Brett Max Kaufman (Of Counsel)
brettmaxkaufman@nyu.edu
TECHNOLOGY LAW & POLICY CLINIC
NEW YORK UNIVERSITY SCHOOL OF LAW
245 Sullivan Street
New York, New York 10012
Telephone: 212-998-6430
Facsimile: 212-995-4031

Joseph C. Gratz (SBN 240676)
jgratz@durietangri.com
DURIE TANGRI LLP
217 Leidesdorff Street
San Francisco, CA 94111
Telephone: 415-362-6666
Facsimile: 415-236-6300

Attorneys for Amicus Curiae
Freedom of the Press Foundation

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

TWITTER, INC.,

Plaintiff,

v.

ERIC HOLDER,
Attorney General of the United States,

UNITED STATES DEPARTMENT OF JUSTICE,

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

FEDERAL BUREAU OF INVESTIGATION,

Defendants.

Case No. 4:14-cv-04480-YGR

BRIEF OF *AMICUS CURIAE* FREEDOM OF THE PRESS FOUNDATION IN SUPPORT OF PLAINTIFF'S OPPOSITION TO DEFENDANTS' PARTIAL MOTION TO DISMISS

Ctrm: 1 – 4th Floor
Judge: Honorable Yvonne Gonzalez Rogers

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

STATEMENT OF INTEREST OF AMICUS CURIAE*

The Freedom of the Press Foundation is a non-profit organization dedicated to helping support and defend public-interest journalism. Freedom of the Press Foundation advocates for transparency and accountability in an effort to preserve the rights guaranteed to the press under the First Amendment and strengthen the public's right to know. As part of that mission, the organization has served as *amicus curiae* in cases addressing First Amendment issues raised by emerging technologies and government surveillance in the federal courts. *See, e.g.*, *Elonis v. United States*, No. 13-983 (U.S. cert. granted June 16, 2014); *Under Seal v. Holder*, No. 13-16732 (9th Cir. argued Oct. 8, 2014); *United States v. Brown*, No. 12-cr-413 (N.D. Tex. judgment entered Jan. 29, 2015).

INTRODUCTION

In the 1970s, the Church Committee conducted a public and probing investigation of National Security Agency ("NSA") surveillance inside the United States that uncovered evidence of pervasive and unwarranted intrusions on Americans' personal privacy. These revelations sparked public outcry and led directly to changes in public policy. Based on information unearthed by the Church Committee, the American public moved their representatives to overhaul domestic intelligence collection and put firm limits on the NSA through the enactment of the Foreign Intelligence Surveillance Act ("FISA") in 1978.

Now, after eighteen months of new revelations published in some of the nation's largest newspapers, the public is currently engaged in the most robust and important debate about government surveillance in the United States since the Church Committee. Yet the government is stifling that debate, attempting to silence key voices—voices uniquely positioned to comment on and offer an informed perspective on the issue—in violation of the First Amendment. By refusing to allow technology companies used by millions of Americans, like Google, Facebook, and Twitter, to speak truthfully about the number and scope of national-security–surveillance requests they receive, the government has muted democratic debate on a matter of central importance to how Americans live their lives and exercise their constitutional rights. While the public is searching for an honest conversation about government

* The Freedom of the Press Foundation wishes to thank N.Y.U. Technology Law & Policy Clinic students Megan Briskman, Matthew W. Callahan, Megan Graham, and Rafael Reyneri for their invaluable contributions to this brief.

surveillance, the government is actively seeking to suppress that discussion and to limit access to knowledge that would create a more robust and informed debate.

Because of the uniquely dual role that technology companies play with respect to government surveillance—at once custodians of Americans' private data and recipients of government requests for that data—these companies have a critical perspective on the issue. Under the First Amendment, they are entitled to share it. For the reasons explained below, the government's restrictions on these technology companies are unconstitutional content-based regulations of speech and impose an unlawful prior restraint.

ARGUMENT

I. TRANSPARENCY REPORTING BY TECHNOLOGY COMPANIES ABOUT GOVERNMENT SURVEILLANCE ON U.S. NETWORKS IS OF PROFOUND IMPORTANCE TO THE AMERICAN PUBLIC AND ONGOING DEMOCRATIC DEBATE.

A. The American public is currently engaged in a robust democratic debate concerning the proper role, scope, and limits of government surveillance.

Since June 2013, a series of news reports and government disclosures has revealed to the American public the widespread nature of government surveillance programs and their intrusion into Americans' personal and private communications. Americans were shocked to discover the government's expansive (and still ongoing) bulk collection of telephony metadata, or phone records, from millions of Americans—an operation that was unprecedented in its scope and implicated virtually all Americans, yet remained secret for nearly twelve years. *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, Guardian, June 6, 2013, http://gu.com/p/3gc62. Further, under a government surveillance program called PRISM, online users' search history, file transfers, emails, photographs, documents, and live chat feeds are collected from major Internet providers if the users communicate with executive-branch–designated "targets"—potentially anyone "reasonably believed" to be a non-American outside of the United States. *See* Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, Guardian, June 7, 2013, http://gu.com/p/3gd58; *see also* Ewen MacAskill & Gabriel Dance, *NSA Files: Decoded–What the Revelations Mean for You*, Guardian, Nov. 1, 2013, http://gu.com/p/3k3ve; Barton Gellman et al., *In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are*, Wash. Post, July 5,

2014, http://wapo.st/1xyyGZF ("The daily lives of more than 10,000 account holders who were not targeted are catalogued and recorded nevertheless."). And under a related program called UPSTREAM, the government is "searching the contents of vast amounts of Americans' e-mail and text communications into and out of the country, hunting for people who mention information about foreigners under surveillance." Charlie Savage, *N.S.A. Said to Search Content of Messages to and From U.S.*, N.Y. Times, Aug. 8, 2013, http://nyti.ms/1L6Quji. Thus, even Americans who are not government targets themselves may still have the full contents of their communications swept up by the government. Under these programs, the government collects and retains extremely personal and sensitive information—including accounts of affairs, illness, and financial struggles, as well as a range of personal photographs from baby pictures to seductive photos—without permission from or even notice to the affected individuals. *See* Gellman et al., *supra*.

Each of these programs raises serious questions about whether the government is abiding by laws passed by Congress and the Fourth Amendment's protection from unwarranted searches and seizures as well as broader privacy values shared by the public. Furthermore, the near-blanket official secrecy surrounding the surveillance programs has sheltered the government from public scrutiny and is antithetical to the values underlying the First Amendment's guarantee of robust, truthful, and unhindered political debate. As the Founders recognized again and again, free speech and open debate are critical to a functioning democracy. *See* Benjamin Franklin, *On Freedom of Speech and the Press*, Penn. Gazette, Nov. 17, 1737 ("Freedom of speech is a principal pillar of a free government; when this support is taken away, the constitution of a free society is dissolved, and tyranny is erected on its ruins. Republics and limited monarchies derive their strength and vigor from a popular examination into the action of the magistrates."); *see also* Letter from James Madison to W.T. Barry (Aug. 4, 1822), *in* 9 *Writings of James Madison* 103 (G. Hunt ed. 1910) ("A popular Government, without popular information, or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or, perhaps both.").

Eighteen months after the still-developing surveillance disclosures began, the scope of Americans' personal privacy rights is unquestionably remains a source of ongoing democratic discourse and intense legislative debates over surveillance reforms. The initial revelations led to a sea change in the

public's opinion on the importance of online privacy,[1] multiple major lawsuits calling for more transparency and arguing constitutional violations,[2] and the introduction of more than a dozen bills in Congress that would increase the privacy rights of Americans.[3] In direct response to the revelations, the Obama Administration appointed a special review group to evaluate many aspects of government surveillance, resulting in an important report that was highly critical of many government surveillance operations and called for reforms.[4] In addition, the Privacy and Civil Liberties Oversight Board held a series of hearings, culminating in a comprehensive unclassified report on the government's expansive collection of telephone records of millions of Americans under Section 215 of the Patriot Act that aimed to enable "the public and the Congress [to] have a long overdue debate about the privacy issues raised" by the Snowden disclosures.[5] The legislative debate over surveillance reform has largely centered on the USA Freedom Act, a bill that would reform the government's ability to conduct Internet and phone surveillance and establish rules governing transparency and reporting to the public and to Congress.[6]

---

[1] *See* Glenn Greenwald, *Major Opinion Shifts, in the US and Congress, on NSA Surveillance and Privacy*, Guardian, July 23, 2013, http://gu.com/p/3hjef.

[2] *See* Kara Brandeisky, *NSA Surveillance Lawsuit Tracker*, ProPublica, July 10, 2013 (last updated Feb. 27, 2014), http://projects.propublica.org/graphics/surveillance-suits.

[3] *See* Michelle Richardson & Robyn Greene, *NSA Legislation Since the Leaks Began*, ACLU Blog of Rights (Aug. 15, 2013, 10:48 A.M.), https://www.aclu.org/blog/national-security/nsa-legislation-leaks-began.

[4] *See* President's Review Grp. on Intelligence & Commc'ns Techs., *Liberty and Security in a Changing World: Report and Recommendations* (2014), http://1.usa.gov/1cBct0k; *see also* Ellen Nakashima & Ashkan Soltani, *NSA Shouldn't Keep Phone Database, Review Board Recommends*, Wash. Post, Dec. 18, 2013, http://wapo.st/1eoK98i.

[5] *See* Privacy & Civil Liberties Oversight Bd., *Report on the Telephone Records Program Conducted Under Section 215 of the USA Patriot Act and on the Operations of the Foreign Intelligence Surveillance Court* 1 (2014), http://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf; *see also* Privacy & Civil Liberties Oversight Bd., *Recommendations Assessment Report* 4 (2015), http://www.pclob.gov/library/Recommendations_Assessment-Report.pdf (noting that the Obama Administration failed to end the bulk telephone records program that the PCLOB recommended over a year ago, despite having the authority to do so without congressional action); Privacy & Civil Liberties Oversight Bd., *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (2014), http://www.pclob.gov/library/702-Report.pdf.

[6] This debate began almost immediately after the Snowden disclosures began in June 2013, and it has increased in intensity over the past year. *See* Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act (USA Freedom Act), H.R. 3361, 113th Cong. (2014); *see also* Tom Risen, *Obama Weighs NSA Options as Deadline Nears*, U.S. News & World Rep., Jan. 26, 2015, http://t.usnews.com/Z677e3 (stating that the bill is likely to be reintroduced in the coming months); Adi Roberston & Nathan Ingraham, *USA Freedom Act for NSA Reform is Voted Down in the Senate*, The Verge (Nov. 18, 2014, 8:29 PM), http://theverge.com/e/7006008 (explaining the bill failed to pass the Senate's sixty-vote cloture rule by only two votes); Ellen Nakashima & Andrea

While that bill stalled in the Senate in the last session of Congress, the legislative debate over the NSA's surveillance programs is far from over: without legislative action re-authorizing the government's surveillance programs, Section 215—the law that the Foreign Intelligence Surveillance Court ("FISC") has held authorizes the government to collect phone data from virtually all Americans—will expire on June 1, 2015. *See* Spencer Ackerman, *Failure to Pass US Surveillance Reform Bill Could Still Curtail NSA Powers*, Guardian, Oct. 3, 2014, http://gu.com/p/42669. As a result, both the executive branch and Congress continue to debate legislative measures centered on surveillance reform. *See, e.g.*, Office of the Dir. of Nat'l Intelligence, *ODNI General Counsel Robert Litt Speaks on Intelligence Surveillance Reform at the Brookings Institute*, IC on the Record (Feb. 4, 2015), http://icontherecord.tumblr.com/post/110099240063/video-odni-general-counsel-robert-litt-speaks-on; Risen, *supra* note 6.

The government has attempted to shape the debate in many ways. The NSA itself has been an active participant in the public discussion, with agency officials appearing before Congress, establishing a public-facing platform to house declassified documents and public communications from the agency, and issuing various reports discussing some of the general rules surrounding the agency's signals intelligence activities. *See* Office of the Dir. of Nat'l Intelligence, *Declassified*, IC on the Record, http://icontherecord.tumblr.com/tagged/declassified; Office of the Dir. of Nat'l Intelligence, *Signals Intelligence Reform 2015 Anniversary Report*, IC on the Record (2015), http://icontherecord.tumblr.com/ppd-28/2015/overview. Yet the release of information by the government has been decidedly one-sided in its point of view, creating a deliberately opaque and misleading picture of how Americans are affected by government surveillance. Many details about the true scale of the government surveillance remain secret, and the government is actively seeking to prevent technology companies from explaining these important details to the public.

Peterson, *House Votes to Curb NSA 'Backdoor' U.S. Data Searches*, Wash. Post, June 20, 2014, http://wapo.st/1jEkcPa (discussing passage of a House bill to curb NSA's ability to conduct warrantless searches of databases for Americans' communications records).

B. Technology companies must be key participants in the ongoing debate about government surveillance in the United States in order to ensure that the public is adequately informed.

Because of their dual roles as custodians of the private data of the American public and as necessary actors in the execution of many government surveillance requests, American technology companies have a critical role to play in informing the public about government surveillance practices. Technology companies are gatekeepers of their users' personal information, putting them in the best position to offer an educated perspective on the government's activities. *See* Pl.'s Opp'n to Partial Mot. to Dismiss 20. Without information from providers, the secrecy provisions of FISA, the FISA Amendments Act, and national-security letters ("NSLs") make it nearly impossible for the American public to learn from independent parties about the scope and scale of government surveillance. Although many technology companies want to share information with the public, they are often prevented from communicating this information. Many of the government's individual requests contain gag orders that not only block disclosure to the target or targets of the surveillance, but also prevent the companies from telling the public that they received any surveillance request at all. *See, e.g.*, 18 U.S.C. § 2709(c). To be sure, secrecy over individual process is necessary to the operation of foreign-intelligence surveillance. But because providers interact with the government over the long term, they can offer the public a well-informed perspective on the aggregate scope and uses of government surveillance without endangering individual investigations. Moreover, companies that observe government surveillance requests over time are better situated to comment on trends concerning the breadth and character of those requests than any party other than the government, meaning they can offer compelling responses to government narratives. *Compare* Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, Wash. Post, June 7, 2013, http://wapo.st/1888aNq (quoting government documents as saying the government can collect data "directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple"), *with* Larry Page, *What the . . .?*, Google Official Blog (June 7, 2013), http://googleblog.blogspot.com/2013/06/what.html (stating that Google has "not joined any program that would give the U.S. government—or any other government—direct access to [their] servers"). Thus, companies can illuminate the public debate by contributing a meaningful and accurate picture of such

surveillance, empowering members of the public to make their own informed decisions about which services they wish to use and how to engage effectively in public discourse concerning potential reforms of government surveillance programs.

Many companies have sought to fill the public-information gap by issuing "transparency reports" that contain aggregate information concerning government requests. Knowing how important government surveillance has become to the public, companies have invested in transparency reports as a way to build the trust of their users and to demonstrate that they take consumers' privacy seriously.[7] The importance that the public has placed on these transparency reports is reflected in the increasing resources companies are pouring into their reports: Where transparency reports were once a rarity from tech companies, since the revelations started eighteen months ago, virtually every major company has publicly committed to releasing transparency reports every six months. Companies now dedicate their own blog sites to reflect on the data that include easy-to-understand charts and interactive features, and are actively competing with each other to provide users with as complete picture as possible concerning how they handle government requests.[8]

The public has received these new efforts at transparency with great enthusiasm. *See* Rainey Reitman, *7 Things to Love About reddit's First Transparency Report*, Electronic Frontier Found. DeepLinks Blog (Feb. 2, 2015), https://www.eff.org/deeplinks/2015/02/7-things-love-about-reddits-first-

[7] *See, e.g.*, Yahoo, *Users First, in Yahoo Transparency Report*, https://transparency.yahoo.com/users-first/index.htm ("Our users place their trust in us and, we take seriously their privacy and our role in promoting freedom of expression. Our commitment to and concern for your privacy, security, and freedom are demonstrated in our users first approach to government activities."); AT&T, Inc., *Transparency Report for 2013*, at 2 (2014), http://soc.att.com/1xwzU57 ("Interest in this topic has increased in the last year. . . . We're committed to providing you with as much transparency and accuracy in this reporting as is possible."); Richard Salgado, *Shedding Some Light on Foreign Intelligence Surveillance Act (FISA) Requests*, Google Official Blog (Feb. 3, 2014), http://googleblog.blogspot.com/2014/02/shedding-some-light-on-foreign.html ("[W]e still believe more transparency is needed so everyone can better understand how surveillance laws work and decide whether or not they serve the public interest.").

[8] *See* Trevor Callaghan, *Transparency Report: New Numbers and a New Look for Government Requests*, Google (Dec. 22, 2014), http://googlepublicpolicy.blogspot.com/2014/12/transparency-report-new-numbers-and-new.html (explaining that Google invested in its transparency report by hiring a digital company to improve the interactive quality of the report to make the information more meaningful to its users); Twitter, *Twitter Transparency Report: Information Requests from January to June 2014* (2015), https://transparency.twitter.com/information-requests/2014/jan-jun (dedicating a third of the website to Twitter's policy for responding to government requests with charts breaking down the location of user's who have been targeted by the government).

transparency-report; Levi Sumagaysay, *EFF 'Who Has Your Back' Report Standouts, for Better or Worse: Apple, Yahoo, Amazon, Snapchat* (May 16, 2014, 11:27 AM), http://www.siliconbeat.com/2014/05/16/eff-who-has-your-back-report-standouts-for-better-or-worse-apple-yahoo-amazon-snapchat. Moreover, in response to the increasing popularity of transparency reports, various collaborative efforts have emerged to help consumers track how various companies treat consumers data, respond to law-enforcement requests, and monitor a company's transparency report for any meaningful changes. *See, e.g.*, Taier Perlman & Peter Micek, *Disclose All the Things! Access Launches Transparency Reporting Index*, AccessNow (Nov. 19, 2014, 1:37 PM), https://www.accessnow.org/blog/2014/11/19/disclose-all-the-things-access-launches-transparency-reporting-index; Electronic Frontier Found., *Who Has Your Back?*, https://www.eff.org/who-has-your-back-2014. The mere existence of these types of projects illustrates the public's demonstrated interest in more—and more accurate—information about government surveillance on the networks of American technology companies.

Yet these transparency reports all contain a gaping hole: companies are not allowed to fully inform their users about national-security–surveillance requests, despite that the fact that the concern over national-security surveillance is what sparked the public's interest in transparency reports in the first place. The result is a skewed public picture that allows the government to hide the full scope of its activities at the same time the national debate over surveillance is taking place.

C. The government has consistently frustrated technology companies' efforts to join and participate in the ongoing public debate.

The government's regulation of the information that technology companies can share with the public has significantly handicapped the terms of the public debate. Beginning in June 2013, in response to ambiguities in news reporting on various NSA surveillance efforts, technology companies sought to set the public record straight regarding the nature and frequency of the information about—and of—their users that they provide to the government. *See* Cecilia Kang, *U.S. Sought Data, Tech Firms Say*, Wash. Post, June 14, 2013, http://wapo.st/145Tb0k (quoting Facebook general counsel Ted Ullyot as writing, "In light of continued confusion and inaccurate reporting related to [government surveillance], we've advocated for the ability to say even more"). As part of these efforts, on June 18, 2013, Google filed suit in the FISC for a declaratory judgment that it could publish new information on law enforcement process

in its transparency report. *See* Mot. for Declaratory J. of Google Inc.'s First Amendment Right to Publish Aggregate Information About FISA Orders 1 (FISC June 18, 2013), http://1.usa.gov/172ZBFb ("Google FISC Mot."). Historically, the government refused to allow companies to break down the number of FISA government requests that they received as a category distinct from other law-enforcement process. *See* Kang, *supra*. In the FISC, Google argued that their "reputation and business has been harmed" by misleading reports of collusion with the government. Google FISC Mot. 3. Ultimately, Microsoft, Yahoo, Facebook, and LinkedIn filed similar lawsuits in the FISC, leading to a consolidated action that, six months later, resulted in a private settlement of the pending actions. *See* Letter from Deputy Att'y Gen. James M. Cole to General Counsels (Jan. 27, 2014) ("DAG Letter"), http://1.usa.gov/1IuJYqL. Under a framework established by the DAG Letter, technology companies can report the numbers of NSLs, several forms of FISA requests, and customer accounts affected by the requests as separate categories only in bands of one thousand, starting with 0–999. *See id.* at 2. In addition, providers are barred from publishing information on a "new capability order" (i.e., the first order of a given type that a provider receives) for two years after its receipt. *Id.* at 3. As an alternative, the DAG Letter allows companies to report two lump sums in bands of 250 requests, starting with 0–249: the total of all forms of national-security process, and the total number of user accounts affected. *Id.*

While the DAG Letter resulted from the settlement of private lawsuits, the government has indicated that the reporting framework it established applies to all "similarly situated" technology companies. Compl. ¶ 29. Troublingly, the government has taken the position that even companies—including Twitter—that have received *zero* of a certain type of national-security process may not publicly reveal that fact, even though they would be under no existing secrecy obligations attendant to individual processes and were not parties to the FISC suit. *See* Compl. ¶ 5; Pl.'s Opp'n to Partial Mot. to Dismiss 2. And many companies have publicly maintained that the bands arrived at in the DAG Letter are too wide to convey meaningful information to the public. *See* Salgado, *supra* note 5 ("Publishing these numbers is a step in the right direction. . . . But we still believe more transparency is needed so everyone can better understand how surveillance laws work and decide whether or not they serve the public interest."); Brad Smith, *Unfinished Business on Government Surveillance Reform* (June 4, 2014), http://blogs.microsoft.com/on-the-issues/2014/06/04/unfinished-business-on-government-surveillance-

reform ("It was a good step, but we believe even more detail can be provided without undermining national security."). When companies have attempted to report number of national-security requests they have received outside the parameters of the DAG Letter, the government has continued, in at least some instances, to stifle their ability to join the public debate on the topic. *See, e.g.*, Compl. ¶ 3. By preventing companies from communicating with their customers about the prevalence of government surveillance over a company's data in a meaningful way, the government continues to manipulate the public narrative and frustrate companies' efforts to engage in public discourse.

II. THE GOVERNMENT'S CONTENT-BASED RESTRICTIONS ON TWITTER'S SPEECH ON MATTERS OF CORE PUBLIC CONCERN FAIL STRICT SCRUTINY.

A. The proper role, scope, and limits of government surveillance are matters of core public concern.

One of the foundational, animating purposes of the First Amendment is to ensure that the public is well informed about the functioning of its government. *See, e.g.*, *Mills v. Alabama*, 384 U.S. 214, 218 (1966) ("[T]here is practically universal agreement that a major purpose of [the First] Amendment was to protect the free discussion of governmental affairs."); *see also, e.g.*, *Gentile v. State Bar of Nev.*, 501 U.S. 1030, 1034 (1991) ("There is no question that speech critical of the exercise of the State's power lies at the very center of the First Amendment."). As a result, the judicial branch has zealously guarded the right of the people to gather and hear truthful information about matters of core public concern. *See, e.g.*, *Thornhill v. Alabama*, 310 U.S. 88, 101–02 (1940) ("The freedom of speech and of the press guaranteed by the Constitution embraces at the least the liberty to discuss publicly and truthfully all matters of public concern without previous restraint or fear of subsequent punishment."). Given the expansive scope and invasive nature of government surveillance programs that implicate the privacy rights of virtually all Americans, information pertaining to government surveillance naturally qualifies as a matter of profound importance to the public and warrants protection under the First Amendment. *See, e.g.*, *Connick v. Myers*, 461 U.S. 138, 145 (1983) ("'[S]peech concerning public affairs is more than self-expression; it is the essence of self-government.'" (quoting *Garrison v. Louisiana*, 379 U.S. 64, 74–75 (1964))); *McKinley v. City of Eloy*, 705 F.2d 1110, 1114 (9th Cir. 1983) (explaining that allowing the public "to make informed decisions about the operation of their government merits the highest degree of first amendment protection").

B. The government's restrictions on sharing information about national-security process with the public are content-based.

In this case, Twitter has alleged unlawful government restrictions on its speech of several stripes, all of which flow from the "terms of government-approved speech" contained in the DAG Letter. Pl.'s Opp'n to Partial Mot. to Dismiss 1. First, the transparency-reporting bands mandated by the DAG Letter prohibit "Twitter's ability to say 'zero,' that is, to truthfully deny receipt of *any* national security legal process, or specific *kinds* of national security legal process." *Id.* (This is the "zero" rule.) Second, the reporting bands are so large as to impede meaningful, truthful speech about the scale of government surveillance requests. (This is the "bands" rule.) And third, the government has taken the position that "similarly situated" companies, including Twitter, must pre-clear transparency reports that do not comply with the rules set out in the DAG Letter with the government before speaking publicly about national-security process the companies (do or do not) receive. *See id.* at 17. (This is the "clearance" rule.) All of these restrictions are content-based and therefore subject to strict scrutiny.

Under the First Amendment, "[a]s a general matter, [the] government has no power to restrict expression because of its message, its ideas, its subject matter, or its content." *Brown v. Entm't Merchs. Ass'n*, 131 S. Ct. 2729, 2733 (2011) (ellipsis omitted) (quoting *Ashcroft v. Am. Civil Liberties Union*, 535 U.S. 564, 573 (2002)). Once it is determined that a restriction is content-based, it must survive strict scrutiny. *See, e.g.*, *McCullen v. Coakley*, 134 S. Ct. 2518, 2530 (2014); *Pleasant Grove City v. Summum*, 555 U.S. 460, 469 (2009) ("[A]ny restriction based on the content of the speech must satisfy strict scrutiny, that is, the restriction must be narrowly tailored to serve a compelling government interest . . . ."). Moreover, a content-based regulation is "presumptively invalid" under the First Amendment, and it can only be saved if the government can show that its regulation is the "least restrictive means of furthering a compelling government interest." *Am. Civil Liberties Union of Nev. v. City of Las Vegas*, 466 F.3d 784, 792 (9th Cir. 2006).

The Supreme Court has explained that a court's "principal inquiry in determining content neutrality . . . is whether the government has adopted a regulation of speech because of disagreement with the message it conveys." *Ward v. Rock Against Racism*, 491 U.S. 781, 791 (1989) (citation omitted); *accord Madsen v. Women's Health Ctr., Inc.*, 512 U.S. 753, 763 (1994). The "threshold consideration" is

thus "the government's purpose" in regulating the speech. *Madsen*, 512 U.S. at 763. A restriction on speech is "content based if it require[s] enforcement authorities to examine the content of the message that is conveyed to determine whether a violation has occurred." *McCullen*, 134 S. Ct. at 2531 (quotation marks omitted) (quoting *FCC v. League of Women Voters*, 468 U.S. 364, 383 (1984)); *see City of Renton v. Playtime Theatres, Inc.*, 475 U.S. 41, 48 (1986).

Because all of the government's restrictions on Twitter are based on what Twitter's transparency report says, the restrictions are patently content-based. *See Doe, Inc. v. Mukasey*, 549 F.3d 861, 877 (2d Cir. 2008) (acknowledging that while gag orders associated with NSLs are not "typical content-based restriction[s]," they are content-based nonetheless). The government's rules over service-provider speech at issue here are specifically aimed at speakers looking to reveal a specific type of information—truthful, aggregate information about government surveillance requests. In other words, the government's restrictions burden speech "because of disagreement with the message it conveys," *Ward*, 491 U.S. at 791 (citation omitted), and they are therefore classic content-based restrictions. *See* Geoffrey R. Stone, *Content-Neutral Restrictions*, 54 U. Chi. L. Rev. 46, 47 (1987) ("Content-based restrictions limit communication because of the message it conveys. Laws that prohibit seditious libel, *ban the publication of confidential information*, forbid the hiring of teachers who advocate violent overthrow of the government, or outlaw the display of the swastika in certain neighborhoods are examples of content-based restrictions." (emphasis added)). Because the information that Twitter may share under the government's rules "depend[s] on whether [it] depict[s]" specified information, *United States v. Stevens*, 559 U.S. 460, 468 (2010)—i.e., "zero" requests or narrower bands than approved by the DAG Letter—the government's restrictions operate as content-based restrictions on Twitter's speech.

C. The government's restrictions on speech are not narrowly tailored to serve a compelling interest.

The restraints placed by the government on Twitter's ability to speak can only be deemed constitutional if they survive strict scrutiny, which requires that they be narrowly tailored to serve a compelling government interest. *United States v. Playboy*, 529 US 803, 813 (2000). The government cannot meet this burden here.

While national security in general, and the protection of national-security information, are admittedly compelling interests, none of the government restrictions at issue in this case are narrowly tailored to those interests. As a result, those restrictions needlessly and unconstitutionally inhibit transparency and prohibit the public from hearing speech—the reporting of "zero" or more meaningful reporting bands—that is uniquely relevant to a roiling public debate.

First, the government's restrictions on aggregate reporting are not narrowly tailored to an interest in protecting specific national-security investigations. At least in theory, the nondisclosure obligations imposed by NSLs and FISA orders serve a more concrete interest—to avoid prematurely alerting a surveillance target that his communications have been searched and thereby thwart an actual (and often covert) investigation. *See, e.g.*, 50 U.S.C. § 1805(c)(2)(B) (requiring recipients of FISA orders to 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*" (emphasis added)). But the release of purely historical, aggregate information about government surveillance requests (the "bands" rule)—including, and especially, historical information about the *absence* of particular types of government surveillance requests (the "zero" rule)—does not pose any threat to that government interest.

Second, the government's restrictions are not narrowly tailored to its more general interest in conducting lawful electronic surveillance with the cooperation of communications providers. There is nothing unique about *any* U.S.-based technology company that places it beyond the reach of the U.S. government's legitimate and lawful legal process—and this fact is not a state secret. Like other providers, Twitter has an interest in complying with legitimate national-security–related requests for information. *See* Pl.'s Opp'n to Partial Mot. to Dismiss 26. If a particular provider has not yet received a certain kind of surveillance request, that circumstance is either a mere coincidence or the result of the fact that its platform is not conducive to private communications of the sort presumably necessary for coordinating criminal acts. *See* Compl. ¶ 7 (explaining how "Tweets" are public by default and broadcast to the entire world).

The government has nowhere explained—and it cannot explain—why more detailed reporting bands than those allowed in the DAG Letter (under the "bands" rule) would in any way jeopardize its interest in issuing national-security process to communications providers and receiving their cooperation.

The government must not only make such a showing, it must show that the restrictions in the DAG Letter are the "least restrictive means" of protecting national-security information. *See Am. Civil Liberties Union of Nev.*, 466 F.3d at 792 (quoting *S.O.C., Inc. v. Cnty. of Clark*, 152 F.3d 1136, 1145 (9th Cir. 1998)). Here, the government's choice to require bands of 1000 is entirely untethered to a justification explaining its relevance, importance, or logic. Certainly, the government has not anywhere made a public case—let alone a compelling one—that bands of 1000 constitute the "least restrictive means" of protecting national-security information. Almost uniformly, technology companies—even those that have signed the DAG Letter—believe that more transparency is required in this debate. *See* Salgado, *supra* note 7 ("Publishing these numbers is a step in the right direction. . . . But we still believe more transparency is needed so everyone can better understand how surveillance laws work and decide whether or not they serve the public interest."); Smith, *supra* ("It was a good step, but we believe even more detail can be provided without undermining national security.").

Nor has the government explained why public discussion of the fact that *in the past*—as opposed to *at present*, or *in the future*—a company has not received a particular type of request (the "zero" rule) would incentivize or protect would-be criminals, or impede investigations of them, to the detriment of the government's general surveillance interest. There is no reason to believe that a provider's transparency report that includes "zero" will incentivize would-be criminals to use its services instead of another's, to evade future surveillance, or to otherwise interfere with the government's ability to surveil the electronic communications of national-security targets. Even those companies that have reported having received zero of certain kinds of surveillance requests still comply with other kinds of government orders and requests.[9] *See, e.g.*, reddit, *reddit Transparency Report, 2014* (2015), https://www.reddit.com/wiki/transparency/2014 (disclosing the fact that reddit has never received an NSL while explaining how it complies with other U.S. legal process). Many service providers who have chosen to report "zero" have, at the same time, explicitly made clear that they will dutifully comply with

[9] Certain companies have published transparency reports including "zero" without submitting those reports to the government for approval.

valid future legal orders requesting their users' data or communications.[10] All the "zero" rule accomplishes is the stifling of legitimate provider efforts to participate in an ongoing public debate of great importance. *See* Ellen Nakashima, *Tech Firms Tussle with DOJ over the Right to Say 'Zero'*, Wash. Post, Dec. 16, 2014, http://wapo.st/139Wus3.

D. The government's clearance rule smacks of viewpoint discrimination, which is always disfavored under the First Amendment.

The restrictions in the DAG Letter also point toward an intentional muzzling of a particular viewpoint—that of the service providers who are seeking to join the public debate. By itself disclosing select surveillance data and preventing service providers from doing the same, the government appears to be attempting to enforce a monopoly over the distribution of information about the number of national-security requests made and the processes by which they occur. The government should not be able to use an overly broad category of national-security classification as a tool to pick and choose who is free to discuss important public-policy issues, and thereby avoid public scrutiny. Such discrimination is always disfavored under the First Amendment, and given its specter in this case, the Court should rigorously apply its strict-scrutiny analysis to ensure that the government's regulations are not motivated by a desire to censor an opposing viewpoint.

The Supreme Court has cautioned that "[i]n the ordinary case it is all but dispositive to conclude that a law is content-based and, in practice, viewpoint-discriminatory." *Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653, 2667 (2011). In this case, there is at least circumstantial evidence that the government is seeking to exclude particular voices from the national conversation about the government's surveillance practices and the national-security requests made of private companies. *See supra* Part I.C.; *cf., e.g.*, *Citizens United v. Fed. Election Comm'n*, 558 U.S. 310, 340 (2010) (stating that the First Amendment is "[p]remised on mistrust of governmental power" and that it is designed to "stand[] against attempts to disfavor certain subjects or viewpoints" from participating in public discourse); *First Nat'l Bank of Bos.*

[10] *See, e.g.*, Pinterest.com, *Our First Transparency Report* (Mar. 3, 2014), http://blog.pinterest.com/post/78882077135/our-first-transparency-report ("Every company that stores information . . . must respond to requests for that information. . . ."); Tumblr, *Tumblr Transparency Report 2013* (2014), https://secure.static.tumblr.com/ahtwo23/FWmn94n2t/transparencyreport2013_letter__5.pdf (detailing the processes it uses to comply with legal government requests for user information).

v. Bellotti, 435 U.S. 765, 777 (1978) (stating that when speech is "indispensible to decisionmaking in a democracy," the "inherent worth of the speech in terms of its capacity for informing the public does not depend upon the identity of its source"). And courts frequently look to the surrounding facts and context of a government restriction on speech to determine if the restriction discriminates based on viewpoint. *See, e.g.*, *Brown v. Cal. Dep't of Transp.*, 321 F.3d 1217, 1223–25 (9th Cir. 2003) (examining the broader context of a regulation and determining that the policy of only allowing particular flags to be flown on highway overpasses constituted viewpoint discrimination).

As discussed above, the DAG Letter instructs companies that they may not report the specific number of a particular form of national-security process. *See* DAG Letter at 2–3. On the other hand, the government issues a public annual report detailing the specific numbers of each form of process it collectively serves on those same providers. *See, e.g.*, Letter from Peter J. Kadzik, Principal Deputy Asst. Att'y Gen. to Hon. Joseph R. Biden, President of U.S. Senate, at 1–2 (Apr. 30, 2014), http://1.usa.gov/16Sw5ln (listing specific numbers of various forms of national-security process served in previous year). By muzzling certain speakers who have specific insights and factual information into how government surveillance operates, the government appears to be attempting to control the public debate about the type and scale of national-security requests it hands out. *See, e.g.*, Ewen MacAskill, *NSA Paid Millions to Cover Prism Compliance Costs for Tech Companies*, Guardian, Aug. 23, 2013, http://gu.com/p/3t92a (quoting Google as requesting the ability to publish more data so it could show that its "compliance with American national security laws falls far short of the wild claims still being made in the press today"); *cf. Waters v. Churchill*, 511 U.S. 661, 674 (1994) (stating that public employees often have special knowledge about the functioning of government and that "public debate may gain much from their informed opinions"); *Wright v. FBI*, Nos. 02–915, 03–226, 2006 WL 2587630, at *7 (D.D.C. July 31, 2006) (emphasizing how views of "knowledgeable, informed, experienced 'insiders' are of particular utility," especially when they comment on issues, like the FBI's counter-terrorism practices, where there is a lack of open public discourse). This Court should be particularly skeptical of the government's restrictions on speech where they amount to enforcement of a one-sided debate. *See, e.g.*, *McCullen*, 134 S. Ct. at 2533 (explaining that courts must pay special attention to First Amendment concerns when selective regulation of speech "'may represent a governmental attempt to give one side of

a debatable public question an advantage in expressing its views to the people'" (quoting *City of Ladue v. Gilleo*, 512 U.S. 43, 51 (1994))); *Citizens United*, 558 U.S. at 340 ("Speech restrictions based on the identity of the speaker are all too often simply a means to control content.").

III. THE GOVERNMENT'S RESTRICTION ON THE PUBLICATION OF TWITTER'S TRANSPARENCY REPORT IS AN UNCONSTITUTIONAL PRIOR RESTRAINT ON CORE POLITICAL SPEECH.

The Supreme Court has consistently held that prior restraints are not only strongly disfavored, but are the "most serious and the least tolerable infringement on First Amendment rights." *Neb. Press Ass'n v. Stuart*, 427 U.S. 539, 559 (1976). As the Court has explained, a prior restraint "has an immediate and irreversible sanction," and "[i]f it can be said that a threat of . . . sanctions after publication 'chills' speech, [a] prior restraint 'freezes' it at least for the time." *Id.* As a result, "[a]ny prior restraint on expression comes . . . with a heavy presumption against its constitutional validity." *Org. for a Better Austin v. Keefe*, 402 U.S. 415, 419 (1971) (quotation marks and citation omitted).

Here, a series of circumstances imposed by the government—principally, the "clearance" rule—are operating as a prior restraint preventing Twitter from publishing its transparency report and from presenting the information it wishes to communicate to the public. Because these restrictions prevent Twitter from speaking in the first instance rather than imposing a penalty after engaging in its desired speech, the restrictions amount to a prior restraint. *See Alexander v. United States*, 509 U.S. 544, 550 (1993). Prior restraints come in two main forms: direct prohibitions on or prior injunctions against publication, and restrictions that act "in operation and effect like a licensing scheme . . . ." *Smith v. Daily Mail Pub. Co.*, 443 U.S. 97, 101 (1979) (quotation marks and citations omitted). This case concerns the latter.[11] The DAG Letter and the accompanying notice to the FISC purport to set the terms by which companies can disclose the numbers of national-security requests they have received. *See* Notice, Compl. Ex. 2, *available at* http://1.usa.gov/1aEx6hD ("It is the Government's position that the terms outlined in the [DAG Letter] define the limits of permissible reporting for the parties and other similarly situated companies."); DAG Letter, *supra*. The language in these documents operates as a prior restraint;

[11] *Amicus* does not contend that the DAG Letter, in and of itself, acts as a prior restraint in general terms or with respect to members of the general public. Rather, it is that the DAG Letter, in conjunction with the government's actions and pronouncements concerning transparency reporting vis-à-vis Twitter and other "similarly situated" providers, operates as a prior restraint on those providers' speech.

companies that want to report information in a manner not outlined in the DAG Letter are forced to self-censor to avoid potential criminal prosecution or to seek governmental approval before they publish information, as Twitter did here. *See* Compl. ¶ 38 (explaining Twitter submitted its draft transparency report to the government seeking "a determination as to exactly which, if any, parts of its transparency report are classified or, in the Department's view, otherwise may not lawfully be published online"). When a company is forced—through a combination of its conversations with the government and an objectively reasonable fear of prosecution for non-compliance—to obtain government sign-off before publishing a document, it faces a prior restraint. *See Smith*, 443 U.S. at 101, 101–06 (holding that a statute with a judicial "prior-approval requirement" before publication of certain information "acts in operation and effect like a licensing scheme" and is an unlawful prior restraint); *see also* Compl. ¶¶ 29, 35, 36, 38 (describing the government's portrayal of the DAG Letter and Notice in conversations with Twitter, and Twitter's submission of its draft transparency report for prior approval prior to ensure compliance with the government's pre-approved reporting scheme).

Twitter's decision to seek approval—and other companies' potential reluctance to publish transparency reports that do not adhere to the government's framework—is all the more reasonable in light of the fact that the government has not specifically disavowed prosecuting Twitter for issuing a transparency report that does not comply with the terms of the DAG Letter. *Cf. Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2345 (2014) (finding First Amendment claim justiciable when the "specter of enforcement" led to a chill on speech). The "specter of enforcement" looms large in this case, creating a situation in which the DAG Letter—compounded by the government's actions after Twitter submitted its report for government clearance—operates as a prior restraint on Twitter's publication of truthful information.

Of course, as with other constitutional protections, the ban on prior restraints is not absolute. However, even in the national-security context, the government's burden in order to sanction a prior restraint is demanding. *See N.Y. Times Co. v. United States*, 403 U.S. 713, 714 (1971) (per curium); *see id.* at 732 n.2 (White, J., concurring) (denying injunction to prevent publication of Pentagon Papers, despite Government's claim that disclosure posed "grave and immediate danger" to national security). Indeed, "every member of the Court in *New York Times*, tacitly or explicitly, accepted [the Court's prior]

condemnation[s] of prior restraint as presumptively unconstitutional," regardless of the subject matter at issue. *Neb. Press Ass'n*, 427 U.S. at 558 (quotation marks and citation omitted); *see also CBS, Inc. v. Davis*, 510 U.S. 1315, 1317 (1994) (Blackmun, J., sitting as circuit justice) (stating that prior restraints have been allowed "only where the evil that would result from the reportage is both great and certain and cannot be mitigated by less intrusive measures"). The government has not shown any such "great and certain" risk to national security posed by the publication of aggregate numbers of national-security requests a given company has historically received. *See supra* Part II.C.

Even to the extent that speech in the national-security context can be conditioned, based on various statutory schemes, on governmental permission, the burden still lies with the government to show that the First Amendment's requirement of adequate procedural protections against "impermissible censorship" has been met. *Mukasey*, 549 F.3d at 871 (citing *Freedman v. Maryland*, 380 U.S. 51, 58 (1965)); *see id.* ("[T]he burden of going to court to suppress speech and the burden of proof in court must be placed on the government." (citing *Freedman*, 380 U.S. at 58–59)). And the government has not met this burden here.

CONCLUSION

Accordingly, the Court should deny Defendants' partial motion to dismiss.

Dated: February 17, 2015

By: */s/ Joseph C. Gratz*

Joseph C. Gratz (SBN 240676)
jgratz@durietangri.com
DURIE TANGRI LLP
217 Leidesdorff Street
San Francisco, CA 94111
Telephone: 415-362-6666
Facsimile: 415-236-6300

Attorneys for Amicus Curiae
Freedom of the Press Foundation

Brett Max Kaufman (Of Counsel)
brettmaxkaufman@nyu.edu
TECHNOLOGY LAW & POLICY CLINIC
NEW YORK UNIVERSITY SCHOOL OF LAW
245 Sullivan Street
New York, New York 10012
Telephone: 212-998-6430
Facsimile: 212-995-4031

CERTIFICATE OF SERVICE

I certify that all counsel of record are being served on February 17, 2015, with a copy of this document via the Court's CM/ECF system.

/s/ Joseph C. Gratz
Joseph C. Gratz