s letter dated April 1, 2014, was filed with this Court as Dkt. No. 1, Ex. 3.
21 Twitter’s draft Transparency Report, which has already been filed and submitted to this Court, is
22 Dkt. No. 1, Ex. 4.

23 56. Through its draft Transparency Report, Twitter seeks to disclose certain
24 categories of quantitative information to its users for the period July 1 to December 31, 2013,
25 including:

- 26 a. The number of NSLs and FISA orders Twitter received, if any, in actual
27 aggregate numbers (including “zero,” to the extent that that number was
28 applicable to an aggregate number of NSLs or FISA orders or to specific
kinds of FISA orders that Twitter may have received);
- 29 b. The number of NSLs and FISA orders received, if any, reported
30 separately, in ranges of one hundred, beginning with 1–99;
- 31 c. The combined number of NSLs and FISA orders received, if any, in
32 ranges of twenty-five, beginning with 1–24;
- 33 d. A comparison of Twitter’s proposed (i.e., smaller) ranges with those
34 authorized by the DAG Letter;

- 1 e. A comparison of the aggregate numbers of NSLs and FISA orders
received, if any, by Twitter and the five providers to whom the DAG
2 Letter was addressed; and
- 3 f. A descriptive statement about Twitter's exposure to national security
surveillance, if any, to express the overall degree of government
4 surveillance it is or may be subject to.

5 57. For five months, Defendant FBI considered Twitter's written request for review
6 of the draft Transparency Report. In a letter dated September 9, 2014, the FBI denied Twitter's
7 request. A copy of the FBI's letter was filed with this Court as Dkt. No. 1, Ex. 5. Defendant
8 FBI's letter did not, as requested, identify exactly which specific information in the draft
9 Transparency Report was classified and therefore could not lawfully be published. Instead, the
10 letter stated that "information contained in the report" cannot be publicly released; it provided
11 examples of such information in the draft Transparency Report; and it relied on a general
12 assertion of national security classification and on the pronouncements in the DAG Letter as its
13 bases for denying publication:

14 We have carefully reviewed Twitter's proposed transparency
report and have concluded that information contained in the report
15 is classified and cannot be publicly released.

16 . . . Twitter's proposed transparency report seeks to publish data. .
17 .in ways that would reveal classified details about [government]
surveillance and that go beyond what the government has
18 permitted other companies to report This is inconsistent with
the January 27th framework [set forth in the DAG Letter] and
19 discloses properly classified information.

20 (Dkt. No. 1, Ex. 5, at 1.) Defendant FBI reiterated that Twitter could engage only in speech that
21 did not exceed the preapproved speech set forth in the DAG Letter. It noted, for example, that
22 Twitter could

23 explain that only an infinitesimally small percentage of its total
24 number of active users was affected by [government surveillance
by] highlighting that less than 250 accounts were subject to all
25 combined national security legal process That would allow
Twitter to explain that all national security legal process received
26 from the United States affected, at maximum, only 0.0000919
percent (calculated by dividing 249 by 271 million) of Twitter's
27 total users. In other words, Twitter is permitted to *qualify* its
description of the total number of accounts affected by all national
28

1 security legal process it has received but it cannot *quantify* that
2 description with the specific detail that goes well beyond what is
3 allowed under the January 27th framework and that discloses
4 properly classified information.

5 (*Id.* at 1–2.) (emphasis in original)

6 58. Because Defendant FBI’s response did not identify the exact information in the
7 draft Transparency Report that could not be published, and because the publication of any
8 specific fact the government considers classified could result in prosecution, fines, and
9 imprisonment, Twitter did not at that time publish any part of the report.

10 59. Defendant FBI did not, as the First Amendment requires, narrowly prohibit only
11 speech that would harm national security; instead, it prohibited all of the speech in Twitter’s
12 draft Transparency Report and thereby prohibited speech that would not properly be subject to
13 classification, in violation of the First Amendment.

14 **F. Twitter Brings Suit Against Defendants**

15 60. On October 7, 2014, Twitter filed a Complaint against Defendants seeking
16 declaratory and injunctive relief. (Dkt. No. 1.)

17 61. On November 17, 2014, Defendant DOJ publicly filed what it described as an “an
18 unclassified copy of [Twitter’s] proposed report, with classified national security information
19 redacted.” (Dkt. No. 21.) This redacted version excised quantitative data regarding Twitter’s
20 receipt of national security legal process that constitutes information regarding matters of very
21 significant public interest and is not properly classified under the government’s own
22 classification standards.

23 62. On January 9, 2015, Defendants filed a partial motion to dismiss. (Dkt. No. 28.)
24 In a footnote, Defendants noted their position that “[o]f course, disclosing the number of Title I
25 orders received would violate” a nondisclosure provision within a FISC order “as it would
26 ‘disclose . . . the existence’ of each of the orders.” (Dkt. No. 28, at 5 n.2.) Defendants also
27 repeatedly claimed that the basis for their prohibition on Twitter’s speech was not the DAG
28 Letter, but rather the underlying national security statutes, including FISA, and FISA orders
issued thereunder.

1 63. On March 4, 2015, Defendants filed a reply in support of the partial motion to
2 dismiss. (Dkt. No. 57.) In that filing, Defendants asserted that “the Government has never taken
3 [the] position” that a communications provider that has never received an NSL or FISA order is
4 prohibited from saying so. (Dkt. No. 57, at 8.)

5 64. A hearing on Defendants’ partial motion to dismiss was held on May 5, 2015.

6 **G. Passage of the USA FREEDOM Act, Supplemental Briefing, and the District**
7 **Court’s Ruling**

8 65. On June 2, 2015, President Obama signed into law the USA FREEDOM Act. The
9 statute contains no express findings, and nothing in the legislative history indicates that Congress
10 made any factual finding regarding how much information regarding U.S. national security
11 requests could be disclosed without harm to national security. The USAFA provides four new
12 options for providers such as Twitter to report the volume of national security process received.
13 Like the DAG Letter, the USA FREEDOM Act provides for wide reporting bands with more
14 granularity permitted where the number of FISA orders received are combined with the number
15 of NSLs received. On its face, the USAFA is permissive: that is, it allows communications
16 providers to use one of the reporting options it provides, but it contains no express prohibition on
17 other disclosures, and it does not amend or otherwise affect any of the nondisclosure
18 requirements in FISA.

19 66. On June 11, 2015, this Court directed the parties to “file supplemental briefing on
20 the effect of this legislation, both as to the pending partial motion to dismiss and as to the
21 ultimate claims for relief in Plaintiff’s Complaint.” (Dkt. No. 69.) The Court subsequently
22 requested additional briefing on discrete questions. (Dkt. No. 81.) Defendants took the position
23 in that supplemental briefing that the USA FREEDOM Act superseded the DAG Letter, but was
24 permissive only and did not itself prohibit any speech. Defendants continued to claim that any
25 prohibition on Twitter’s speech came from the underlying national security statutes, including
26 FISA, and FISA orders issued thereunder.

27
28

1 classification authority [must] determine[] that the unauthorized disclosure of the information
2 reasonably could be expected to result in damage to the national security . . . and the original
3 classification authority is able to identify or describe the damage.” *Id.* For classification at the
4 “Secret” and “Top Secret” levels, the classifying entity must expect “serious” and “exceptionally
5 grave” damage, respectively. *Id.* § 1.2.

6 76. The information that Defendants redacted from Twitter’s draft Transparency
7 Report was not properly classified under Executive Order No. 13526. That information therefore
8 is not properly classified and, as a consequence, is therefore protected by the First Amendment.

9 77. The federal government often classifies information that could not be expected to
10 cause damage to U.S. national security. For example, Secretary of State John Kerry has stated
11 that “there’s a massive amount of overclassification.” He said: “People just stamp it on quickly
12 because it’s a way to sort of be correct if anybody had a judgment that somehow they had been
13 wrong about whether it should be classified or not. So the easy thing is to classify it and put it
14 away.” Mark Hensch, *Kerry: State has ‘massive amount of overclassification,’* The Hill (Sept. 5,
15 2015), available at [http://thehill.com/blogs/ballot-box/presidential-races/252769-kerry-state-has-](http://thehill.com/blogs/ballot-box/presidential-races/252769-kerry-state-has-massive-amount-of-overclassification)
16 [massive-amount-of-overclassification](http://thehill.com/blogs/ballot-box/presidential-races/252769-kerry-state-has-massive-amount-of-overclassification). In 2014, the Defense Intelligence Agency admitted that its
17 personnel “often misclassify, and typically that means over-classify, information.” Matt Sledge,
18 *Intelligence Agencies Won’t Release Reports of Excessive Secrecy*, Huffington Post (Jan. 31,
19 2014), available at [http://www.huffingtonpost.com/2014/01/28/cia-over-classification-](http://www.huffingtonpost.com/2014/01/28/cia-over-classification-report_n_4680479.html)
20 [report_n_4680479.html](http://www.huffingtonpost.com/2014/01/28/cia-over-classification-report_n_4680479.html).

21 78. In October 2010, President Obama signed into law H.R. 533, The Reducing Over-
22 Classification Act. This bipartisan legislation is specifically intended to “decrease over-
23 classification and promote information sharing.” Ben Rhodes, *The President Signs H.R. 533, The*
24 *Reducing Over-Classification Act* (Oct. 7, 2010), available at
25 [https://www.whitehouse.gov/blog/2010/10/07/president-signs-hr-553-reducing-over-](https://www.whitehouse.gov/blog/2010/10/07/president-signs-hr-553-reducing-over-classification-act)
26 [classification-act](https://www.whitehouse.gov/blog/2010/10/07/president-signs-hr-553-reducing-over-classification-act). In this legislation, the U.S. Congress found that “over-classification of
27 information interferes with accurate, actionable, and timely information sharing, increases the
28

1 cost of information security, and needlessly limits stakeholder and public access to information.”
2 Reducing Over-Classification Act, Pub. L. 111-258, § 2 (2010).

3 79. Defendants have neither alleged nor demonstrated, nor, on information and belief,
4 can Defendants demonstrate, that the quantitative information Defendants seek to censor poses a
5 threat to U.S. national security, let alone one that is “serious” or “exceptionally grave.” The
6 quantitative information Twitter seeks to release does not, on information and belief, reveal
7 intelligence sources and methods or include specific details about any FISA orders or NSLs
8 Twitter may have received.

9 80. Twitter is an independent corporation and ECS that responds to numerous forms
10 of legal process. Through its transparency reporting, Twitter seeks to publish quantitative data
11 about activity (if any) that it has conducted, using its own personnel and resources. Information
12 about the amount of national security process with which Twitter has been obligated to comply is
13 not “owned by, produced by or for, or . . . under the control of the United States Government.”
14 Exec. Order No. 13526 § 1.1.

15 81. Because Defendants cannot meet the standards necessary for a proper original
16 classification decision, Defendants are foreclosed from asserting that Twitter’s draft
17 Transparency Report constitutes a “derivative” document. Derivative classification means the
18 “incorporating, paraphrasing, restating, or generating in new *form information that is already*
19 *classified*, and marking the newly developed material consistent with the classification markings
20 that apply to the source information.” *Id.* § 6.1(o) (emphasis added). Because the aggregate
21 quantitative information that Twitter seeks to publish was not “already classified,” the draft
22 Transparency Report cannot be a derivatively classified document.

23 82. If the information that Twitter seeks to publish is not properly classified under
24 Executive Order No. 13526, then the government has no other basis for prohibiting its
25 disclosure. Various laws limit Twitter’s disclosure of information related to the legal process it
26 accepts, but those laws cannot and do not automatically classify that information. Defendants
27 rely on the nondisclosure provisions in FISA as a basis for restricting Twitter’s ability to publish
28

1 its draft Transparency Report, but those provisions do not restrict disclosure of the information
2 redacted from that Report.

3 83. In restraining Twitter's speech, Defendants have misinterpreted FISA, which does
4 not prohibit Twitter from disclosing the information it seeks to publish about the number of
5 FISA orders it has received, if any. Instead, FISA protects the secrecy of the contents of specific
6 FISA orders, their targets, and details of ongoing investigations. Twitter has no statutory
7 obligation to remain silent about whether or not it has ever received FISA orders as a general
8 matter, nor do FISA or the terms of FISA orders prohibit Twitter from disclosing the aggregate
9 number of each type of FISA order it may have received, or whether it has received no orders at
10 all or no orders of a particular type.

11 84. To the extent that FISA's secrecy provisions are construed to categorically
12 prohibit Twitter from publishing the quantitative information it seeks to publish, the FISA
13 secrecy provisions are unconstitutional, including because they constitute a prior restraint and
14 content-based restriction on speech in violation of Twitter's First Amendment right to speak
15 about truthful matters of public concern. The restriction also constitutes viewpoint
16 discrimination, as Defendants have allowed speech on this issue that conforms to their own
17 viewpoint, but barred other interested parties from expressing different views on the same topic.
18 Moreover, the restriction on Twitter's speech is not narrowly tailored to serve a compelling
19 governmental interest.

20 85. When the federal government improperly classifies information and then prevents
21 its publication, it violates the First Amendment. Therefore, Twitter seeks a declaration that (a)
22 the standards set forth in Executive Order No. 13526 constitute the only grounds on which the
23 government may rely to prohibit disclosure of the redacted information in the draft Transparency
24 Report; (b) the FISA nondisclosure provisions have no applicability to the redacted information
25 in the draft Transparency Report; and (c) the redacted information in the draft Transparency
26 Report was improperly classified, and that Twitter has a First Amendment right to release the
27 report publicly in unredacted form or, in the alternative, to release the report with all of the
28 information not properly classified under Executive Order No. 13526.

COUNT III

The Espionage Act is unconstitutional as applied to Twitter.

92. Twitter incorporates the allegations contained in paragraphs 1 through 91, above.

93. Defendants’ public statements have given rise to a reasonable concern that Twitter would face prosecution under the Espionage Act, including under 18 U.S.C. § 793(d), if it were to disclose the aggregate number of FISA orders it has received, if any, or any other information in its draft Transparency Report that has been redacted by Defendants and/or is not consistent with the permissible transparency reporting options in the USAFA.

94. Given the confusion that Defendants have created regarding what disclosures are permissible as a result of Defendants’ contradictory positions on reporting zero requests, the basis or bases for prohibiting speech (whether it derives from classification authority or from the nondisclosure provisions of FISA), and their pattern of selective declassification of specific FISA-related and other national security matters to allow government speech, it is unlawful to apply or threaten to apply criminal penalties to communications providers that seek only to share with their users the number of requests they may receive and/or other information regarding the amount of requests received after a fixed period of nondisclosure. Furthermore, the Espionage Act itself does not prohibit Twitter from disclosing the aggregate number of FISA orders it may have received, if any, or any other information in its draft Transparency Report that has been redacted by Defendants, as such prohibition would be an unconstitutional violation of Twitter’s First Amendment rights.

95. Any such prosecution of Twitter would be unconstitutional as violating Twitter’s First Amendment right to speak truthfully about matters of public interest.

96. Twitter seeks a declaration that any such prosecution would violate the Constitution and an injunction barring Defendants from prosecuting Twitter for engaging in constitutionally-protected speech.

PRAYER FOR RELIEF

WHEREFORE, Twitter prays for the following relief:

A. A declaratory judgment that:

- i. The standards set forth in Executive Order No. 13526 constitute the only grounds on which the government may rely to prohibit disclosure of the redacted information in the draft Transparency Report;
- ii. The redacted information in the draft Transparency Report is not subject to classification under the standards in Executive Order No. 13526, and that Twitter has a First Amendment right to release the entire report publicly in unredacted form or, in the alternative, to release the report with all of the information not properly classified under Executive Order No. 13526;
- iii. The FISA nondisclosure provisions have no applicability to the redacted information in the draft Transparency Report;
- iv. Any interpretation of FISA that prohibits publication of the unredacted Transparency Report is unconstitutional;
- v. The FISA secrecy provisions are facially unconstitutional under the First Amendment because they do not require nondisclosure orders to contain a defined duration;
- vi. The FISA secrecy provisions are unconstitutional under the First Amendment as applied to Twitter;
- vii. FISA does not restrict reporting aggregate numbers of FISA orders received;
- viii. Any interpretation of FISA that prohibits reporting aggregate numbers of FISA orders received is unconstitutional;
- ix. Prosecution of Twitter under the Espionage Act for disclosing the aggregate number of FISA orders it has received, if any, or any other information in its draft Transparency Report that has been redacted by Defendants, would be a violation of Twitter’s First Amendment rights; and
- x. Defendants may not prohibit Twitter from publishing, in Transparency Reports covering periods of time subsequent to the draft Transparency Report, the categories of information that this Court finds not subject to classification, and therefore protected by the First Amendment, in connection with the draft Transparency Report.

B. A preliminary and permanent injunction prohibiting Defendants, their affiliates, agents, employees, and attorneys, and any and all other persons in active concert or participation with them, from seeking to enforce the unconstitutional prohibitions on Twitter’s speech, or to prosecute or otherwise seek redress from Twitter for exercising its First Amendment rights.

1 C. A preliminary and permanent injunction (a) barring Defendants, their affiliates,
2 agents, employees, and attorneys, and any and all other persons in active concert or participation
3 with them, from prohibiting Twitter from publishing information redacted by Defendants from
4 the draft Transparency Report that is not properly classified; and (b) barring defendants from
5 prohibiting Twitter from publishing similar information in future Transparency Reports covering
6 subsequent periods of time.

7 D. An award of attorneys' fees and costs to Twitter to the extent permitted by law.

8 E. Such further and other relief as this Court deems just and proper.

9
10 Dated: May 24, 2016

MAYER BROWN LLP
ANDREW JOHN PINCUS

11
12
13 /s/ Andrew John Pincus
ANDREW JOHN PINCUS (*Pro Hac Vice*)
apincus@mayerbrown.com
1999 K Street, NW
Washington, DC 20006
Telephone: (202) 263-3220
Facsimile: (202) 263-3300

14
15
16
17 MAYER BROWN LLP
LEE H. RUBIN (SBN 141331)
lrubin@mayerbrown.com
Two Palo Alto Square, Suite 300
3000 El Camino Real
Palo Alto, CA 94306-2112
Telephone: (650) 331-2000
Facsimile: (650) 331-2060

18
19
20
21 PERKINS COIE LLP
MICHAEL A. SUSSMANN (*Pro Hac Vice*)
MSussmann@perkinscoie.com
700 Thirteenth Street, NW, Suite 600
Washington, DC 20005-3960
Telephone: (202) 654-6333
Facsimile: (202) 654-9127

22
23
24
25 Attorneys for Plaintiff
TWITTER, INC.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

CERTIFICATE OF SERVICE

The undersigned certifies that, on May 24, 2016, I caused the foregoing document to be filed electronically through the Court’s CM/ECF System and served on all counsel of record.

/s/ Andrew John Pincus
ANDREW JOHN PINCUS

Attorneys for Plaintiff
TWITTER, INC.