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

MAYER BROWN LLP
LEE H. RUBIN (SBN 141331)
lrubin@mayerbrown.com
DONALD M. FALK (SBN 150256)
dfalk@mayerbrown.com
Two Palo Alto Square, Suite 300
3000 El Camino Real
Palo Alto, CA 94306-2112
Tel: (650) 331-2000 / Fax: (650) 331-2060

*Attorneys for Plaintiff Twitter, Inc.*

**UNITED STATES DISTRICT COURT**

**NORTHERN DISTRICT OF CALIFORNIA**

**OAKLAND DIVISION**

TWITTER, INC.,

Plaintiff,

v.

LORETTA E. LYNCH, Attorney General of the United States,

THE UNITED STATES DEPARTMENT OF JUSTICE,

JAMES E. COMEY, Director of the Federal Bureau of Investigation, and THE FEDERAL BUREAU OF INVESTIGATION,

Defendants.

Case No. 14-cv-4480-YGR

**TWITTER, INC.'S OPPOSITION TO DEFENDANTS' MOTION FOR SUMMARY JUDGMENT**

Date: January 24, 2017
Time: 2:00 p.m.
Courtroom 1, Fourth Floor
Hon. Yvonne Gonzalez Rogers

# TABLE OF CONTENTS

## TABLE OF AUTHORITIES

**Cases** **Page(s)**



**TABLE OF AUTHORITIES - Continued**

**Cases** **Page(s)**



**Statutes and Rules** **Page(s)**



**Other Rules & Regulations** **Page(s)**

**TABLE OF AUTHORITIES - Continued**

**Other Authorities** **Page(s)**

## STATEMENT OF ISSUE TO BE DECIDED

Whether Defendants' motion should be denied (1) because they have not carried their burden of showing that the restrictions on Twitter's speech, based on the permissive statutory reporting bands in the USA Freedom Act, are narrowly tailored to avoid serious damage to U.S. national security, or (2) pursuant to Fed. R. Civ. Proc. 56(d), the motion is not ripe for consideration, as Twitter is entitled to complete discovery to determine whether the government's speech restrictions on Twitter are unconstitutional.

## INTRODUCTION

Given the core First Amendment values at stake in this litigation—not only Twitter's right to express its view on a matter of significant public concern, but also the public's right to information necessary to hold political officials accountable—the government bears a "heavy burden" to justify its restrictions on Twitter's speech. *N.Y. Times Co. v. United States*, 403 U.S. 713, 714 (1971) (per curiam) ("*Pentagon Papers*"). Instead of shouldering that burden, however, the government asks this Court to rubberstamp the government's own unsupported conclusions that national security concerns justify its prior restraint on Twitter's speech. Indeed, much of the government's brief proceeds as if this case were governed by the defunct statutory scheme that gave "conclusive effect" to the government's national security assertions, *Twitter, Inc. v. Lynch*, 139 F. Supp. 3d 1075, 1080 (N.D. Cal. 2015)—a provision that two courts held unconstitutional and Congress wisely repealed.

The government's request for "utmost deference," is insupportable. Motion for Summary Judgment ("MSJ") 18. It is well-established that content-based prior restraints—like the speech restriction here—are "presumptively unconstitutional and may be justified only if the government proves that they are narrowly tailored to serve compelling state interests." *Reed v. Town of Gilbert*, 135 S. Ct. 2218, 2226 (2015); *see also Al Haramain Islamic Found., Inc. v. U.S. Dep't of Treasury*, 686 F.3d 965, 982 (9th Cir. 2012) ("*Al Haramain v. Treasury*"). Abstract or vague invocations of even "serious" damage to national security are insufficient, *see Pentagon Papers*, 403 U.S. at 714, and courts have a constitutional duty to review claims that a speech restriction is necessary to protect national security with a "very careful, indeed a skeptical, eye," *Al-Haramain*

*Islamic Found., Inc. v. Bush*, 507 F.3d 1190, 1203 (9th Cir. 2007) ("*Al-Haramain v. Bush*").

Rather than conducting the individualized inquiry needed to justify a content-based restraint, the government maintains that it may ban any speech that falls outside the disclosure bands in 50 U.S.C. § 1874—a statute that sets out only the disclosures the government *must* permit, while expressly allowing the government to permit more detailed disclosures when justified, *see* 50 U.S.C. § 1874(c). Yet the government's unclassified evidence provides no indication that the ranges in the broad disclosure bands, or their duration, are narrowly tailored to serve the compelling interest of avoiding harm to national security. Indeed, the government did not specify its evidentiary support in the statement of undisputed facts this Court's standing order requires.

The government asserts that it may constitutionally restrict Twitter's speech because it has classified all aggregate information about national security process that falls outside the reporting bands in section 1874. But the government should be put to its proofs—subject to cross-examination and other testing of evidence—of the critical assumptions underlying its classification decision. Section 1874(a) is one-size-fits-all: it applies the permissive reporting bands of 250 or 500 requests to all electronic communications service ("ECS") providers, regardless of the number of users or of national security requests received. To demonstrate that its restriction of Twitter's speech is narrowly tailored, however, the government must show that the disclosure of specific, aggregate numbers can reasonably be expected to cause serious damage to national security no matter how many requests are involved or how many users the platform has. *See* MSJ 2:6, 27:2, 31:5; Steinbach Decl. ¶¶ 1, 5, 30, 39 (asserting that disclosure "reasonably could be expected to result in serious damage").

For example, the government must show that a national security risk is posed by disclosures of 15 or 75 or 155 aggregate requests (rather than 0–499) whether an ECS provider has 300 or 300 million users. The government must show that a disclosure that 5,672 accounts (rather than 5,500–5,999) were under surveillance would pose the same sufficiently serious risk to national security as a disclosure that only 3 accounts were under surveillance (rather than 0–499). And while some statutory bands shrink to 100 after a year, the statute never permits disclosure of specific aggregate numbers. The government thus must show that specific numbers never become

sufficiently stale that they can be disclosed without risking "direct, immediate, and irreparable damage to [national security]." *Pentagon Papers*, 403 U.S. at 730 (Stewart, J., concurring).

The government's unclassified evidence demonstrates none of this. The government nevertheless asks the Court to dispose of this case prematurely, before any reasonable discovery and without the benefit of any genuine adversarial process. That course of action would short-circuit the "procedural safeguards," including meaningful judicial review, necessary for a prior restraint to "avoid[] constitutional infirmity." *Freedman v. State of Maryland*, 380 U.S. 51, 58 (1965). Resolving this motion before discovery is complete also runs counter to Rule 56(d), because Twitter (the nonmovant) has shown that additional facts (including what may be learned from cross-examining the government's "original classifying authority") may further reveal a genuine factual dispute as to whether the government has met its exacting burden to justify its restraints on Twitter's speech. *See* Rubin Decl. ISO Opp. to MSJ ("Rubin Decl."), ¶¶ 11, 25. Twitter is also entitled to obtain security clearance for its lead counsel in order to ensure even-handed and robust *in camera* review—to the extent secrecy is required—of the constitutionality of the government's bases for its classification decision. Clearance will also facilitate any classified discovery ordered under Rule 56(d). In short, the government's unripe and meritless motion should be denied.

## FACTUAL AND PROCEDURAL HISTORY

Twitter has long demonstrated its commitment to providing meaningful transparency to its users and the public about the privacy of the information they share with Twitter. Since 2012, Twitter has published a semiannual "transparency report" providing the aggregate numbers of requests for user information received from governments across the globe, including the United States. ECF No. 21–1. In response to significant media and public concern about government surveillance of Americans' phone records, Twitter sought government approval to publish a Draft Transparency Report that disclosed the *total* numbers of National Security Letters ("NSLs") and requests for user information under the Foreign Intelligence Surveillance Act of 1978 ("FISA"), if any, received between July 1 and December 31, 2013—now nearly three years ago.[1] Twitter also

[1] An NSL is an administrative subpoena from the FBI directing an electronics communications (cont'd)

sought permission to disclose that it had received "zero" of a particular kind of request whenever that might be the case. *See* ECF No. 21–1.

On September 9, 2014, the government informed Twitter that "information contained in the [Draft Transparency] [R]eport is classified and cannot be publicly released." ECF No. 21–2, at 1. The government accordingly generated an unclassified version of the Draft Transparency Report by redacting all the numerical references and characterizations in the Report. *See* ECF No. 21–1. The government asserted that those numbers were classified because their disclosure was "inconsistent with the January 27th framework." ECF No. 21–2, at 1.[2]

Twitter brought this action in response. Its initial complaint alleged that the DAG Letter violated the Administrative Procedure Act, and that the statutory provisions on which the DAG letter was predicated were facially unconstitutional. *See* ECF No. 1. While this case was pending, Congress passed the Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act (the "USA Freedom Act"), Pub. Law No. 114-23, 129 Stat. 268 (June 2, 2015), which superseded the DAG letter and amended the underlying statutes. *See Twitter v. Lynch*, 139 F. Supp. 3d at 1079–80. On October 14, 2015, this Court held *sua sponte* that Twitter's claims were moot, and directed Twitter to file an amended complaint in order to permit Twitter to adapt its claims to the governing statutory authority. *Id.* at 1083.

The Second Amended Complaint ("SAC") asserts that the government's continuing effort to restrain Twitter's speech remains unconstitutional. *See* ECF No. 114. Count I asserts that the government violated the First Amendment in restraining Twitter's publication of the Draft Trans-

---

service provider to turn over certain subscriber information, *see* 18 U.S.C. § 2709; a FISA request permits the FBI to obtain significantly more subscriber information, including message content, but requires pre-approval (after very limited review) by the Foreign Intelligence Surveillance Court (the "FISC"), *see* 50 U.S.C. §§ 1801, 1804, 1805.

[2] The "January 27th framework" refers to a January 27, 2014, letter from Deputy Attorney General James M. Cole to the general counsels of Facebook, Google, LinkedIn, Microsoft and Yahoo! (the "DAG Letter"). *See* ECF No.1, Exh. 1. The DAG Letter was the product of a settlement of litigation those companies brought in the FISC to challenge restrictions on their disclosure of information about the government's surveillance program. *See id.* at 1. The DAG Letter purported to apply to all ECS providers—not just the parties to the litigation. *See id.*: *see also* ECF No.1, Exh. 3. It provided that ECS providers could disclose the number of NSLs and FISA requests the provider received every six months in broad bands of 1000, starting from 0 to 999, or in bands of 250 if the provider aggregated together all the different kinds of national security process it received. ECF No.1, Exh. 1, at 3.

parency Report because its restrictions do not narrowly prohibit only speech that would harm national security (*see* SAC ¶ 59) and thus the underlying classification of the disputed information is unconstitutional. Count II alleges that the classification and prior restraint on Twitter's publication of the redacted information violates the Administrative Procedure Act. *See* 5 U.S.C. §§ 701 *et seq.* And Count III presents an as-applied challenge to the constitutionality of the Espionage Act, 18 U.S.C. § 793(d), on the ground that its application here would permit the government to prosecute Twitter for constitutionally protected speech. Each cause of action turns on the constitutionality of the government's classification of the aggregate numbers that Twitter seeks to disclose.

On November 10, 2016, Twitter served targeted requests for production of documents and interrogatories on the government. *See* Rubin Decl. ¶¶ 3–4, Exh. A–B. Twitter has also served a notice of deposition (with the declaration required by 28 C.F.R. § 16.23(c)) to take the deposition of Executive Assistant Director Michael Steinbach, whom the summary judgment motion identifies as the original classification authority and whose declaration accompanies the motion. *See* Rubin Decl., ¶ 22, Exh. D. In a conference call regarding the status of Defendants' overdue discovery responses, the government represented that, aside from producing documents and information that it has relied upon in its motion, it intends to object (and not respond) to Twitter's discovery requests on the ground that its summary judgment motion should be resolved without discovery. *Id.* at ¶ 7.[3] Earlier today, the government served its responses to Twitter's First Set of Interrogatories; as represented, the responses are generally confined to information that the government is affirmatively relying on in support of its Motion. *Id.* ¶ 8, Exh. C.

## ARGUMENT

### A. The Government's Content-Based Prior Restraint of Twitter's Speech Is Presumptively Unconstitutional and Subject to Strict Scrutiny.

The government incorrectly suggests that this Court could uphold the constitutionality of the government's content-based restraint on Twitter's speech *without* considering whether the

[3] The government's summary judgment motion was not accompanied by a separate statement "of the material facts as to which the moving party contends there is no genuine issue to be tried" as required by Rule 9 of this Court's Standing Order. That failure provides an additional basis to deny the government's unripe motion. *See Falcon Enters., Inc. v. Publishers Serv., Inc.*, 438 F. App'x 579, 582 (9th Cir. 2011).

restriction is narrowly tailored to serve a compelling government interest. *See* MSJ 10, 21 n.10. Indeed, the government appears to think that the only pertinent question is whether it reasonably interpreted its own administrative guidelines to conclude that a restraint on Twitter's speech was proper. MSJ 10; *cf.* Executive Order 13526 (reciting the four conditions for classification, the last being that the information sought to be disclosed "could reasonably be expected to result in damage to the national security").

That logic is circular: It would require the Court to determine the constitutionality of a prior restraint solely by reference to the administrative standard used to impose it. But to the extent the government's application of its administrative guidelines conflicts with the First Amendment—by imposing a prior restraint in the absence of a direct and immediate harm to national security, by circumventing the narrow-tailoring requirement, or both—it is the *administrative regime* that gives way, not the First Amendment. As explained below, the government's speech restriction cannot survive First Amendment review.

**1. The Restriction on Twitter's Speech Is Presumptively Unconstitutional Because It Depends on the Content of Twitter's Message.**

The government's restriction on Twitter's speech is content-based: Twitter may convey information about the number of NSLs and FISA orders it receives, if any, but only if it uses the broad bands in a government-approved formula. *See Reed*, 135 S. Ct. at 2227 ("Government regulation of speech is content based if a law applies to particular speech because of the topic discussed or the idea or message expressed."). Twitter may not speak about its receipt of national security process if its message contains more precise aggregate numbers. Because the legality of Twitter's message depends on its content, the government's restrictions are "presumptively unconstitutional" and may be sustained "only if the government proves that they are narrowly tailored to serve compelling state interests." *Id.* at 2226.

Indeed, the restriction here is particularly suspect because it is viewpoint-based: it effectively "license[s] one side of a debate"—the government—"to fight freestyle," while restricting the range of speech available to the other side. *R.A.V. v. City of St. Paul*, 505 U.S. 377, 392 (1992). Restrictions on an ECS provider's ability to disclose the *fact* that it has received national

security process could "'becom[e] a means of suppressing a particular view,' that is, the view that certain federal investigative powers impose profoundly on individual civil liberties to the point that they violate our constitution." *Doe v. Gonzales*, 386 F. Supp. 2d 66, 75 (D. Conn. 2005) (quoting *Forsyth Cty. v. Nationalist Movement*, 505 U.S. 123, 130–31 (1992)).

The past few years have seen a surge in public concern about the scope of the government's surveillance activities, and the lack of meaningful accountability and oversight. *See, e.g.*, George Gao, *What Americans Think About NSA Surveillance, National Security and Privacy*, PewRes.Ctr. (May 29, 2015), http://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/. For example, the Pew Research Center recently reported that "[a] majority of Americans (54%) disapprove of the U.S. government's collection of telephone and internet data as part of anti-terrorism efforts," and "two-thirds believe there aren't adequate limits on what types of data can be collected." *Id.* In addition, "*70% of social networking site users* . . . are at least somewhat concerned about the government accessing some of the information they share on social networking sites without their knowledge." Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PewRes.Ctr. (Nov. 12, 2014) (emphasis added), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.

As a potential recipient of national security process, Twitter has a unique and valuable perspective on the scope of government surveillance, as well as information that would significantly enhance informed public debate. Twitter wishes to use that information "to dispel . . . users' [well-documented] fears" about the privacy of the information they share with Twitter by providing more precise (yet still aggregate) data about "the limited scope of U.S. surveillance on its platform." ECF No. 21–1, at 2 (Draft Transparency Report).[4] The prior restraint at issue here not only prevents Twitter from conveying this message, but also compels Twitter—if it wishes to speak at all—"to mislead [its] users by reporting overly broad ranges of requests." *Id.*

The impact of the government's restriction on Twitter's speech would be sufficient by itself to trigger strict scrutiny, but the infringement on constitutional freedoms extends far beyond

[4] This action does not challenge the government's restrictions on the disclosure of any other information regarding national security process, if any, in Twitter's possession.

Twitter's rights. As explained above, most social networking site users report concerns about clandestine government surveillance on social media sites, and Twitter reasonably fears that such concerns may have a chilling effect on user speech. More important, without meaningful information about the scope of the government's surveillance program, the public cannot critically review the program or hold officials accountable for its conduct. It was the "desire for government accountability in the face of perceived abuses" that "inspired the Framers to guarantee the rights to speak, to publish, and to petition government." *Cooper v. Dillon*, 403 F.3d 1208, 1214 (11th Cir. 2005). That is because "[t]he right[s] of citizens to inquire, *to hear*, to speak, and *to use information* to reach a consensus is a precondition to enlightened self-government and a necessary means to protect it." *Garcia v. Google, Inc.*, 786 F.3d 727, 730 (9th Cir. 2015) (emphases added) (quoting *Citizens United v. Fed. Election Comm'n*, 558 U.S. 310, 339 (2010)). "The First Amendment creates an open marketplace where ideas, most especially political ideas, may compete without government interference." *N.Y. State Bd. of Elections v. Lopez Torres*, 552 U.S. 196, 208 (2008). To permit the government to restrain the disclosure of information necessary to hold political officials accountable runs contrary to the most fundamental First Amendment principles.

To be sure, the United States has a compelling interest in ensuring the safety of its citizens. Twitter does not dispute that achieving this interest may sometimes require agencies charged with protecting the national security to operate under a cloak of secrecy. But demonstrating a compelling interest is only half of the government's burden under strict scrutiny review, and "[s]imply saying 'military secret,' 'national security,' . . . 'terrorist threat' or invoking an ethereal fear that disclosure will threaten our nation is insufficient" to justify a content-based restraint on speech. *Al-Haramain v. Bush*, 507 F.3d at 1203. As Judge Illston recently observed regarding the potential disclosure of substantive, case-specific information, "[a]s a content-based restriction on speech, [an] NSL nondisclosure provision[] must be narrowly tailored to serve [the government's national security interest] . . . without unduly burdening speech." *In re Nat'l Sec. Letters*, No. 11-CV-02173-SI, 2016 WL 4501210, at *18 (N.D. Cal. Mar. 29, 2016); *see id.* at *20 (finding that restriction in one case was not narrowly tailored).

**2. The Government's Restriction on Twitter's Speech Is a Prior Restraint, Which Triggers a "Heavy Presumption" That It Is Unconstitutional.**

Rigorous constitutional scrutiny applies here for the independent reason that the restriction is a prior restraint—"the most serious and the least tolerable infringement on First Amendment rights." *Neb. Press Ass'n v. Stuart*, 427 U.S. 539, 559 (1976); *see also Pentagon Papers*, 403 U.S. at 714.[5] Prior restraints are inherently suspect because they stop speech even before it occurs, without the "safeguards of the criminal process," and with "less opportunity for public appraisal and criticism." *Neb. Press Ass'n*, 427 U.S. at 589–90 (Brennan, J., concurring) (quoting T. Emerson, *The System of Freedom of Expression* 506 (1970)).

As the party seeking to impose a prior restraint, the government must overcome a "heavy presumption against its constitutional validity." *Id.*, 427 U.S. at 558 (internal quotation marks omitted) (quoting *Carroll v. Princess Anne*, 393 U.S. 175 (1968)). Though the Supreme Court has yet to consider prior restraints in the FISA context, it has consistently placed an onerous burden on the government whenever "the prior restraint falls upon the communication of news and commentary on current events." *Id.* at 559.

In *Pentagon Papers*, for example, the Supreme Court's per curiam opinion held that the United States could not constitutionally enjoin the publication of a "classified" study that discussed sensitive information about the Vietnam war. 403 U.S. at 714. This was so even though, at the time of publication, the United States was still engaged in Vietnam, and the study involved material that had been classified as "Top Secret" and "Secret." *United States v. N.Y. Times Co.*, 328 F. Supp. 324, 326 (S.D.N.Y. 1971). Several Justices wrote separately to explain their differing rationales for joining the Court's opinion. Justice Stewart, joined by Justice White, explained that the government may constitutionally restrict core speech only when the government can demonstrate that "disclosure . . . will surely result in direct, immediate, and irreparable damage to our Nation or its people." 403 U.S. at 730 (Stewart, J., joined by White, J., concurring). Indeed, this was the most *government-friendly* standard that any member of the majority proposed to determine the constitutionality of designating material "classified" and thus

[5] The government takes the position that FISA itself restrains Twitter from disclosing the redacted information in the draft Transparency Report. *See* MSJ 22-23.

not subject to disclosure. *See also* 403 U.S. at 714–19 (Black, J., concurring) (prior restraints on core speech are never constitutional); *id.* at 719–24 (Douglas, J., concurring) (same); *id.* at 726 (Brennan, J., concurring) (prior restraints might be permissible during wartime).

*Pentagon Papers* makes clear, therefore, that prior restraints on speech of public interest are subject to rigorous judicial scrutiny. Like the New York Times in *Pentagon Papers*, Twitter here seeks to publish information of widespread public interest, relating to the operation of government, over an objection that the publication would result in serious harm to national security.[6] As in *Pentagon Papers*, therefore, the government's attempt to restrict Twitter's speech can be upheld only upon a showing, not only that the restraint is narrowly tailored to a compelling government interest, but that the interest is the prevention of "direct, immediate and irreparable damage" to national security. As explained below, in the absence of the most robust adversary proceeding practicable, the Court should not conclude that either showing has been made.

**3. The Strict Scrutiny Applicable to this Content-Based Prior Restraint Precludes the "Utmost" Deference the Government Seeks.**

The government overreaches in asserting that this Court must accord "utmost deference" to its classification determination. MSJ 18. On the contrary, the government must establish that its prior restraint on speech is narrowly tailored to serve a compelling government interest (protecting the national security of the United States). And the government can meet that threshold only by offering specific, concrete evidence sufficient to satisfy the court that the restricted speech would "surely" result in "immediate, and irreparable," damage to national security. *Pentagon Papers*, 403 U.S. at 730; *Holder v. Humanitarian Law Project*, 561 U.S. 1, 27–28 (2010); *Al-Haramain v. Bush*, 507 F.3d at 1203–04. In asking the Court to grant summary judgment without determining whether its speech restrictions are in fact narrowly tailored to avoid harm to national security, the government relies principally on cherry-picked quotes culled from cases that have no application here.

*C.I.A. v. Sims*, 471 U.S. 159 (1985), for example, did not involve a First Amendment

[6] Consumers increasingly get their news from ECS platforms like Twitter, YouTube, and Facebook, rather than traditional news sources. *What Is Happening to Television News?*, Univ. of Oxford, Reuters Inst. for the Study of Journalism (April 6, 2016), http://www.digitalnewsreport.org/publications/2016/what-is-happening-to-television-news/.

claim. Rather, *Sims* merely held that—as a matter of statutory interpretation—the Freedom of Information Act ("FOIA") did not require the CIA to disclose the *specific names* of various individuals and entities who provided the Agency's intelligence. *Id.* at 173. The deference accorded the Executive's interpretation of a statute has no bearing on the application of strict scrutiny to a content-based prior restraint.[7]

Similarly, neither *Snepp v. United States*, 444 U.S. 507 (1980), nor *Department of Navy v. Egan*, 484 U.S. 518 (1988), were decided on First Amendment grounds. Each turned on the rights of the United States acting in its capacity as employer: *Snepp* involved a *post*-publication remedy for the employee's breach of contractual and fiduciary duties, and *Egan* held that the Merit Systems Protection Board lacked authority to review the denial of an employee's security clearance. And it has long been established that "[a] government entity has broader discretion to restrict speech when it acts" as an employer. *Garcetti v. Ceballos*, 547 U.S. 410, 418 (2006); *see also Snepp*, 444 U.S. at 509 n.3 (federal employer may impose "reasonable restrictions on employee activities that in other contexts might be protected by the First Amendment"). It was in the employment context that the court in *Shaffer v. DIA*, 102 F. Supp. 3d 1 (D.D.C. 2015), sustained a subset of redactions that the government sought, but only on the basis of "a precise explanation for each" redaction. *Id.* at 3. Other redactions were rejected.

Nor does *Holder v. Humanitarian Law Project*, 561 U.S. 1 (2010), suggest that courts should simply defer to the government's determination that a speech restriction is necessary to protect national security. On the contrary, the Court in that case rested on an extensive factual record supporting the government's assertions, and flatly rejected the government's invitation to apply only "intermediate scrutiny." *Id.* at 27–28. The Court made clear that restrictions on speech must survive more exacting review, even in the national security context. *Id.*

*Holder* involved an as-applied challenge to a federal statute which criminalized the knowing provision of "material support or resources to a foreign terrorist organization." *Id.* at 1. The plaintiffs claimed that the statute unconstitutionally prohibited them from supporting the

[7] *Center for National Security Studies v. U.S. Department of Justice*, 331 F.3d 918, 920 (D.C. Cir. 2003), similarly involved an attempt to compel the government *under the FOIA* to disclose *detailed personal information* about individuals detained after the September 11 terrorist attacks.

"lawful" activities of foreign terrorist organizations. The attorney general had adduced evidence that the terrorist groups at issue were responsible for "extensive suicide bombings and political assassinations" that had killed thousands, *id.* at 29–30, and that support for such groups was "fungible" because any donation "frees up other resources within the organization that may be put to violent ends," *id.* at 30–31. In light of this evidence, the Court was "convinced that Congress [and the Executive] w[ere] justified" in concluding that speech made "under the direction of, or in coordination with foreign [terrorist] groups" does, in fact, advance terrorism. *Id.* at 26, 29–31.

But *Holder* does not help the government here. Though the Court found the statute constitutional *as applied* to the plaintiffs, it took pains to emphasize that its holding was narrow, and did not apply to "pure political speech." *Id.* at 25–26 (plaintiffs remain free to "speak and write freely about the [terrorist organizations], the governments of [the countries in which those organizations operated], human rights, and international law"). "In particular," the Court explained its holding "in no way suggest[ed] that a regulation of independent speech would pass constitutional muster, *even if the government were to show that such speech benefits foreign terrorist organizations.*" *Id.* at 39 (emphasis added). As a prior restraint, the restriction of "independent speech" here is even less likely to survive review.

Finally, the government's presentation of *Al-Haramain v. Bush* misapprehends the legal principles undergirding that decision. That case involved a claim by a designated terrorist organization that it had unlawfully been subject to warrantless electronic surveillance. 507 F.3d at 1193. The evidence establishing that the surveillance had occurred was classified as "Top Secret," but had been inadvertently disclosed during a proceeding to freeze the organization's assets. *Id.* After viewing the "Top Secret" document with a "very careful, indeed a skeptical, eye," the Ninth Circuit agreed that it was properly protected by the state secrets privilege. *Id.* at 1203. Without that document, the plaintiff could not establish standing. *Id.* at 1204–05.

Thus, *Al-Haramain v. Bush* stands, not for a rule of unquestioning deference to assertions of national security concerns, but for precisely the opposite proposition: that judges reviewing claims relating to national security have a "special burden to assure [themselves]" that constitutional rights are not being unduly infringed. *Id.* at 1203–04. That is especially so if review

requires some use of *in camera* proceedings, which (if conducted *ex parte*) "ineluctably place[] the court in a role that runs contrary to our fundamental principle of a transparent judicial system." *Id.* The Ninth Circuit reached its conclusion in *Al-Haramain v. Bush* only after "spen[ding] considerable time examining the government's declarations (both publicly filed and those filed under seal)," and finding that the government's assertions were "*exceptionally* well documented." *Id.* at 1203 (emphasis added). To be sure, the court "acknowledge[d]" the need for some "defer[ence] to the Executive on matters of foreign policy and national security," but nonetheless insisted that the government produce "sufficient detail" to permit "meaningful examination" of its state secrets privilege claim. *Id.* at 1203.

**B. The Government Has Not Carried Its Burden of Establishing—as a Matter of Law—That Its Prior Restraint on Twitter's Speech Is Narrowly Tailored to Achieving the Government's National Security Interest.**

From all that appears in the unclassified record, the government's showing cannot withstand the "critical, and indeed, skeptical" review that *Al-Haramain v. Bush*, 507 F.3d at 1203, requires to ensure that a content-based, prior restraint is narrowly tailored (as required by *Al-Haramain v. Treasury*, 686 F.3d at 997) to protecting national security,.

**1. The Government's Reliance on the Disclosure Bands Without Any Individualized Inquiry into the Risks Posed by Twitter's Speech Precludes a Finding That the Prior Restraint Was Narrowly Tailored.**

To begin with, the government has not explained how a prohibition on disclosure beyond the bands in 50 U.S.C. § 1874 is narrowly tailored to prevent a national security risk that would be sufficiently severe to justify the kind of speech restriction placed on Twitter here—that is, a content-based prior restraint. The statute itself contemplates that different forms of disclosures may be appropriate in particular circumstances, with the bands serving only as a safe harbor. *See* 50 U.S.C. § 1874(c). Thus, contrary to the government's assertion that the bands stake out Congress's view of the limit of what can safely be disclosed, *see* MSJ 14 (citing *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 635 (1952) (Jackson, J., concurring)), Congress has expressly authorized the government to permit more granular disclosures on a case-by-case basis, as appropriate.

By presenting those broad reporting bands as the sole basis for asserting that Twitter's

contemplated disclosures would seriously damage national security, the government has conceded that it failed to make an individualized inquiry into whether Twitter's *specific* proposed speech would cause such harm. *See* Steinbach Decl. ¶ 23 (only basis for September 8, 2014 classification was "January 27 framework"—i.e., the broad reporting bands), ¶ 29 (information more granular than permitted under the current reporting scheme necessarily is "properly classified"). That is, the government has not assessed whether any incremental harm to national security would result from the disclosure of Twitter's specific numbers rather than the corresponding bands, in light of Twitter's user base of 240 million (at the time of the Draft Transparency Report), the passage of time (the Report covers a time period dating back almost three years), and other pertinent factors. Yet to carry its burden here, the government must show that there is "good reason" to believe that Twitter's intended disclosures would harm national security, *John Doe, Inc. v. Mukasey*, 549 F.3d 861, 883 (2d Cir. 2008), *as modified* (Mar. 26, 2009), a belief that must be "well documented" rather than speculative, *Al-Haramain v. Bush*, 507 F.3d at 1203.

Indeed, Judge Illston recently observed that the government had "*not* shown that it is generally necessary to prohibit recipients from disclosing the mere fact of their receipt of NSLs." *In re Nat'l Sec. Letter*, 930 F. Supp. 2d 1064, 1076 (N.D. Cal. 2013). Judge Illston further suggested that—when disclosure could be shown to harm national security (for example, if the ECS "had only a handful of subscribers")—nondisclosure could be required on a case-by-case basis. *See id.* She accordingly struck down the pre-USA Freedom Act regime on the grounds that it did "nothing to account for the fact that when no such national security concerns exist, thousands of recipients of NSLs are nonetheless prohibited from speaking out about the mere fact of their receipt, rendering the statute impermissibly overbroad and not narrowly tailored." *Id.* On remand from the Ninth Circuit to consider the issues in light of the USA Freedom Act, Judge Illston found that nondisclosure was justified as to only three of the four NSLs at issue. *See In re: Nat'l Sec. Letters*, No. 11-CV-02173-SI, 2016 WL 4501210, at *18 (N.D. Cal. Mar. 29, 2016). That is, an individualized inquiry produced individualized, narrowly tailored results—and invalidated the restraint as to one individual NSL.

The government's restrictions here are plainly not the product of individualized inquiry or narrow tailoring. The government imposed a prior restraint on Twitter's speech, not based on an actual finding that permitting the speech would seriously damage national security, but because Twitter's proposed disclosure was more precise than the permissive band structure in the USA Freedom Act. Yet the Steinbach affidavit and the government's motion provide no specific, concrete basis to conclude that the bands in the Act are "narrowly tailored" to serving the national security interest. The government offers nothing to show why those bands accurately delimit the disclosures that would harm national security, for all providers and in all circumstances, and no matter how stale the disclosed information may be. (Any rationale the government may offer in the classified declaration simply underscores why, as explained below, Rule 56(d) and due process require that Twitter be permitted to probe the government's evidence, both classified and unclassified.) As a purported basis for a prior restraint, the bands are unconstitutional as applied to Twitter.

**2. On the Public Record, the Government Has Not Shouldered, Much Less Carried, Its Burden to Show That Its Restraint Is Narrowly Tailored to Avoid Serious Damage to National Security.**

The government's abstract references to a "mosaic" theory, *see, e.g.*, Steinbach Decl. ¶¶ 28, 30, cannot discharge its burden. It may be that "adversaries of the United States" may "piece[] together" a "mosaic of information" that "could allow them, for example, to better evade ongoing investigations and/or more effectively formulate or revise their counter-surveillance efforts." *Id.* ¶ 28. In the absence of detailed reasoning and specific, corroborating evidence showing precisely *why* Twitter's disclosure of more granular numerical data would harm national security, however, this contention proves far too much. The government could *always* say that the disclosure of new information would give foreign terrorists one more piece of the puzzle necessary to unlock the secrets of U.S. government surveillance. But that seemingly unlimited logic would permit the government to "operate in virtual secrecy in all matters dealing, even remotely, with 'national security,' resulting in a wholesale suspension of First Amendment rights." *Detroit Free Press v. Ashcroft*, 303 F.3d 681, 709–10 (6th Cir. 2002).

Nor does the evidence offered in support of the government's abstract "mosaic" theory withstand the reasonably "critical" scrutiny required by *Al-Haramain v. Bush*, 507 F.3d at 1203. For example, the government maintains that disclosing data about the number of national security process requests Twitter has received, if any, in "smaller bands would tend to reveal whether the government does or does not have a significant presence and investigative focus on communications occurring on a [specific] platform," thus signaling to terrorists which platforms are "more or less safe" for them to use. Steinbach Decl. ¶ 36. But, at least for large providers like Twitter, there is *already* sufficient information in the public sphere that the government has expressly permitted—presumably without harming national security—to allow judgments about which platforms are "safer" for clandestine communications. For example, a person can already glean from detailed, publicly available "Transparency Reports" that, from January to June 2015, between 16,000 to 16,500 Google accounts were subject to user content surveillance under FISA. *Google Transparency Report*, GOOGLE (last visited Dec. 7, 2016), https://www.google.com/transparencyreport/userdatarequests/US/. In the same time period, between 14,000 and 14,449 AT&T accounts were subject to national-security-related content monitoring, *Transparency Report*, AT&T (last visited Dec. 7, 2016), http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html, as were 1,500 to 1,999 Verizon accounts, *United States Report*, VERIZON (last visited Dec. 7, 2016), http://www.verizon.com/about/portal/transparency-report/us-report/. These reports also permit anyone to track changes in the number of accounts under surveillance over time: for Google, for example, a 30% increase in one reporting period. *See, e.g., Google Transparency Report* (showing an increase in accounts subject to requests for user content increased from 16,000 to 16,500 in January–June 2015, to 21,000 to 21,499 in July–December 2015). Adversaries could also glean the total number of subscribers or users on each platform listed above (112.1 million retail wireless users for Verizon and 128.640 million for AT&T as of the fourth quarter of 2015). *See* Verizon Commc'ns, Inc., Annual Report (Form 10-K) (Feb. 23, 2016); AT&T, Inc., Annual Report (Form 10-K) (Feb. 18, 2016).

Thus, by cross-referencing data from the Transparency Reports referenced above (which the government has permitted to be disseminated), with data in corporate annual and quarterly

reports, adversaries can assess their respective likelihood of being monitored on a given ECS platform. The government's motion and supporting declaration do not even begin to show why the information Twitter has sought to publish in its Draft Transparency Report would provide the enemy with any materially beneficial insights into U.S. counterintelligence that cannot be gleaned from the disclosure the government has already permitted.[8]

The government's related suggestion that slightly more granular numerical information would, as part of the "mosaic," reveal materially new information about the government's "capabilities" is also implausible on its face. It is public knowledge that the United States can serve national security surveillance requests on any ECS provider. And the relevant statutes set out exactly what kinds of information the government can obtain through NSL and FISA procedures. *See* 18 U.S.C. § 2709 (subscriber name, address, and billing records) (NSL); 50 U.S.C. §§ 1801, *et seq.* (same information, plus message contents) (FISA request). In short, the government has not established any meaningful nexus between the disclosure of slightly more granular, aggregate data about the total number of requests received and the government's capabilities—much less a reason to believe that Twitter's disclosure would cause "direct, immediate, and irreparable damage" to national security, *Pentagon Papers*, 403 U.S. at 730 (Stewart, J., concurring).

It might be that a report disclosing a specific amount of surveillance activity by a very small or new ECS provider could provide some useful information to the targets of that surveillance. Yet the government provides no public record evidence providing "good reason" to believe, *Mukasey*, 549 F.3d at 883, that any of the aggregate numerical data in the Twitter Draft Transparency Report would give rise to the kind of "tip off" concerns that may be present at the low end of the spectrum with small volume ECS providers.[9] Indeed, Twitter's Draft Transparency

[8] The government's evidence is largely irrelevant to the narrow tailoring question. There is no logical connection between the lurid examples of terrorists' use of ECS platforms, *see, e.g.*, Steinbach Decl. ¶ 33, and any increased threat to national security presented by the disclosures Twitter seeks to make here.

[9] It also might be different if the information at issue would reveal new and different surveillance capabilities—perhaps that a new medium was subject to surveillance. But the proposed numerical data here do not implicate that concern. In any event, the USA Freedom Act already addresses that issue by requiring ECS providers not previously subject to NSL or FISA requests to wait 540 days (rather than 180 days) before disclosing "information relating to such new order or directive." 50 U.S.C. § 1874(b)(1)(B).

Report discloses that it has approximately 240 million users (as of that six-month reporting period in 2013), and its more granular information could not possibly "tip off" anyone regarding the government's surveillance program or activities.

Nothing in the government's public filing suggests that the permissive statutory bands in the USA Freedom Act are narrowly tailored to restrain only speech that risks damage to national security, so that disclosure outside of the statutory bands is *per se* classified and may be restrained without further analysis. Indeed, the provision in 50 U.S.C. § 1874(c) authorizing other forms of disclosure suggests that Congress recognized that the bands are *not* narrowly tailored, and that some circumstances will warrant, or compel, more specific disclosures.

Most striking, the bands are inflexible and apply with equal force, regardless of the size of the ECS provider. To impose the same limits regardless of whether the provider has 240 or 240 million users (Twitter's reported number of users at the time of its Draft Transparency Report), the government would have to show that the threat presented by actual numbers remains the same regardless of the size of the provider. Yet the government has offered on the public record no "good reason" to believe that a disclosure of any granular number by an ECS with such a large user base like Twitter's would create any risk to national security.[10]

Nor does the statute reflect a particular threshold above which disclosure of actual numbers rather than bands would not harm national security. To establish that the bands are narrowly tailored to suppress no more speech than necessary, the government must show "good reason" to conclude that the threat posed by specific numbers is the same whether the total number of requests disclosed is 1 or 10,001. *Mukasey*, 549 F.3d at 883. And the government must demonstrate good reason to reach the related conclusions that, for example, a report that in successive six-month periods there were 1,672 and 2,112 requests harms national security in a way that disclosing a change from 1,500–1,999 to 2,000–2,499 requests does not.

[10] As part of its "mosaic theory," the government also alludes to a risk of more granular disclosure by other ECS providers, with each disclosure providing an "additional piece of the puzzle" for adversaries to exploit. See Steinbach Decl. ¶ 32. But the government has not even attempted to show that more granular reporting by other providers would contribute any material insights into the government's well-known capabilities to serve national security process. The risk that other providers in the future may seek to make more granular disclosures cannot relieve the government of its present burden to show that its restrictions on Twitter's speech are narrowly tailored.

The government's position is further undercut by the fact that ECS providers have been publishing actual numbers relating to their receipt of *criminal* process for years, *see* Transparency Reports, *supra*, at p.16. Yet the government has not attempted to classify that information, nor offered any evidence that such disclosures have thwarted domestic law enforcement efforts in a way that might justify more cryptic disclosures in the national security context.

Finally, the government must show that the duration of its restraint is narrowly tailored. The Act recognizes that national security permits the bands to narrow five- to ten-fold after a year has passed. *See* 50 U.S.C. § 1874. The government should have to show both that this increase in granularity would harm national security if it occurred earlier, and that any disclosure of exact numbers remains a national security threat even as to requests from two or more years in the past.

**3. The Pertinent History of Classification and Disclosure Underscores the Need for Thorough and Skeptical Scrutiny of the Restraints on a Complete Record.**

In addition to these evidentiary deficiencies, the history of declassification of previously classified documents provides reason for the Court to cast a "very careful, indeed a skeptical, eye" upon the government's judgment that it has struck a constitutional balance between national security and the First Amendment. *Al-Haramain v. Bush*, 507 F.3d at 1203. Due to litigation by ECS providers, President Obama's 2013 directive calling for greater transparency of government surveillance activities, and the passage of the USA Freedom Act, this Court has significantly more information at its disposal than courts had even five years ago. And that information shows that the government has consistently taken an overzealous position about the severity of the security threat posed by disclosures about the volume of its surveillance activities.

For example, the government maintains that all this recently declassified information continues to this day "to meet the classification requirements of Executive Order 13526 [setting forth the criteria for classification]." Steinbach Decl. ¶ 20.[11] At the same time, however, the government acknowledges that "exceptional circumstances [specifically, the "strong public interest in information," *id.* ¶ 15] . . . outweigh the need for [classification]." *Id.* ¶ 20. No wonder

[11] "Secret" or "Confidential" classification applies only to information posing a threat of "serious damage" or "damage to the national security," respectively. *Id.* § 1.2(a)(2),(3). And "[i]f there is significant doubt about the need to classify information, it shall not be classified." *Id.* § 1.1(b).

the Ninth Circuit requires courts to take a "skeptical" view of government justifications for restraints on speech in similar circumstances. *Al-Haramain v. Bush*, 507 F.3d at 1203. The government cannot have it both ways: If, as it claims, it would be justified in classifying the information that has been or could be disclosed under the DAG Letter and the USA Freedom Act, that would mean that the Attorney General, and Congress, were complicit in approving the disclosure of information that actually posed a danger to national security. Rather than make that assumption, the Court should draw the obvious inference that the classification was (and similar classifications remain) unconstitutionally overbroad.

For example, the government concedes that it previously classified its report summarizing the aggregate number of NSLs and FISA orders issued in 2013 as "Top Secret," reflecting an assessment that public disclosure was "expected to cause exceptionally grave damage to the national security." Steinbach Decl. ¶ 17. That report was declassified on June 23, 2014—within six months—and is now available to public. *Id.* So far as we can tell, the government has offered no evidence that "exceptionally grave damage" to national security has resulted from disclosure of that Report or similar since-declassified material. This disconnect between the government's prediction of grave harm to national security and reality suggests that the government's classification decisions were not narrowly tailored to its national security interest.

The DAG Letter reflecting the January 27th framework reflected a similarly swift reversal of position. After insisting that any disclosures of aggregate national security requests that did not include criminal process would harm national security, Steinbach Decl. ¶ 11, the government permitted ECS providers to report total NSLs received, total FISA content requests received, and total "customer selectors targeted under FISA content orders," if the data was disclosed in six-month periods and *in bands of 1,000*. *Id.*, Exh. 1, at 1. Only one year later, the USA Freedom Act declassified "additional data," *id.*, Exh. 2, permitting disclosure in narrower bands (of 100, 250, and 500), and of even more categories of national security process. *See* 50 U.S.C. § 1874(a).

The Court should scrutinize the government's current assertions in light of this pattern of recognition by Congress and the Executive alike that too much information about national security process has been withheld from the public.

**C. The Government Has Offered No Authority for Its Decision to Classify the *Absence* of Receipt of National Security Process**.

Even putting aside the other deficiencies in the government's classification analysis relating to aggregate data, it bears noting that the government has offered no authority whatsoever for its classification of the fact that an ECS platform has received *none* of a particular kind of national security process. Answer ¶ 6, ECF No. 120. As the government explains, the authority under which it purports to restrict Twitter's speech is Executive Order 13526, which requires, *inter alia*, that information sought to be classified be "owned by, produced by or for, or under the control of" the government. Exec. Order 13526, § 1.1(a)(2). The government asserts that national security process requests served upon Twitter are "owned by" and "produced by" the government because the government creates those documents, and "[t]hese materials . . . do not lose the characteristics of having been owned, produced by, and under control of the government" when they are served on private third parties. MSJ 16:17–19; 16:27–17:1.

Yet even if the government is correct that it owns the documents it creates, even after they leave its possession, under no theory does the government own the fact of its inaction. Ownership of documents provided no basis to classify the fact that a provider has *not* received any such documents—or a provider's accurate report of that fact. In other words, the government has failed to identify any authority that would confer upon it the power to classify the "zero." That is unsurprising; the notion that the government can classify the *absence* of a fact—an absence perceptible to private parties without any action by the government—would permit very broad restrictions on an entire category of speech.

**D. Resolution of This Unripe Motion Should Be Deferred Under Rule 56(d)**.

Under Rule 56(d), a motion for summary judgment should be denied or deferred as necessary to permit discovery when the nonmovant has been precluded from presenting "facts essential to justify its opposition." Deferral pending discovery is especially appropriate here because the premature resolution of the government's motion would short-circuit the procedural safeguards that the Constitution requires to "obviate the dangers of a censorship system." *Freedman*, 380 U.S. at 58. Under *Freedman*, in order to "avoid constitutional infirmity," a system of prior restraint must permit meaningful and independent judicial review, through an "adversary

proceeding," of the government's determination that a particular restraint is constitutional. *Id.* Yet the government here has sought at every turn to preempt any meaningful "adversary proceeding." The government now asks the Court to resolve this case before Twitter has an opportunity to test the government's proffered bases for its classification decisions.

Twitter has served document requests and interrogatories that expressly seek both unclassified and classified information from the government. The government's responses were due December 15, 2016; that period has been extended to December 22 at the government's request. In addition, Twitter has served a notice to take the deposition of Executive Assistant Director Michael Steinbach. Rubin Decl. ¶ 22, Exh. D. The government has informed Twitter that it plans to resist any discovery beyond the evidence that it is expressly relying on to support its motion, *see* Rubin Decl., ¶ 7, and its responses to Twitter's First Set of Interrogatories (served today) are consistent with the government's stated intention *See* Rubin Dec. ¶¶ 8–9, Exh. C.

There is no basis to preclude unclassified discovery from proceeding in this case. The government justifies its prior restraint on Twitter's speech by resting on its previous determination that disclosure outside of predetermined reporting bands would jeopardize national security. As far as the public record reflects, the government assumes rather than explains any "good reason," *Mukasey*, 549 F.3d at 883, for deciding that—for every provider and at every volume of requests—bands of 250 or 500 pose a lesser risk to national security than actual numbers (or narrower bands). Moreover, as explained above, the permissible reporting bands have changed over time, giving even more reason for skepticism of the government's position.

Twitter's discovery seeks to test the government's conclusory assertions in order to show that the current band framework—the basis for the government's redactions to Twitter's Draft Transparency Report—is not narrowly tailored to the government's compelling interest in protecting the nation's security. The discovery seeks highly relevant documents and information shedding light on the details surrounding the government's redactions of Twitter's Draft Transparency Report (including the identity of persons involved and the classification process undertaken at the time of the redactions), reasons for the government's various declassification decisions over time, the reasons for changes in the band reporting structure, the legislative and

executive materials that provide the basis for the current reporting bands, and the negotiation materials that led to the adoption of different reporting bands as part of a settlement of the 2013 FISA action. *See* Rubin Decl. ¶¶ 12–24.[12] This discovery is likely to develop facts that, at the least, establish a genuine factual dispute as to whether the government's restraints on Twitter's speech are constitutional. Rubin Decl. ¶ 24. Indeed, without this discovery, this Court cannot meaningfully review the government's assertions that restricting Twitter's speech is necessary to protect its national security interest.

Similarly, Twitter should be permitted to take the deposition of Mr. Steinbach, on whose testimony the government's motion principally relies. Twitter intends to examine Mr. Steinbach on the bases for the government's reliance on the statutory reporting bands in setting the boundary between permissible speech and that which would be reasonably expected to harm the nation. In light of the government's near-exclusive reliance on Mr. Steinbach's testimony, any grant of summary judgment without affording Twitter the opportunity to take his deposition would raise profound due process concerns. *Al Haramain v. Treasury*, 686 F.3d at 981; *Am.-Arab Anti-Discrimination Comm. v. Reno*, 70 F.3d 1045, 1060 (9th Cir. 1995) ("*ADC*").

**E. Due Process Requires that Twitter's Lead Counsel Be Permitted to Obtain the Clearance Necessary to Participate in Any Classified *In Camera* Proceedings.**

Due process also requires that Twitter's lead counsel be permitted to obtain the security clearance needed to participate in any *in camera* proceedings. As the Ninth Circuit has recognized, "*in camera* review ineluctably places the court in a role that runs contrary to our fundamental principle of a transparent judicial system." *Al-Haramain v. Bush*, 507 F.3d at 1203. *Ex parte* proceedings also lack the "adversary" character required in the First Amendment context to ensure the fair and robust representation of Twitter's (and the public's) interests. *Freedman*, 380 U.S. at 58. For these reasons, *ex parte* proceedings are "presumptively unconstitutional"—even in cases involving national security. *Al Haramain v. Treasury*, 686 F.3d at 981.

Indeed, the Ninth Circuit has held that—except in the "most extraordinary [of] circum-

[12] In its responses to Twitter's First Set of Interrogatories, the government refused to respond to a number of Twitter's requests solely on the grounds of relevance. *See* Rubin Decl. ¶_. Twitter believes these objections are unfounded, and, absent a negotiated resolution, intends to move to compel responses to these targeted discovery requests.

stances"—due process prohibits adjudication of the merits of a claim through *ex parte, in camera* proceedings. *ADC*, 70 F.3d at 1070. In *ADC*, the government urged a court to deny two aliens' legalization applications on the basis of classified documents—offered in *ex parte, in camera* proceedings—that related to the aliens' association with known terrorist organizations. *See id.* at 1067, 1069–70. Though the evidence implicated national security, the Ninth Circuit affirmed a judgment permanently enjoining the government from using the evidence outside of the adversarial process. *Id.* at 1071.

In so holding, the court specifically distinguished precedents permitting *in camera* review for the limited purpose of resolving issues *collateral* to the merits of a case—for example, the government's invocation of the "state secrets" privilege (as was the case in *Al Haramain v. Bush*, for example). *Id.* at 1070. The court conceded that, in "rare cases," a determination that a document is protected by the state secrets privilege could "operate[] as a complete shield to the government and result[] in the dismissal of a plaintiff's [tort] suit." *Id.* at 1070. But even when the *ex parte* proceedings indirectly resolve the merits of a claim, they do so only by making information "unavailable" for use by "either side." *Id.* The infringement on a party's due process right is therefore significantly *less* than in the "inherently unfair" setting where the government seeks simultaneously to rely on evidence to carry its *own* burden, while preventing its adversary from testing that evidence—thus presenting an "enormous risk of error." *Id.*

In *Al Haramain v. Treasury*, the Ninth Circuit addressed the question left open by *ADC*: In the "extraordinary circumstances" in which *some* use of *ex parte* proceedings is necessary to resolve a party's claims, what procedural safeguards does due process require? The Ninth Circuit concluded that, "[t]o the extent . . . helpful . . . and . . . feasible," due process requires (a) disclosure of relevant, unclassified material; and (b) that "the designated entity" be permitted to obtain "the appropriate security clearance" for its counsel. 686 F.3d at 983. That solution rested on the premise that "a lawyer for the designated entity who has the appropriate security clearance . . . does not implicate national security when viewing the classified material because, by definition, he or she has the appropriate security clearance." *Id.*

The court found the "value" of these procedures "undeniable": Without such safeguards,

"the designated entity cannot possibly know how to respond to [the government's] concerns," and "[w]ithout knowledge of a charge, even simple factual errors may go uncorrected despite potentially easy, ready, and persuasive explanations." *Id.* at 982.

Finally—contrary to the government's position in this litigation—the court held that the government *must* permit counsel for the opposing party to obtain the security clearance, unless *the government* can show how counsel's participation would itself harm national security or be unduly burdensome—a burden the government has not even attempted to overcome here. *Id.* at 983–84 (also suggesting that courts determine, on a "case-by-case" basis, other procedural safeguards—including declassification of information—that could "feasibl[y]" be employed to maintain an adversarial process when dealing with cases involving classified information).

*Al Haramain v. Treasury* forecloses the government's effort to avoid initiating the security clearance process needed to permit Twitter's lead counsel meaningfully "to respond to . . . concerns" raised in the *in camera* proceedings. 686 F.3d at 982. Following that procedure here is especially appropriate because this case addresses information classified under a mosaic theory, that Twitter employees who lack security clearances themselves assembled from the mere receipt of national security process. In support of its resistance to clearance here, the government relies on cherry-picked quotes from nonbinding and unpersuasive authorities from other circuits. *See* MSJ 19. As binding precedent makes clear, due process requires that Twitter have access to reasonable discovery including (through counsel with a security clearance) the classified information on which the government seeks to rely to restrain Twitter's speech or that otherwise directly bears on the government's proffered bases for its speech restrictions. Procedural "fairness" cannot be "obtained by secret, one-sided determinations of facts decisive of rights." *ADC*, 70 F.3d at 1069 (quoting *Anti-Fascist Comm. v. McGrath*, 341 U.S. 123, 170 (1951) (Frankfurter, J., concurring)) (rejecting government's assertion that its national security interest justified reliance on *ex parte, in camera* proceedings to resolve the merits of a case).

## CONCLUSION

The motion for summary judgment should be denied.

Dated: December 19, 2016

MAYER BROWN LLP

/s/ Lee H. Rubin

LEE H. RUBIN (SBN 141331)
lrubin@mayerbrown.com
DONALD M. FALK (SBN 150256)
dfalk@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

ANDREW JOHN PINCUS (*Pro Hac Vice*)
apincus@mayerbrown.com
1999 K Street, NW
Washington, DC 20006
Telephone: (202) 263-3220
Facsimile: (202) 263-3300

*Attorneys for Plaintiff Twitter, Inc.*