UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.

IN RE MOTION FOR DECLARATORY JUDGMENT OF A FIRST AMENDMENT RIGHT TO PUBLISH AGGREGATE INFORMATION ABOUT FISA ORDERS	)	Docket No. Misc. 13-03
IN RE MOTION TO DISCLOSE AGGREGATE DATA REGARDING FISA ORDERS	)	Docket No. Misc. 13-04
IN RE MOTION FOR DECLARATORY JUDGMENT TO DISCLOSE AGGREGATE DATA REGARDING FISA ORDERS AND DIRECTIVES	)	Docket No. Misc. 13-05
IN RE MOTION FOR DECLARATORY JUDGMENT TO DISCLOSE AGGREGATE DATA REGARDING FISA ORDERS AND DIRECTIVES	)	Docket No. Misc. 13-06
IN RE MOTION FOR DECLARATORY JUDGMENT TO REPORT AGGREGATED DATA REGARDING FISA ORDERS	)	Docket No. Misc. 13-07

THE UNITED STATES' OPPOSITION TO THE COMPANIES' MOTION TO STRIKE THE GOVERNMENT'S *EX PARTE* RESPONSE TO MOTIONS TO DISCLOSE AGGREGATE DATA REGARDING FISA ORDERS

JOHN P. CARLIN
Acting Assistant Attorney General
for National Security

J. BRADFORD WIEGMANN
Deputy Assistant Attorney General

INTRODUCTION

The companies seek to strike the classified redacted information in the Government's response to their motions for declaratory judgment unless the Government discloses the information to their counsel. But the Government's response is consistent with Rule 7(j) of this Court's Rules of Procedure, which expressly authorizes the Government to file classified submissions *ex parte* in adversarial proceedings. The rule only requires that "[t]he unclassified or redacted version, at a minimum, must clearly articulate the government's legal arguments." None of the legal arguments in the Government's public brief have been redacted. The brief was carefully reviewed to provide as much information as possible to the companies and to the public, consistent with national security. The redacted information supports the Government's decision to classify the data the companies seek to disclose. That classification decision is within the discretion of the Executive Branch, and in any event does not interfere with the legal arguments the companies can offer.

Indeed, the classified information is irrelevant to the companies' argument about the scope of the Foreign Intelligence Surveillance Act's nondisclosure provisions, which is an issue of statutory construction. The companies argue that FISA only bars the disclosure of information that would reveal a particular target of surveillance, and does not bar disclosure of information (even classified information) that would compromise surveillance generally. If the companies' narrow interpretation of FISA were correct, then the Government's classified submission – which does not relate to disclosures of particular surveillance targets, but rather explains how an adversary could use the companies' proposed disclosures to determine the capabilities and limits of the Government's surveillance – would be irrelevant.

As to the companies' First Amendment challenge, the Government has disclosed the basis for its classification decision, a judgment that is constitutionally committed to the Executive. Because the basis for the decision is provided, the companies can challenge whether the disclosure prohibitions are narrowly tailored to protect the information classified by the Executive Branch.[1]

In any event, even where classified evidence is central to a civil case, unlike here, it is well-settled that a Court can review classified information *ex parte* and *in camera.* That rule applies irrespective of whether counsel could qualify for security clearances. Accordingly, the companies' motion to strike should be denied.

ARGUMENT

I. The Government Has Met and Exceeded the Requirements of Rule 7(j).

The Government's public brief meets and exceeds the requirements of Rule 7(j). The rule clearly provides that submissions to the Court "which may include classified information" will be reviewed by the Court "*ex parte* and *in camera*" and that adversarial parties will receive only "an unclassified or redacted version" which "clearly articulate[s] the government's legal arguments." Rule of Procedure 7(j). Not only does the Government's public brief "clearly articulate the government's legal arguments," the legal arguments are fully disclosed. The redacted information contains no additional legal arguments, no case citations, and no discussion of statutory or other law.

[1] When the Government initially filed its responsive memorandum, footnote 4 of that brief was classified and redacted. The Government has since decided to release footnote 4. A public version of the Government's responsive memorandum is attached as Exhibit A.

The overwhelming majority of the Government's brief is available to the public and the companies. *See* Response of the United States to Motions for Declaratory Judgment (Govt. Response).[2] There are approximately 50 paragraphs in the brief, and only two are fully redacted and only four are partly redacted. There are no redactions in any section of the argument aside from the section entitled "The Information that the Companies Seek to Disclose is Classified." That argument is primarily factual, and the unredacted portions of the section "clearly articulate" the only legal arguments it contains, including: (1) that the information that the companies wish to disclose has been classified at the Secret level, *id.* at 5-6; (2) that this Court does not independently review Executive Branch classification decisions, *id.* at 6 (quoting *In re Mot. for Release of Ct. Records*, 526 F. Supp. 2d 484, 491 (For. Intel. Sur. Ct. 2007)); (3) that Executive Branch classification decisions are entitled to "the utmost deference," *id.* (quoting *Dep't of the Navy v. Egan*, 484 U.S. 518, 530 (1988)); and (4) that such deference is especially appropriate where the Executive Branch bases its classification decision, as here, on a review of all pertinent information, including whether disclosure of the data in the manner proposed by the companies would risk filling out the mosaic of information available to our adversaries in their efforts to assess and avoid our surveillance capabilities, *id.* at 6-7 (citing cases).

The redactions appear solely in the Government's description of the *factual* basis for the FBI's classification, but even this portion of the Government's response is substantially unredacted and provides the essential reasons supporting the classification decision, as follows:

[2] The companies complain about redactions in the supporting declaration filed by the Government. But Rule 7(j) only requires the provision of "the government's legal arguments," and these are contained in the Government's brief.

The detailed disclosures the companies propose would reveal the nature and extent of FISA-authorized process served on the major providers in this country. The potential harm from such disclosures is easy to illustrate.

First, the disclosure of FISA data in specific numbers and by specific FISA provisions, as the companies seek, would provide adversaries significant information about the Government's collection capabilities with respect to particular providers. Disclosures of FISA information in a manner that would permit our adversaries to identify those collection capabilities would harm national security by allowing them to switch providers to avoid surveillance.

. . . .

Second, for similar reasons, the companies' proposed unilateral disclosures would allow our adversaries to infer when the Government has acquired a collection capability on new services. . . .

Third, the proposed disclosures would also enable our adversaries to gain significant information about which platforms and services are not subject to surveillance, or are subject to only limited surveillance. . . . Disclosing precise numbers associated with each provision or title of FISA, as the companies propose, would provide our adversaries with even more specific information, which they could use to track the Government's sources and methods of FISA-authorized intelligence collection.

If these leading Internet companies are permitted to make these disclosures, the harms to national security would be compounded by the fact that other companies would surely seek to make similar disclosures. As a result, our adversaries could soon be able to obtain a comprehensive picture of FISA-related surveillance activities.

In addition, the disclosure of precise numbers of FISA orders reasonably could be expected to cause other serious harms to national security. . . .

There is little doubt that foreign adversaries can and will glean important national security information from publicly available data. Indeed, the Intelligence Community knows that our adversaries actively gather information to assess such capabilities and react to avoid surveillance. If our adversaries know which platforms the Government *does not* surveil, they can communicate over those platforms when, for example, planning a terrorist attack or the theft of state secrets. Such disclosures could significantly and irreparably harm counterterrorism and counterintelligence efforts. Other types of harm can also result from adversaries learning which platforms the Government *does* surveil. Most obviously, they can avoid them. But as this Court has recognized, they can also use that information to engage in deceptive tactics or disinformation campaigns that could undermine intelligence operations and that could even expose Government personnel to the risk of physical harm.

Id. at 7, 9-11 (citations omitted).

Accordingly, the companies have received considerably more than the "clear articulation" of the Government's legal arguments required by Rule 7(j). Although the companies are entitled to an adequate description of the Government's legal arguments, they are not entitled to "knowledge of the specific evidence on which [FBI] relied" in classifying the information that the companies seek to disclose, where that evidence is itself classified. *Jifry v. FAA*, 370 F.3d 1174, 1184 (D.C. Cir. 2004).

II. It Is Well-Established That Courts May Review Classified Information *Ex Parte* and *In Camera,* Including in Constitutional Challenges.

The companies argue that if Rule 7(j) permits the Government's *ex parte* filing (as it does), such an interpretation "would make the rule unconstitutional." Mot. to Strike at 5. Contrary to their argument, it is well-established that Courts can review classified national security information *ex parte* and *in camera.*[3]

A. Rule 7(j) Appropriately Accommodates the Executive Branch's Constitutional Responsibility to Protect National Security.

By expressly providing that the Government need not disclose classified information in adversarial proceedings, Rule 7(j) recognizes that the Executive Branch is constitutionally charged with the responsibility to protect national security information. *See, e.g., Dep't of Navy v. Egan*, 484 U.S. 518, 527 (1988). The Government has a compelling interest in the protection of such information, *id.,* and "the protection of classified information must be committed to the broad discretion of the agency responsible, and this must include broad discretion to determine who may have access to it," *id.* at 529; *see also, e.g., Holy Land Found.*

[3] The companies suggest that the Court should apply the canon of constitutional avoidance. *See* Mot. to Strike at 5 n.2. That cannon is inapplicable because Rule 7(j) is unambiguous. *See, e.g., HUD v. Rucker*, 535 U.S. 125, 134-35 (2002). The Rule unambiguously authorizes the Government to file classified submissions *ex parte* and *in camera,* and the rule raises no serious constitutional issues.

for Relief & Devel. v. Ashcroft, 333 F.3d 156, 164 (D.C. Cir. 2003) (recognizing the "primacy of the Executive in controlling and exercising responsibility" over national security information).

In furtherance of the Executive Branch's responsibility to protect sensitive national security information, the President has issued an Executive Order governing the use and protection of classified information. *See* Exec. Order 13,526, 75 Fed. Reg. 707 (Dec. 29, 2009); *see also* FISC Rule of Procedure 3 (providing that the Court will "[i]n all matters . . . comply with the security measures established pursuant to . . . Executive Order 13526"). Pursuant to this order, access to classified information is permitted only where the recipient has a requisite security clearance and there has been a determination that the recipient has a "need-to-know" the information. Exec. Order 13,526 § 4.1(a). A "need-to-know" is "a determination within the executive branch in accordance with directives issued pursuant to this order that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function." *Id.* § 6.1(dd).

In this case, some of the redacted information is classified at the Secret level, which means that disclosure "reasonably could be expected to cause serious damage to the national security," while other redacted information is classified at the Top Secret level (and is designated as sensitive compartmented information, *see* 50 U.S.C. § 3024(j)), which means that disclosure "reasonably could be expected to cause exceptionally grave damage to the national security." *See* Exec. Order 13,526 § 1.2(a). Although counsel for some of the companies may have security clearances, none may lawfully access sensitive compartmented information, and none has been found to have a "need-to-know" any of the classified information in order to perform a governmental function.

A private party or counsel in non-criminal litigation does not have a "need-to-know" classified information even where, unlike here, the information is central to the case. *See, e.g.*, *Sterling v. Tenet*, 416 F.3d 338, 348 (4th Cir. 2005); *Holy Land Found.*, 333 F.3d at 164; *Ellsberg v. Mitchell*, 709 F.2d 51, 61 (D.C. Cir. 1983) (explaining that the rule denying counsel access to classified information is "well settled"). And although even classified information that is "central" to a civil case can be withheld, the classified information at issue here is not even central to the companies' arguments.

The companies' first argument, that FISA's nondisclosure provisions preclude only disclosure of information concerning the targets of FISA surveillance, is a pure legal interpretation of the statute. Although the Government's brief establishes that the data the companies seek to disclose is classified, under the companies' narrow interpretation it is irrelevant that the data is classified. Under their argument, it is also irrelevant that the disclosures would undermine the secrecy of surveillance in significant ways that do not implicate a particular target. The companies' interpretation – that FISA would prohibit only disclosures concerning discrete targets and would permit damaging disclosures about the surveillance more generally – is simply implausible and nowhere apparent from the text and structure of FISA, as the Government explains in non-redacted portions of its brief. Govt. Response at 12-16.

In the alternative, the companies argue in their declaratory judgment motions that prohibiting them from disclosing classified data about any FISA process they receive is not narrowly tailored under the First Amendment. But they cannot premise their First Amendment claim on challenging the Government's decision to classify the data they seek to disclose. This Court does not independently review Executive Branch classification decisions. *See In re Mot. for Release of Ct. Records*, 526 F. Supp. 2d 484, 491 (For. Intel. Sur. Ct. 2007). Because the

Government has fully disclosed the key reasons for that classification decision, the companies can argue that the disclosure restrictions are not narrowly tailored to protect those national security concerns. The companies do not need specific classified examples or details supporting these harms to argue that the nondisclosure prohibitions are not narrowly tailored to address them.

Finally, there is no reason to risk the disclosure of any of the information redacted from the Government's public brief, given its sensitivity and limited value to the companies' arguments. While the Government does not doubt the good faith of the companies and their counsel, "any such disclosure [of classified information] carries with it serious risk that highly sensitive information may be compromised." *Halkin v. Helms*, 598 F.2d 1, 7 (D.C. Cir. 1978) (citation omitted); *accord Sterling*, 416 F.3d at 348. The companies' assertion that counsel for some of the companies already know "the core information that the government seeks to protect in this [underlying] litigation . . . as well as with even more sensitive information, such as the names and identifiers of the targets of [FISA] orders," is of no moment. Mot. to Strike at 9. Past access to classified information for one purpose does not establish a need to know classified information for a different purpose. *See Doe v. CIA*, 576 F.3d 95, 105-06 (2d Cir. 2009) (rejecting argument that government's refusal to allow plaintiffs or their counsel access to classified information to oppose invocation of state secrets privilege unconstitutionally interfered with their ability to prosecute a discrimination lawsuit, where "[t]hey do not ask the CIA for access to classified information that [wa]s new to them"); *see also Pfeiffer v. CIA*, 60 F.3d 861, 864 (D.C. Cir. 1995). And, in any event, the classified information that has been redacted from

the public version of the Government's brief is qualitatively different from any sensitive information that may have been provided to certain companies as part of the FISA process.[4]

B. Rule 7(j) Does Not Raise Any Constitutional Issues.

Contrary to the companies' argument, Rule 7(j) raises no constitutional issues because, as discussed above, it is well-established that courts can review classified national security information *ex parte* and *in camera*. Numerous courts have rejected the same constitutional arguments the companies assert here.

1. Due Process Does Not Require the Government to Disclose Classified Information in Civil Litigation.

The companies invoke the Due Process Clause, but due process does not require the Government to disclose classified information in civil litigation. Rather, due process is "flexible and calls for such procedural protections as the particular situation demands." *Morrissey v. Brewer*, 408 U.S. 471, 481 (1972). Where the Government has a legitimate interest in protecting the secrecy of information, as it inarguably does with classified national security information, the opposing party's "interests as a litigant are satisfied by the ex parte/in camera decision of an impartial district judge." *Meridian Int'l Logistics, Inc. v. United States*, 939 F.2d 740, 745 (9th Cir. 1991); *accord Hayden v. National Sec. Agency*, 608 F.2d 1381, 1385 (D.C. Cir. 1979) (in the national security context, "this court has accepted the idea of In camera review of . . . documents without the presence of [plaintiff's] counsel").

---

[4] The companies' focus on "the names and identifiers of targets" mirrors the narrow focus of their underlying merits motions. *See, e.g.*, LinkedIn Mot. at 8-9 (contending that the non-disclosure obligation imposed by FISA extends only to the "identity" of subscribers and the "substance of communications"). While it is important to protect the secrecy of the identity of foreign intelligence targets, that is not the only type of national security information that is protected from disclosure. *See* Govt. Response at 14-16.

In *Holy Land Foundation for Relief & Development v. Ashcroft*, 333 F.3d 156 (D.C. Cir. 2003), the court held that "due process require[s] the disclosure of *only* the unclassified portions of the administrative record" to the plaintiff. *Id.* at 164 (citation omitted) (emphasis in original). The case raised First Amendment challenges to the Government's decision to block the foundation's assets, and the Government relied on both classified and unclassified evidence in taking that action. *Id.* at 164. The court based its conclusion, in part, on "the primacy of the Executive in controlling and exercising responsibility over access to classified information, and the Executive's compelling interest in withholding national security information from unauthorized persons in the course of executive business." *Id.* (internal quotation marks and citation omitted). Other cases have consistently rejected such due process challenges to submitting classified information *ex parte* and *in camera*.[5]

The companies rely heavily on *Al Haramain Islamic Foundation, Inc. v. United States Department of Treasury*, 686 F.3d 965 (9th Cir. 2012), but that case further supports the Government's position. In *Al Haramain*, the court held that due process did not require the

---

[5] *See, e.g., Jifry*, 370 F.3d at 1184 (holding that due process was satisfied although the plaintiffs were not given "knowledge of the specific [classified] evidence on which [the Government] relied" in making the challenged decision); *People's Mojahedin Org. of Iran v. Dep't of State*, 327 F.3d 1238, 1242-43 (D.C. Cir. 2003) ("The Due Process Clause requires only that process which is due under the circumstances of the case" and this does not include disclosure to the opposing party of classified intelligence relied on by the Government); *Global Relief Found., Inc. v. O'Neill*, 315 F.3d 748, 754 (7th Cir. 2003) (rejecting a challenge to a statute that, like Rule 7(j), "authorize[d] the use of classified evidence that may be considered *ex parte* by the district court"); *National Council of Resistance of Iran v. Dep't of State*, 251 F.3d 192, 208 (D.C. Cir. 2001) (holding that due process required notice but that the Government "need not disclose the classified information to be presented *in camera* and *ex parte* to the court"); *id.* at 207 (reasoning "that [the] strong interest of the government [in protecting against the disclosure of classified information] clearly affects the nature ... of the due process which must be afforded petitioners"); *Patterson v. FBI*, 893 F.2d 595, 600 n.9 (3d Cir. 1990) (citing cases); *see also Weberman v. National Sec. Agency*, 668 F.2d 676, 678 (2d Cir. 1982) ("The risk presented by participation of counsel outweighs the utility of counsel, or adversary process, in construing a [classified document].").

disclosure to the plaintiff's counsel of classified information relied on by the Government to support subjecting the foundation to terrorism-related sanctions. *Id.* at 980-81. Despite the fact that the Government action would render a purported religious charitable organization "financially defunct," *id.* at 980, the court held that the Government's national security interests justified the use of classified information without disclosure to plaintiff or its counsel, *id.* at 982. *See also id.* at 981 ("Not surprisingly, all federal courts to have considered [plaintiff's] argument have rejected it."). In light of the significant interests asserted by the foundation in that case, it follows that the use of *in camera, ex parte* information is permitted here.

2. The First Amendment Does Not Force the Government to Disclose Classified Information to Justify a Nondisclosure Requirement.

The companies also invoke the First Amendment, but as *Holy Land* demonstrates, the Government's right to file classified information *ex parte* and *in camera* also applies in cases involving First Amendment challenges. The companies' position that they are entitled to see all of the classified information in the Government's brief, on First Amendment grounds, would give plaintiffs a right to see classified information any time they challenge a nondisclosure obligation regarding other sensitive information. But it cannot be that the Government's only option for safeguarding classified information is to expose to private parties additional sensitive classified information. *See Bassiouni v. FBI*, 436 F.3d 712, 722 n.7 (7th Cir. 2006) ("We do not believe that Congress meant to place law enforcement agencies in the catch-22 of either divulging current investigatory activities or not asserting the law enforcement [interest].").

In an analogous case, *Stillman v. Central Intelligence Agency*, 319 F.3d 546 (D.C. Cir. 2003), the court denied counsel access to classified information where the plaintiff challenged on First Amendment grounds the Government's determination that information he sought to publish

was classified. *Id.* at 547-48. Although the Government determined that plaintiff's counsel could qualify for a security clearance, *id.*, the Government denied counsel access to the classified information based on his lack of a need to know, *id.* at 547. The district court determined that the First Amendment required that plaintiff's counsel be given access to the materials to challenge the classification decision, and the Government appealed. *Id.* at 547-48. In reversing the district court, the court of appeals observed that in cases involving classified information, "*in camera* review of affidavits, followed if necessary by further judicial inquiry, will be the norm." *Id.* at 548 (citation omitted). On remand, the district court upheld the Government's classification decision on the basis of *ex parte*, *in camera* submissions, giving "substantial deference" to the Government. *Stillman v. CIA,* 517 F. Supp. 2d 32, 39 (D.D.C. 2007). Likewise, in *Tabbaa v. Chertoff*, 509 F.3d 89 (2d Cir. 2007), the plaintiff raised First and Fourth Amendment challenges, but the court "viewed, *ex parte* and *in camera*, the classified intelligence at issue in order to ensure independently that there was a sufficient basis for" the Government declaration. *See id.* at 93 n.1.

The companies rely on *John Doe, Inc. v. Mukasey,* 549 F.3d 861 (2d Cir. 2008), to argue that their First Amendment challenge gives them a special right of access to classified information. Mot. to Strike at 6. But that reliance is puzzling, because the statute governing nondisclosure of National Security Letters (NSLs) at issue in *Doe* expressly authorizes the Government to submit materials *ex parte* and *in camera,* and the court of appeals accepted a classified submission *ex parte* that provided a supplemental justification for the nondisclosure requirement at issue in that case. *See* 549 F.3d at 881-82 & n.15. The court determined that it should largely defer to the Government's arguments regarding the need to maintain secrecy, even

though NSLs are unclassified. *Id.* at 882 ("Such a judgment is not to be second-guessed, but a court must receive some indication that the judgment has been soundly reached.").

Importantly, even though this Court is constitutionally entitled to review classified information *ex parte* and *in camera*, the Government has provided to the companies and to the public significant information regarding the nature of the harms underlying its decision to classify the data the companies seek to disclose. And as argued above, the redactions in the Government's brief do not materially affect any of the arguments the companies can offer in favor of disclosing the classified data. Accordingly, the Government's compliance with Rule 7(j) raises no First Amendment issues.

CONCLUSION

For the reasons discussed above, the companies' Motion to Strike should be denied.

December 6, 2013

Respectfully submitted,

JOHN P. CARLIN
Acting Assistant Attorney General
for National Security

J. BRADFORD WIEGMANN
Deputy Assistant Attorney General
National Security Division

N. CHRISTOPHER HARDEE
Chief Counsel for Policy
National Security Division

/s/ Jeffrey M. Smith
JEFFREY M. SMITH
NICHOLAS J. PATTERSON
U.S. Department of Justice
National Security Division
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530
Phone: (202) 514-5600
Fax: (202) 514-8053

Attorneys for the United States of America

CERTIFICATE OF SERVICE

I hereby certify that a true copy of the United States' Opposition to the Companies' Motion to Strike the Government's *Ex Parte* Response to Motions to Disclose Aggregate Data Regarding FISA Orders was served by the Government via Federal Express overnight delivery on this 6th day of December, 2013, addressed to:

Albert Gidari
Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101

Attorney for Google Inc.

James Garland
Covington & Burling LLP
1201 Pennsylvania Avenue, NW
Washington, DC 20004-2401

Attorney for Microsoft Corporation

Marc J. Zwillinger
ZwillGen PLLC
1705 N Street, NW
Washington, DC 20036

Attorney for Yahoo! Inc.

Carl J. Nichols
Wilmer Cutler Pickering Hale and Dorr LLP
1875 Pennsylvania Avenue, NW
Washington, DC 20006

Attorney for Facebook, Inc.

Jerome C. Roth
Munger, Tolles & Olson LLP
560 Mission Street, 27th Floor
San Francisco, CA 94105

Attorney for Linkedin Corporation

/s/ Jeffrey M. Smith

Exhibit A

[redacted]

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.

IN RE AMENDED MOTION FOR DECLATORY JUDGMENT OF A FIRST AMENDMENT RIGHT TO PUBLISH AGGREGATE INFORMATION ABOUT FISA ORDERS	Docket No. Misc. 13-03
IN RE MOTION TO DISCLOSE AGGREGATE DATA REGARDING FISA ORDERS	Docket No. Misc. 13-04
IN RE MOTION FOR DECLARATORY JUDGMENT TO DISCLOSE AGGREGATE DATA REGARDING FISA ORDERS AND DIRECTIVES	Docket No. Misc. 13-05
IN RE MOTION FOR DECLARATORY JUDGMENT TO DISCLOSE AGGREGATE DATA REGARDING FISA ORDERS AND DIRECTIVES	Docket No. Misc. 13-06
IN RE MOTION FOR DECLARATORY JUDGMENT TO REPORT AGGREGATED DATA REGARDING FISA ORDERS	Docket No. Misc. 13-07

(U) RESPONSE OF THE UNITED STATES TO MOTIONS FOR DECLARATORY JUDGMENT BY GOOGLE INC., MICROSOFT CORPORATION, YAHOO! INC., FACEBOOK, INC., AND LINKEDIN CORPORATION

JOHN P. CARLIN
Acting Assistant Attorney General
for National Security

TASHINA GAUHAR
Deputy Assistant Attorney General
for Intelligence

[redacted]

[redacted]

[redacted]

TABLE OF CONTENTS

[redacted]

TABLE OF AUTHORITIES

CASES:

[redacted]

(U) INTRODUCTION

(U) The United States Government firmly supports a policy of appropriate transparency with respect to its intelligence activities. As the President has emphasized, such a policy furthers accountability and increases public trust in the Government's activities. Consistent with this approach, the Government is actively engaged in a careful review of classified information related to the foreign intelligence surveillance activities authorized by this Court. The purpose of this review is to make public as much information about these activities as is consistent with the national security interests of the United States. In conducting this review, the Government must balance the need to inform the public about these activities with the need to protect classified sources and methods of intelligence collection, including the Government's ability (or inability) to conduct surveillance on particular electronic communication service providers or platforms. Releasing information that could induce adversaries to shift communications platforms in order to avoid surveillance would cause serious harm to the national security interests of the United States. *See* Declaration of Andrew G. McCabe, Acting Executive Assistant Director, Federal Bureau of Investigation (FBI) (attached).

(U) Balancing the competing interests at stake, the Government has taken a number of significant steps—above and beyond what the law requires—in order to promote transparency and to accommodate the legitimate interests of companies, including those that have filed motions before this Court and others that have not. For example, for the first time, in the winter of 2013, the Government agreed that companies may report the aggregate number of National Security Letters (NSLs) they receive, in numerical ranges and on a periodic basis.[1] More

[1] (U) NSLs are a type of administrative subpoena issued by U.S. Government agencies, particularly the Federal Bureau of Investigation (FBI), when investigating matters related to national security. *See* 12

[redacted]

[redacted]

recently, the Government, in consultation with the Court, agreed to permit companies to make a wider set of disclosures by opting instead to report, in certain bands, the aggregate number of criminal and national security related orders they receive from federal, state, and local government entities combined, and the number of user accounts affected by such orders. A number of companies have agreed to exercise that option, which allows them to demonstrate to their customers that the sum total of *all* such process affects only a tiny fraction of the companies' user accounts.[2]

(U) In addition, on August 29, 2013, the Government announced that it will report annually the total number of orders issued nationwide and the total number of targets the orders affect. The report will include (a) the number of Foreign Intelligence Surveillance Act (FISA) orders or warrants issued based on probable cause (*i.e.*, pursuant to Title I, Title III, Section 703, or Section 704 of FISA) and the number of targets affected by those orders or warrants; (b) the number of directives issued pursuant to Section 702 of FISA and the number of targets affected by those directives; (c) the number of orders issued pursuant to FISA's pen register provision (Title IV of FISA) and the number of targets affected by those orders; (d) the number of orders issued pursuant to FISA's business records provision (Title V of FISA) and the number of targets affected by those orders; and (e) the number of NSLs issued by the Government nationwide and the number of targets affected by the NSLs.

U.S.C. § 3414; 15 U.S.C. §§ 1681u, 1681v; 18 U.S.C. § 2709; 50 U.S.C. § 3162 (NSL statutory authorities).

[redacted]

[redacted]

[redacted]

(U) The Government's annual report of the use of various FISA authorities will provide the public significant information about how often the Government uses its foreign intelligence investigative authorities. The companies' ability to disclose how often they have responded to Government process will allow them to inform their customers about the likelihood that their information will be disclosed. On the other hand, because the Government's reporting will not be broken down by company, and the companies' reporting will aggregate criminal and non-criminal, content and non-content, and federal, state and local process, these reports will not provide our adversaries with a roadmap to the existence or extent of Government surveillance of any particular provider or communications platform.

(U) Dissatisfied with the Government's efforts to strike the appropriate balance between the public interest in transparency and the protection of national security, the petitioners seek declaratory relief that would effectively give every communications provider in the United States the right to reveal the nature and scope of any FISA surveillance of their communications platforms. Such information would be invaluable to our adversaries, who could thereby derive a clear picture of where the Government's surveillance efforts are directed and how its surveillance activities change over time, including when the Government initiates or expands surveillance efforts involving providers or services that adversaries previously considered "safe."

(U) In their original motions, Google and Microsoft sought to publish one aggregate number for all the FISA process they receive. After failing to reach a settlement with the Government, however, they amended their motions to seek relief that would present an even greater risk to national security: the right to disclose the *precise number* of FISA process they may receive under *each separate provision* of FISA. *See* Amended Google Mot. at 7; Microsoft

[redacted]

[redacted]

Mot. at 5. Microsoft goes still further, seeking to disclose separate categories for "non-content" requests and "content *and* non-content" requests. *Id.* (emphasis in original). After Google and Microsoft filed their amended motions, Yahoo! Inc., Facebook, Inc., and LinkedIn filed motions seeking essentially the same scope of relief.

(U) Because revealing FISA data on a company-by-company basis would cause serious harm to national security, such data has been classified by the FBI. That classification decision establishes that unilaterally disclosing the information would undermine the secrecy of the surveillance, in violation of this Court's orders, which require any company that has received a FISA order to protect the secrecy of the intelligence acquisitions. The companies assert that the secrecy requirements apply only to particular surveillance targets. But that implausible reading ignores the forest for the trees. It would permit damaging disclosures that would reveal sources and methods of surveillance potentially nationwide. The secrecy provisions in the orders flow from statutory requirements that, according to their plain language, protect such sources and methods, not just particular collection efforts. Indeed, limiting the secrecy protections only to information revealing a particular surveillance target would authorize a wide range of other damaging disclosures, from the nature of surveillance targets to their general locations, among others.

(U) Contrary to the companies' argument that they have a First Amendment right to disclose this sensitive national security information, it is well-settled that prohibitions on the disclosure of classified information, such as the ones contained in this Court's orders, satisfy the First Amendment. The Government has a compelling interest in protecting such national

[redacted]

[redacted]

security information from disclosure, and the prohibitions on disclosure are narrowly tailored to protect that interest.

(U) Finally, insofar as the companies argue that no other laws or regulations prohibit the disclosures they seek, the Court lacks jurisdiction to issue declaratory relief unrelated to prohibitions imposed pursuant to FISA. Because the data the companies seek to disclose is classified, the disclosures are prohibited by other sources of law, such as nondisclosure agreements between the Government and company employees. The interpretation and application of such non-FISA prohibitions are outside the specialized jurisdiction of this Court.

(U) Accordingly, the Court should deny the companies' motions for declaratory relief.

(U) ARGUMENT

I. (U) The Court-Ordered Nondisclosure Obligations Imposed Pursuant to FISA Prevent the Companies from Unilaterally Publishing Classified FISA Data.

(U) The companies assert that the information they seek to disclose is not classified, disregarding the harms to national security the proposed disclosures would likely cause. But classification judgments belong to the Executive Branch, not the companies, and the Executive Branch has classified the information. The companies' flawed premise undermines their entire argument: the only plausible reading of FISA, and the Court's orders, is that FISA orders and directives bar recipients from disclosing properly classified information about the nature and scope of the authorized surveillance activities.

A. (U) The Information that the Companies Seek to Disclose is Classified.

(U) The companies fail to address the harm their disclosures would cause to national security, beyond pointing out that they do not seek to disclose individual surveillance targets.

[redacted]

[redacted]

The companies' narrow focus on individual targets ignores that the disclosures would risk revealing the Government's collection capabilities as they presently exist and as they develop in the future. McCabe Decl. ¶ 30. Such disclosures could therefore cause significant harm to national security. As a result, the FBI has classified the data the companies seek to publish at the Secret level. *Id.* ¶ 27; *see also id.* ¶¶ 22-26.

(U) The FBI's assessment of harm is entitled to deference. This Court has previously held that "there is no role for this Court independently to review, and potentially override, Executive Branch classification decisions." *In re Mot. for Release of Ct. Records*, 526 F. Supp. 2d 484, 491 (Foreign Intel. Sur. Ct. 2007). As the Court recognized, if the U.S. Foreign Intelligence Surveillance Court (FISC) "were to assume the role of independently making declassification and release decisions . . . there would be a real risk of harm to national security interests and ultimately to the FISA process itself." *Id.* Moreover, "even if a typical FISC judge ha[s] more expertise in national security matters than a typical district court judge, that expertise would still not equal that of the Executive Branch, which is constitutionally entrusted with protecting the national security." *Id.* at 495 n.31. This Court's holding is consistent with the fact that "courts have traditionally shown the *utmost deference*" to the Executive Branch's authority to classify and control access to national security information. *Department of the Navy v. Egan*, 484 U.S. 518, 530 (1988) (emphasis added) (quoting *United States v. Nixon*, 418 U.S. 683, 710 (1974)).

(U) The FBI based its classification decision on a review of all pertinent information, including whether disclosure of the data in the manner proposed by the companies would risk filling out the mosaic of information available to our adversaries in their efforts to assess and

[redacted]

[redacted]

avoid our surveillance capabilities. McCabe Decl. ¶ 23. Deference to the Executive Branch is especially appropriate in such circumstances, where assessing the likely harm requires knowledge of many other pieces of information and intelligence expertise regarding how additional disclosures would help adversaries form a more complete mosaic to guide their efforts. *See CIA v. Sims*, 471 U.S. 159, 178-79 (1985); *United States v. Marchetti*, 466 F.2d 1309, 1318 (4th Cir. 1972); *accord United States v. Yunis*, 867 F.2d 617, 623 (D.C. Cir. 1989) ("Things that did not make sense to the District Judge would make all too much sense to a foreign counter-intelligence specialist who could learn much about this nation's intelligence-gathering capabilities from what these documents revealed about sources and methods.").

(U) The detailed disclosures the companies propose would reveal the nature and extent of FISA-authorized process served on the major providers in this country. The potential harm from such disclosures is easy to illustrate.

(U) First, the disclosure of FISA data in specific numbers and by specific FISA provisions, as the companies seek, would provide adversaries significant information about the Government's collection capabilities with respect to particular providers. Disclosures of FISA information in a manner that would permit our adversaries to identify those collection capabilities would harm national security by allowing them to switch providers to avoid surveillance.

[redacted]

[redacted]

[redacted]

[redacted] Second, for similar reasons, the companies' proposed unilateral disclosures would allow our adversaries to infer when the Government has acquired a collection capability on new services. [redacted]

[redacted] Third, the proposed disclosures would also enable our adversaries to gain significant information about which platforms and services are not subject to surveillance, or are subject to only limited surveillance. [redacted]

[redacted]

[redacted]

[redacted] Disclosing precise numbers associated with each provision or title of FISA, as the companies propose, would provide our adversaries with even more specific information, which they could use to track the Government's sources and methods of FISA-authorized intelligence collection.

(U) If these leading Internet companies are permitted to make these disclosures, the harms to national security would be compounded by the fact that other companies would surely seek to make similar disclosures. *See id.* ¶ 48. As a result, our adversaries could soon be able to obtain a comprehensive picture of FISA-related surveillance activities.

[redacted] In addition, the disclosure of precise numbers of FISA orders reasonably could be expected to cause other serious harms to national security. [redacted]

[redacted]

[redacted]

[redacted] There is little doubt that foreign adversaries can and will glean important national security information from publicly available data. Indeed, the Intelligence Community knows that our adversaries actively gather information to assess such capabilities and react to avoid surveillance. *Id.* ¶ 30; [redacted]. If our adversaries know which platforms the Government *does not* surveil, they can communicate over those platforms when, for example, planning a terrorist attack or the theft of state secrets. *Id.* ¶¶ 39[redacted] Such disclosures could significantly and irreparably harm counterterrorism and counterintelligence efforts. *Id.* ¶ 39. Other types of harm can also result from adversaries learning which platforms the Government *does* surveil. Most obviously, they can avoid them. But as this Court has recognized, they can also use that information to engage in deceptive tactics or disinformation campaigns that could undermine intelligence operations and that could even expose Government personnel to the risk of physical harm. *See In re Mot. for Release of Ct. Records,* 526 F. Supp.2d at 494; [redacted]

(U) In contrast, reporting an aggregate number of both national security and criminal process—which the Government has told the companies they can release—would not tend to disclose the Government's classified surveillance capabilities. The aggregate number would combine both content and non-content requests, so that our adversaries would not know, for example, whether a particular provider was responding to requests for subscriber identity information via an NSL, or was providing the full content of communications pursuant to a FISA

[redacted]

or Title III wiretap order. Thus, the extent of the Government's actual capabilities would be masked from our adversaries.

(U) It is quintessentially an Executive Branch responsibility to assess these risks to national security and to determine what information can be disclosed consistent with both transparency and national security interests. The Government cannot agree to the disclosures the companies seek because the disclosures will harm national security by risking the disclosure of the Government's capabilities to conduct surveillance with respect to particular providers and Internet platforms. In assessing whether the companies' proposed disclosures will undermine the secrecy of the Government's intelligence collection activities under FISA, the Court should defer to the judgment of the Executive Branch.

B. (U) The Court-Ordered Nondisclosure Obligations Required Under FISA Prohibit the Companies from Publishing Classified Sources and Methods of FISA Surveillance.

(U) As explained below, the nondisclosure provisions in FISA orders are prescribed by statute and require companies to protect the secrecy of authorized surveillance. Because the information the companies seek to disclose has been properly classified, it follows that protecting the secrecy of the acquisitions underlying that information requires keeping the information secret. The companies would interpret this Court's orders as protecting only information about specific targets, therefore permitting the broad disclosure of damaging information about the Government's sources and methods of surveillance overall. But such a result is contrary to the text and purpose of the secrecy provisions in FISA on which the orders are based.

(U) As an initial matter, the provisions of FISA should be enforced as written, *Connecticut Nat'l Bank v. Germain,* 503 U.S. 249, 253-54 (1992), and neither provision at issue

[redacted]

here contains the "particular target" limitation on secrecy that the companies advance. Titles I and VII of FISA provide that FISA orders "shall direct," and FISA directives "may direct," recipients to provide the Government with "all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition," without limitation. 50 U.S.C. § 1881a(h)(1)(A) (Title VII); *see also* 50 U.S.C. § 1805(c)(2)(B) (similar language for Title I).[4] Additionally, the orders "shall direct" and the directives "may direct" that recipients "maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition or the aid furnished" that such electronic communication service provider maintains. 50 U.S.C. § 1881a(h)(1)(B) (Title VII); *see also* 50 U.S.C. § 1805(c)(2)(C) (similar language for Title I).[5] Consistent with the Executive Branch's authority to control classified information, that provision explicitly

[4] (S/NF) To the extent that the moving companies receive process pursuant to Titles I and VII, the Title VII directives contain the statutorily permitted nondisclosure provisions, while the Title I orders contain nondisclosure requirements that track the statutory provision, although not identically. Title I orders typically contain language such as: "This order and warrant is sealed and the specified person and its agents and employees shall not disclose to the targets or to any other person the existence of the order and warrant or this investigation or the fact of any of the activities authorized herein or the means used to accomplish them, except as otherwise may be required by legal process and then only after prior notification to the Attorney General." Of course, disclosing the number of Title I orders received would violate such a provision as it would "disclose . . . the existence" of each of the orders.

[5] (U) The other FISA titles that provide search or surveillance authorities also contain nondisclosure provisions. *See* 50 U.S.C. § 1824(c)(2)(B)-(C) (requiring Title III orders to require the recipient to assist in the physical search "in such a manner as will protect its secrecy" and provide that "any records concerning the search or the aid furnished" that the recipient retains be maintained under appropriate security procedures); 50 U.S.C. § 1842(d)(2)(B) (requiring Title IV orders to direct that recipients "furnish any information, facilities, or technical assistance necessary to accomplish the installation and operation of the pen register or trap and trace device in such a manner as will protect its secrecy," and provide that "any records concerning the pen register or trap and trace device or the aid furnished" that the recipient retains shall be maintained under appropriate security procedures); 50 U.S.C. § 1861(d)(1) (providing that "[n]o person shall disclose to any other person that the [FBI] has sought or obtained tangible things pursuant to an order under" Title V of FISA). Because the potential national security harm at issue is the disclosure of information that could provide adversaries with information about the Government's electronic surveillance capacities, the nondisclosure provisions in Titles I and VII – the titles that concern electronic surveillance – are most relevant here.

[redacted]

provides for Executive Branch approval of the companies' procedures for maintaining all records associated with surveillance. The provision is not limited to protecting only specific targeting information that such records would reveal, and on its face does not give companies the right to disclose classified information so long as records are disclosed in large groups.

(U) Moreover, "[i]t is a fundamental canon of statutory construction that the words of a statute must be read in their context and with a view to their place in the overall statutory scheme." *Davis v. Michigan Dep't of Treas.*, 489 U.S. 803, 809 (1989). Reading a "particular target" limitation into FISA's secrecy provisions would be inconsistent with FISA's strong protections for the secrecy of the intelligence collection activities subject to the Court's review. Although the Government is seeking to make public as much information about these activities as the national security interests of the United States will permit, "[i]n the FISA context, there is an unquestioned tradition of secrecy, based on the vitally important need to protect national security." *In re Mot. for Release of Ct. Records,* 526 F. Supp.2d at 490-91 (citing *Haig v. Agee,* 453 U.S. 280, 307 (1981)). Such protections extend not just to targets but also to surveillance sources and methods generally, because "[t]he identification of targets and methods of surveillance would permit adversaries to evade surveillance, conceal their activities, and possibly mislead investigators through false information." *Id.* at 494.

(U) The implausibility of interpreting the "secrecy of the acquisition" to reach only the identification of targets is illustrated not only by the FBI's declaration but by the wide range of other damaging disclosures that interpretation would permit. There are numerous types of damaging disclosures that could be made without revealing the identity of a particular target, including general information concerning the type of target and their locations. The same is true

[redacted]

of the companies' narrow interpretation that the "records" they must protect extend only to the "identity" of subscribers or the "substance of communications," *see* LinkedIn Mot. at 8-9.

(U) It would be illogical to conclude that Congress enacted a "comprehensive statutory scheme designed to protect FISC records from routine public disclosure," *In re Mot. for Release of Ct. Records*, 526 F. Supp. 2d at 491, while allowing every public company to reveal damaging information about the nature and scope of surveillance under each separate title or provision of FISA. *Cf. Whitman v. American Trucking Ass'ns*, 531 U.S. 457, 468 (2001) (Congress "does not, one might say, hide elephants in mouseholes."). And although the companies invoke FISA's congressional reporting requirements to support their contemplated disclosures, those reporting requirements are another example of the careful protections provided for FISA information. Unlike the classified reports submitted to Congress, the information publicly reported pursuant to FISA provides aggregated data at a level of detail far less than even what the Government recently committed to provide voluntarily, and certainly not comparable to what the companies now seek. None of the Government's disclosures report company-by-company data.

(U) Accordingly, most reasonably construed, FISA's secrecy provisions prohibit the disclosure of FISA-related data in a manner that would provide insights into the Government's intelligence activities and risk harm to national security. The companies' proposed disclosures reasonably could be expected to cause serious harm to national security by revealing the Government's electronic surveillance capabilities and targeting actions on a company-by-company basis, potentially nationwide. *See* Part I.A *supra*. Relatedly, the disclosure of the classified data would reveal FISA-related sources and methods, and thus would be plainly

[redacted]

[redacted]

inconsistent with maintaining "records concerning the acquisition" in a manner that will protect its secrecy as determined by the Executive Branch.

(U) For these reasons, the Court should reject the companies' contention that any orders and directives they have received only prevent disclosures that concern particular surveillance targets. Their motions should be denied because their proposed disclosures would risk harm to national security by revealing the nature and scope of intelligence collection activities conducted by the Government pursuant to FISA.

II. (U) The Prohibitions on Disclosure Satisfy the First Amendment Because They Are Narrowly Tailored to Promote Compelling National Security Interests.

(U) The companies' First Amendment challenge turns on the same flawed premise that undermines their statutory argument. They argue that prohibiting their proposed disclosures would violate the First Amendment because the disclosures would not reveal particular surveillance targets, and therefore would not cause harm to national security. But as detailed above, the disclosures risk causing serious harm to national security. The Court's orders barring such disclosure satisfy any level of First Amendment scrutiny because they are narrowly tailored to serve a compelling governmental interest.

(U) As the companies acknowledge, "[t]he Government has a compelling interest in protecting . . . the secrecy of information important to our national security." *Snepp v. United States*, 444 U.S. 507, 509 n.3 (1980); *Department of the Navy v. Egan*, 484 U.S. at 527; *United States v. Sterling*, 724 F.3d 482, 509 (4th Cir. 2013). The companies' contemplated disclosures risk significant harm to national security by revealing the nature and scope of the Government's intelligence collection on a company-by-company basis throughout the country. *See* Part I.A, *supra*. This "evaluation of the facts by the Executive . . . is entitled to deference" even in

[redacted]

assessing First Amendment interests because, "when it comes to collecting evidence and drawing factual inferences in this area, the lack of competence on the part of the courts is marked, and respect for the Government's conclusions is appropriate." *Holder v. Humanitarian Law Project*, 130 S. Ct. 2705, 2727 (2010) (internal quotation marks and citation omitted).

(U) The Government's interest in preventing harm to national security is more than sufficient to outweigh the companies' interests in speaking about the particular FISA process they may receive. The principal case on which the companies rely, *Doe v. Mukasey,* 549 F.3d 861 (2d Cir. 2008), supports the Government's position. In *Doe,* the court concluded that the nondisclosure requirement applicable to unclassified NSLs "is not a typical prior restraint or a typical content-based restriction warranting the most rigorous First Amendment scrutiny." *Id.* 877. The court reached that conclusion after rejecting analogies to government processes in which the limited public interest in disclosure justifies lower First Amendment scrutiny, such as grand juries, civil discovery, or pre-publication review. *Id.* at 876-77. The court distinguished grand jury secrecy as "inher[ent] in the nature of the proceeding," whereas NSLs "might or might not" justify secrecy. *Id.* But FISA proceedings and foreign intelligence collection are subject to even stronger secrecy protections than grand juries and necessarily involve classified information. *See, e.g., In re Mot. for Release of Ct. Records,* 526 F. Supp.2d at 490 ("It is this highly classified, and fundamentally secret, nature of FISC records that distinguishes them from the records of other courts."). Accordingly, the companies' First Amendment interests should be evaluated against the "comprehensive statutory scheme designed to protect FISC records from routine public disclosure" and the absence of any long-standing practice of releasing the kind of information they seek to disclose. *Id.* at 491.

[redacted]

(U) Even outside the unique FISA context, *Doe* concluded that, while a "conclusory assertion" of harm would be insufficient to justify a prohibition, courts should defer to the "Government's considered assessment of *why* disclosure in a particular case may result in an enumerated harm related to such great matters as international terrorism or clandestine intelligence activities." 549 F.3d at 881 (emphasis in original). Even as to unclassified NSLs, nondisclosure can be justified where the Government "indicate[s] the nature of the apprehended harm and provide[s] a court with some basis to assure itself (based on *in camera* presentations where appropriate) that the link between disclosure and risk of harm is substantial." *Id.* at 881-82 (a "demonstration of a reasonable likelihood of potential harm, related to international terrorism or clandestine intelligence activities, will virtually always outweigh the First Amendment interest in speaking about such a limited and particularized occurrence as the receipt of an NSL and will suffice to maintain the secrecy of the fact of such receipt"). Here, the Government has explained in detail the serious harm to national security that the companies' proposed disclosures reasonably could be expected to cause.

(U) Recognizing that the Government has a compelling interest in protecting national security, the companies argue that the prohibitions on disclosure are not narrowly tailored. But the restrictions are narrowly tailored because there are no "less restrictive alternatives [that] would be at least as effective in achieving" the Government's compelling interest. *Reno v. ACLU*, 521 U.S. 844, 874 (1997); *see also Humanitarian Law Project*, 130 S. Ct. at 2723-30 (upholding a statute that restricted plaintiffs from "communicating a message" because the Government had "adequately substantiated" its determination that the statutory restriction served "the Government's interest in combating terrorism [which] is an urgent objective of the highest order"). The Government has demonstrated why vital national security considerations preclude

[redacted]

[redacted]

disclosure of information about FISA-authorized surveillance that will reveal the Government's surveillance activities by provider and platform. *See* Part I.A *supra.*

(U) Relying on authority involving the disclosure of individual NSLs, the companies argue that the disclosure prohibitions are not narrowly tailored because aggregate disclosures of FISA data by large providers, such as themselves, will not reveal a particular surveillance target. But this is another example of their flawed premise. The harm to national security that led the FBI to classify the information concerns the disclosure of intelligence sources and methods of electronic surveillance, not the identification of a particular individual recipient of process. Irrespective of whether disclosures would tend to reveal a particular surveillance target, they would allow adversaries to derive a clear picture of the nature and extent of the Government's FISA surveillance activities with respect to every major provider in the country. Such harm to national security would result from disclosure of the data by any type of provider, large or small, and from the totality of information that would be disclosed. The Government is entitled to significant deference in assessing the harms to national security, and its judgment—not that of the providers—is critical to determining the scope of the prohibitions on disclosure that are necessary to protect national security interests. *See, e.g.*, *Sims*, 471 U.S. at 178-79; *Marchetti*, 466 F.2d at 1318; *Yunis*, 867 F.2d at 623.

(U) The companies also argue that the Government's public disclosures of aggregated FISA data somehow demonstrate that the prohibitions on the companies' proposed disclosures are not narrowly tailored. On the contrary, the Government's voluntary disclosures of FISA data demonstrate that the Government seeks to protect such information in a narrowly tailored manner and has carefully stopped short of permitting disclosures that would cause harm. None of the Government's public disclosures reveal any information that would allow our adversaries

[redacted]

[redacted]

to determine the Government's surveillance capabilities of specific companies or specific platforms, or the timing of when the Government acquires certain surveillance capabilities. *See* McCabe Decl. ¶ 66. Rather, the Government has provided as much data as reasonably possible, consistent with national security, to inform the public about the nature of its intelligence activities.

(U) Finally, the companies argue that the public debate about the Government's surveillance activities justifies disclosure. Although the Government has attempted to release as much information as possible about the intelligence collection activities overseen by this Court, the public debate about surveillance does not give the companies the First Amendment right to disclose information that the Government has determined must remain classified. The companies are "correct in asserting that certain benefits could be expected" from public disclosure, but the argument "'proves too much'." *In re Mot. for Release of Ct. Records*, 526 F. Supp. 2d at 494 (citation omitted). It fails to account for the "detrimental consequences of broad public access" to such information. *Id.* at 494-95; *see also Snepp*, 444 U.S. at 509 n.3; *Egan*, 484 U.S. at 527.[6]

[6] (U) Moreover, it is unclear whether the companies need to disclosure such data to serve their interests in responding to erroneous reporting about their role in Government surveillance. The companies contend that they need to disclose FISA data to respond to "inaccurate media reporting" that suggests that the companies "provide[] the United States Government with direct access to [their] servers and network infrastructure." Am. Microsoft Mot. at 3; *accord* Am. Google Mot. at 2; Yahoo! Mot. at 2; Facebook Mot. at 2. But the companies fail to explain why disclosing precise numbers of various types of FISA orders that they may have received is necessary or even relevant to refuting mistaken reports that the Government has unlimited "direct access" to the companies' servers. Indeed, the companies make clear that, without the need to disclose any classified information, they have been able to clearly and forcefully respond to the inaccurate or misleading reporting. *See* Am. Google Mot. at 2-3 (referencing statement of Larry Page and David Drummond); Facebook Mot. at 2 (referencing statement of Mark Zuckerberg). And the Government itself has responded forcefully to such erroneous reports. *See, e.g.*, Office of the Director of National Intelligence, IC on the Record, available at http://icontherecord.tumblr.com/topics/section-702. There is reason to believe that these efforts have been successful. *See* Joseph Menn, *Analysis: Despite fears, NSA revelations helping U.S. tech industry*, Reuters, 9/15/13 RTRSUSTOP

[redacted]

[redacted]

(U) Accordingly, there is no constitutional impediment to protecting from disclosure properly classified information about the Government's sources and methods of intelligence collection. Such disclosures reasonably could be expected to cause serious harm to national security. The prohibitions on disclosure at issue here are narrowly tailored to prevent such harm.

III. (U) As a Court of Limited Jurisdiction, This Court Cannot Provide Declaratory Relief Regarding Legal Prohibitions on Disclosure Outside of FISA.

(U) The companies seek relief that goes well beyond restraints imposed pursuant to FISA. They also seek a declaration that "no applicable law or regulation" prohibits their proposed disclosures. *See* Am. Google Mot. at 7; *see also* LinkedIn Mot. at 1; Am. Microsoft Mot. at 5. But the interpretation and application of these other potential prohibitions on disclosure is not within this Court's specialized jurisdiction.

(U) Because the information that the companies seek permission to disclose is properly classified, it is subject to prohibitions on the disclosure of classified information. For example, employees of the companies have signed nondisclosure agreements that prohibit disclosure of classified information, whether publicly, to another employee or agent, or to any other person.

13:09:19 ("Google Inc. and Facebook Inc. [] say privately that they have felt little if any impact on their business [from the disclosures]. Insiders at . . . Microsoft Corp.[] also say they are seeing no fallout.").

(U) Additionally, as described above, the Government has permitted the companies to release the aggregate number of governmental requests for information (combining criminal and national security requests), which would demonstrate that only an exceptionally small percentage of their customers' accounts are subject to any governmental process at all. *See, e.g.*, Ted Ullyot, General Counsel, Facebook, *Facebook Releases Data Including All National Security Requests* (June 14, 2013), http://newsroom.fb.com/News/636/Facebook-Releases-Data-Including-All-National-Security-Requests ("With more than 1.1 billion monthly active users worldwide, this means that a tiny fraction of one percent of our user accounts were the subject of any kind of U.S. state, local, or federal U.S. government request (including criminal and national security-related requests) in the past six months.").

[redacted]

See McCabe Decl. ¶ 65.[7] Where relevant employees have entered into nondisclosure agreements that prohibit them from disclosing classified information, "[t]he Government is entitled to enforce its agreements to maintain the confidentiality of classified information." *United States v. Pappas*, 94 F.3d 795, 801 (2d Cir. 1996); *see also Wilson v. CIA*, 586 F.3d 171, 183-84 (2d Cir. 2009). Nondisclosure agreements are "a reasonable means for protecting this vital interest" that are consistent with the First Amendment. *Snepp*, 444 U.S. at 509 n.3. Other laws and regulations might also prohibit the companies' proposed disclosures. *See, e.g.*, 18 U.S.C. § 798(a)(3).

(U) This Court would not have jurisdiction to assess the potential applicability of such prohibitions, even if it could otherwise do so. Like any other Article III court, this Court has an obligation to assure itself of its jurisdiction before proceeding to the merits of a dispute. *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 94 (1998); *see also In re Sealed Case*, 310 F.3d 717, 731-32 (For. Intelligence Surv. Ct. of Rev. 2002) (FISC operates within "the constitutional bounds that restrict an Article III court"). As the Supreme Court has held, "[f]or a court to pronounce upon the meaning or the constitutionality of a state or federal law when it has no jurisdiction to do so is, by very definition, for a court to act ultra vires." *Steel Co.*, 523 U.S. at 101-02.

---

[7] (U) Both the current standard nondisclosure agreement, which went into effect in July 2013, and the previous version contained the following language: "I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency . . . responsible for the classification of . . . information or last granting me a security clearance that such disclosure is permitted.") *See* Standard Form 312: Classified Information Nondisclosure Agreement (effective July 2013), *available at*: http://www.gsa.gov/ portal/forms/ download/116218; Standard Form 312: Classified Information Nondisclosure Agreement (effective prior to July 2013), *available at:* http://armypubs.army.mil/eforms/pdf/s312.PDF.

[redacted]

[redacted]

(U) This Court, like all Article III courts, is a "court[] of limited jurisdiction marked out by Congress." *International Custom Prods., Inc. v. United States*, 467 F.3d 1324, 1326 (Fed. Cir. 2006) (quoting *Aldinger v. Howard*, 427 U.S. 1, 15 (1976)). This Court has been granted a narrow and specialized (but vital) jurisdiction limited to certain specified applications and certifications that may be filed by the Government and two types of petitions that a private party may file. *See* 50 U.S.C. §§ 1804, 1823, 1842, 1861, 1881. Thus, FISA does not provide this Court with jurisdiction to provide declaratory relief regarding the applicability or enforceability of non-FISA prohibitions on disclosure.

(U) Nor could such relief fall within this Court's inherent jurisdiction. Beyond those powers necessary for the exercise of its statutory jurisdiction or useful to adjudicate such cases, such as the power to construe the Court's own orders and procedures, "inherent power, which might be termed irreducible inherent authority, encompasses an extremely narrow range of authority involving activity so fundamental to the essence of a court as a constitutional tribunal that to divest the court of absolute command within this sphere is really to render practically meaningless the terms 'court' and 'judicial power.'" *Eash v. Riggins Trucking Inc.*, 757 F.2d 557, 562 (3d Cir. 1985) (*en banc*). The review and construction of nondisclosure agreements and other prohibitions on disclosure unrelated to FISA or the Court's rules and orders fall far outside the powers that "necessarily result to [this Court] from the nature of [the] institution," and therefore fall outside the Court's inherent jurisdiction. *Chambers v. NASCO, Inc.*, 501 U.S. 32, 43 (1991) (citation omitted).

(U) The companies rely on the Declaratory Judgment Act (DJA), 28 U.S.C. § 2201, but the DJA cannot create jurisdiction where jurisdiction is lacking. The DJA provides that "[i]n a case of actual controversy within its jurisdiction, . . . any court of the United States, upon the

[redacted]

filing of an appropriate pleading, may declare the rights and other legal relations of any interested party seeking such declaration." However, the DJA is "procedural only." *Chevron Corp. v. Naranjo*, 667 F.3d 232, 244 (2d Cir. 2012) (quoting *Skelly Oil Co. v. Phillips Petroleum Co.*, 339 U.S. 667, 671 (1950)). It "does not create an independent cause of action," *id.*, and it "is not an independent source of federal jurisdiction." *C&E Servs., Inc. v. District of Columbia Water & Sewer Auth.*, 310 F.3d 197, 201 (D.C. Cir. 2002) (quoting *Schilling v. Rogers*, 363 U.S. 666, 677 (1960)).[8]

(U) While the DJA refers to "any court of the United States," the Supreme Court has held that it does not necessarily confer the power to grant declaratory relief on a specialized tribunal of limited, statutorily specified jurisdiction. *See United States v. King*, 395 U.S. 1, 3-4 (1969). In *King*, the Supreme Court unanimously held that the DJA did not confer the power to grant declaratory relief on the United States Court of Claims, an Article III court of specialized jurisdiction. *See id.* at 4. The Court reasoned that the type of relief contemplated by the DJA "ha[d] never been 'within [the Court of Claims'] jurisdiction'" given that, unlike a court that exercises general federal question and diversity jurisdiction, the Court of Claims had, since its creation in 1855, a specialized and narrow jurisdiction. *Id.* (quoting the DJA).

(U) Given the limited jurisdiction of the FISC, the level of specificity with which Congress described it, and its "esoteric nature," *In re Mot. for Release of Ct. Records*, 526 F. Supp. at 486, it is unlikely that Congress intended to provide "expanded jurisdiction," *King*, 395 U.S. at 4, to broadly grant declaratory relief, pursuant to the DJA, about companies' rights to

[8] (U) Additionally, the DJA provides a court with "discretion to determine whether it will exert jurisdiction over a proposed declaratory action or not," and this has been "consistently interpreted . . . as a broad grant of discretion to district courts to refuse to exercise jurisdiction over a declaratory action that they would otherwise be empowered to hear." *Dow Jones & Co. v. Harrods Ltd.*, 346 F.3d 357, 359 (2d Cir. 2003).

[redacted]

make public disclosures. This is particularly so given that Congress created this Court and imbued it with specialized jurisdiction after *King* was decided. *See, e.g.*, *McQuiggen v. Perkins*, 133 S. Ct. 1924, 1934 n.3 (2013) ("Congress legislates against the backdrop of existing law.").[9]

(U) Because this Court lacks jurisdiction to review the applicability of the nondisclosure agreements or any other laws or regulations beyond FISA that restrict the disclosure of classified information, this Court should reject the companies' request for broad declaratory relief concerning such prohibitions.

[9] (U) An additional feature of FISA that counsels against a finding that the Court can exercise general declaratory powers pursuant to the DJA is the limited statutory appellate jurisdiction of the Foreign Intelligence Surveillance Court of Review. Unlike federal circuit courts of appeals, which have a general statutory grant of jurisdiction over all final judgments by district courts within their respective circuits, *see* 28 U.S.C. § 1291, FISA contains specific appellate provisions that vest the Court of Review with appellate jurisdiction over particular types of rulings from this Court. *See, e.g.*, 50 U.S.C. §§ 1803(b), 1822(d), 1861(f)(3), 1881a(h)(6)(A), 1881a(i)(4)(A), 1881b(f)(1), 1881c(e)(1). In an appropriate case, the Court of Review (like this Court) could issue an extraordinary writ pursuant to the All Writs Act, 28 U.S.C. § 1651.

[redacted]

[redacted]

(U) CONCLUSION

(U) For the reasons stated above, the Motions should be denied.

September 30, 2013

Respectfully submitted,

JOHN P. CARLIN
Acting Assistant Attorney General
for National Security

TASHINA GAUHAR
Deputy Assistant Attorney General
for Intelligence

CHRISTOPHER HARDEE
Chief Counsel for Policy
National Security Division

/s/ Nicholas J. Patterson
JEFFREY M. SMITH
NICHOLAS J. PATTERSON
U.S. Department of Justice
National Security Division
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530
Phone: (202) 514-5600
Fax: (202) 514-8053

Attorneys for the United States of America

[redacted]

[redacted]

(U) CERTIFICATE OF SERVICE

(U) I hereby certify that a true copy of the Response of the United States to Motions for Declaratory Judgment by Google Inc., Microsoft Corporation, Yahoo! Inc., Facebook, Inc., and Linkedin Corporation was served by hand-delivery on this 30th day of September, 2013, to Christine Gunning, Chief of Operations, Litigation Security Group, or her delegate, for forwarding to the Court. Additionally, redacted copies of the brief and accompanying declaration were served by the Government via Federal Express overnight delivery on this 30th day of September, 2013, addressed to:

Albert Gidari
Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101

Attorney for Google Inc.

James Garland
David N. Fagan
Alexander A. Berengaut
Covington & Burling LLP
1201 Pennsylvania Avenue, NW
Washington, DC 20004-2401

Attorneys for Microsoft Corporation

Marc J. Zwillinger
Jacob A. Sommer
ZwillGen PLLC
1705 N Street, NW
Washington, DC 20036

Attorneys for Yahoo! Inc.

[redacted]

[redacted]

Carl J. Nichols
Wilmer Cutler Pickering Hale and Dorr LLP
1875 Pennsylvania Avenue, NW
Washington, DC 20006

Attorney for Facebook, Inc.

Jerome C. Roth
Jonathan H. Blavin
Justin P. Raphael
Munger, Tolles & Olson LLP
560 Mission Street, 27th Floor
San Francisco, CA 94105

Attorneys for LinkedIn Corporation

/s/ Nicholas J. Patterson
Nicholas J. Patterson

[redacted]