Eric D. Miller, Bar No. 218416
EMiller@perkinscoie.com
Michael A. Sussmann, D.C. Bar No. 433100
(*pro hac vice to follow*)
MSussmann@perkinscoie.com
James G. Snell, Bar No. 173070
JSnell@perkinscoie.com
Hayley L. Berlin, D.C. Bar No. 1011549
(*pro hac vice to follow*)
HBerlin@perkinscoie.com
PERKINS COIE LLP
3150 Porter Drive
Palo Alto, CA 94304-1212
Tel: 650-838-4300
Fax: 650-838-4350

Attorneys for Plaintiff
Twitter, Inc.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

TWITTER, INC.,

Plaintiff,

v.

ERIC HOLDER, Attorney General of the United States,

THE UNITED STATES DEPARTMENT OF JUSTICE,

JAMES COMEY, Director of the Federal Bureau of Investigation, and

THE FEDERAL BUREAU OF INVESTIGATION,

Defendants.

Case No. 14-cv-4480

COMPLAINT FOR DECLARATORY JUDGMENT, 28 U.S.C. §§ 2201 and 2202

I. NATURE OF THE ACTION

1. Twitter brings this action for declaratory judgment 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, while at the same time prohibiting service providers such as Twitter from providing their own informed perspective as potential recipients of various national security-related requests.

3. Twitter seeks to lawfully publish information contained in a draft Transparency Report submitted to the Defendants on or about April 1, 2014. After five months, Defendants informed Twitter on September 9, 2014 that "information contained in the [transparency] report is classified and cannot be publicly released" because it does not comply with their framework for reporting data about government requests under the Foreign Intelligence Surveillance Act ("FISA") and the National Security Letter statutes. This framework was set forth in a January 27, 2014 letter from Deputy Attorney General James M. Cole to five Internet companies (not including Twitter) in settlement of prior claims brought by those companies (also not including Twitter) (the "DAG Letter").

4. The Defendants' position forces Twitter either to engage in speech that has been preapproved by government officials or else to refrain from speaking altogether. Defendants provided no authority for their ability to establish the preapproved disclosure formats or to impose those speech restrictions on other service providers that were not party to the lawsuit or settlement.

5. Twitter's ability to respond to government statements about national security surveillance activities and to discuss the actual surveillance of Twitter users is being unconstitutionally restricted by statutes that prohibit and even criminalize a service provider's disclosure of the number of national security letters ("NSLs") and court orders issued pursuant to FISA that it has received, if any. In fact, the U.S. government has taken the position that service

providers like Twitter are even prohibited from saying that they have received zero national security requests, or zero of a particular *type* of national security request.

6. These restrictions constitute an unconstitutional prior restraint and content-based restriction on, and government viewpoint discrimination against, Twitter's right to speak about information of national and global public concern. Twitter is entitled under the First Amendment to respond to its users' concerns and to the statements of U.S. government officials by providing more complete information about the limited scope of U.S. government surveillance of Twitter user accounts—including what types of legal process have *not* been received by Twitter—and the DAG Letter is not a lawful means by which Defendants can seek to enforce their unconstitutional speech restrictions.

II. PARTIES

7. Plaintiff Twitter, Inc. ("Twitter") is a corporation with its principal place of business located at 1355 Market Street, Suite 900, San Francisco, California. Twitter is a global information sharing and distribution network serving over 271 million monthly active users around the world. People using Twitter write short messages, called "Tweets," of 140 characters or less, which are public by default and may be viewed all around the world instantly. As such, Twitter gives a public voice to anyone in the world—people who inform and educate others, who express their individuality, who engage in all manner of political speech, and who seek positive change.

8. Defendant Eric Holder is the Attorney General of the United States and heads the United States Department of Justice ("DOJ"). He is sued in his official capacity only.

9. Defendant DOJ is an agency of the United States. Its headquarters are located at 950 Pennsylvania Avenue, NW, Washington, D.C.

10. Defendant James Comey is the Director of the Federal Bureau of Investigation ("FBI"). He is sued in his official capacity only.

11. Defendant FBI is an agency of the United States. Its headquarters are located at 935 Pennsylvania Avenue, NW, Washington, D.C.

III. JURISDICTION

12. This Court has original subject matter jurisdiction under 28 U.S.C. § 1331, as this matter arises under the Constitution, laws, or treaties of the United States. More specifically, this Court is authorized to provide declaratory relief under the Declaratory Judgment Act, 28 U.S.C. §§ 2201–2202, relating to, among other things, Twitter's contention that certain nondisclosure requirements and related penalties concerning the receipt of NSLs and court orders issued under FISA, as described below, are unconstitutionally restrictive of Twitter's First Amendment rights, either on their face or as applied to Twitter, and Twitter's contention that Defendants' conduct violates the Administrative Procedure Act, 5 U.S.C. § 551, *et seq.*

IV. VENUE

13. Venue is proper in this Court under 28 U.S.C. § 1391(b) because a substantial part of the events giving rise to the action occurred in this judicial district, Twitter resides in this district, Twitter's speech is being unconstitutionally restricted in this district, and the Defendants are officers and employees of the United States or its agencies operating under the color of law.

V. FACTUAL BACKGROUND

A. NSL and FISA Provisions Include Nondisclosure Obligations

i. The NSL Statute

14. Section 2709 of the federal Stored Communications Act authorizes the FBI to issue NSLs to electronic communication service ("ECS") providers, such as Twitter, compelling them to disclose "subscriber information and toll billing records information" upon a certification by the FBI that the information sought is "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities." 18 U.S.C. § 2709(a), (b).

15. Section 2709(c)(1) provides that, following certification by the FBI, the recipient of the NSL shall not disclose "to any person (other than those to whom such disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect to the request) that the Federal Bureau of Investigation has sought or obtained access to information or records." 18 U.S.C. § 2709(c)(1). This nondisclosure obligation is imposed upon an ECS by the FBI unilaterally, without prior judicial review. At least two United States district courts have found the nondisclosure provision of § 2709 unconstitutional under the First Amendment. *In re Nat'l Sec. Letter*, 930 F. Supp. 2d 1064 (N.D. Cal. 2013); *Doe v. Gonzales*, 500 F. Supp. 2d 379 (S.D.N.Y. 2007), *affirmed in part, reversed in part, and remanded by Doe, Inc. v. Mukasey*, 549 F.3d 861 (2d Cir. 2008).

16. Any person or entity that violates a NSL nondisclosure order may be subject to criminal penalties. 18 U.S.C. §§ 793, 1510(e).

ii. The Foreign Intelligence Surveillance Act

17. Five subsections ("Titles") of FISA permit the government to seek court-ordered real-time surveillance or disclosure of stored records from an ECS: Title I (electronic surveillance of the content of communications and all communications metadata); Title III (disclosure of stored content and noncontent records); Title IV (provisioning of pen register and trap and trace devices to obtain dialing, routing, addressing and signaling information); Title V (disclosure of "business records") (also referred to as "Section 215 of the USA Patriot Act"); and Title VII (surveillance of non-U.S. persons located beyond U.S. borders).

18. A number of authorities restrict the recipient of a FISA order from disclosing information about that order. These include requirements in FISA that recipients of court orders provide the government with "all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy," 50 U.S.C. § 1805(c)(2)(B); the Espionage Act, 18 U.S.C. § 793 (criminalizing unauthorized disclosures of

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.