

THE HONORABLE JAMES L. ROBERT

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

MICROSOFT CORPORATION,

Plaintiff,

v.

THE UNITED STATES DEPARTMENT
OF JUSTICE, and LORETTA LYNCH, in
her official capacity as the Attorney
General of the United States,

Defendant.

No. 16-CV-00538JLR

STIPULATED MOTION FOR LEAVE TO
FILE BRIEF *AMICUS CURIAE* OF
TWITTER, INC. IN SUPPORT OF
MICROSOFT CORPORATION'S
OPPOSITION TO DEFENDANT'S
MOTION TO DISMISS

Noted on Motions Calendar:
September 2, 2016

Twitter, Inc. ("Twitter") hereby moves for leave to file the attached Brief *Amicus Curiae* in Support of Plaintiff Microsoft Corporation's Opposition to Defendant's Motion to Dismiss. Consistent with the Court's guidance in its Order dated August 23, 2016 (Dkt. 42, at 3 n.1), both parties have consented to the filing of Twitter's proposed Brief *Amicus Curiae*.

I. THE PROPOSED AMICUS

Twitter is a global information sharing and distribution network serving over 310 million monthly active users around the world. People using Twitter write short messages, called "Tweets," of 140 characters or fewer, which are public by default and may be viewed all around the world instantly. As such, Twitter gives a public voice to anyone in the world—people who inform and educate others, who express their individuality, who engage in all manner of political speech, and who seek positive change.

1 Twitter is firmly committed to providing meaningful transparency to its users and the
2 public regarding governmental demands for user records. To that end, Twitter recently filed a
3 second amended complaint in a lawsuit against the Department of Justice and the Federal Bureau
4 of Investigation challenging indefinite gags on its ability to discuss or describe orders issued
5 pursuant to the Foreign Intelligence Surveillance Act. *Twitter v. Lynch*, No. 14-cv-4480-YGR,
6 Second Amended Complaint (N.D. Cal. May 24, 2016). Twitter is an electronic communications
7 service provider as that term is defined in the Electronic Communications Privacy Act, 18 U.S.C.
8 § 2510(15), and is therefore subject to nondisclosure orders issued pursuant to 18 U.S.C.
9 § 2705(b) (“Section 2705(b)”) and other governmental requests for account information.

10 **II. THE PROPOSED AMICUS OFFERS THE COURT A UNIQUE PERSPECTIVE**

11 Twitter’s proposed brief offers a unique perspective in three related ways. First, the brief
12 provides the Court with information, never before released, about the number and type of Section
13 2705(b) orders that Twitter has received. This information can give the Court a broader
14 understanding about how Section 2705(b) is used in practice. Second, the brief focuses on
15 technology and policy instead of law. It shows how the challenged Section 2705(b) operates as
16 the linchpin for secret government surveillance under the Stored Communications Act. Twitter
17 believes that this explanation can help the Court understand the legal arguments asserted by the
18 parties by placing the challenged provision in context. Third, the brief brings to the Court’s
19 attention the fact that the government regularly seeks unlimited nondisclosure orders in a variety
20 of contexts outside of Section 2705(b), and that a number of courts have recently rejected this
21 practice.

22 **III. CONCLUSION**

23 Because Twitter offers both “unique information [and] perspective that can help the
24 court” beyond what the parties have briefed, and because the issues before the Court “have
25 potential ramifications beyond the parties directly involved,” Twitter respectfully requests leave
26 to file the attached Brief *Amicus Curiae*. *Skokomish Indian Tribe v. Goldmark*, No. C13-

1 5071JLR, 2013 WL 5720053, at *1 (W.D. Wash. Oct. 21, 2013) (Robart, J.) (citing *NGV*
2 *Gaming, Ltd. v. Upstream Point Molate, LLC*, 355 F. Supp. 2d 1061, 1067 (N.D. Cal. 2005)); *see*
3 *also Neonatology Assocs., P.A. v. C.I.R.*, 293 F.3d 128, 132 (3d Cir. 2002) (Alito, J.) (“Even
4 when a party is very well represented, an amicus may provide important assistance to the court,”
5 including by “argu[ing] points deemed too far-reaching for emphasis by a party” or “explain[ing]
6 the impact a potential holding might have on an industry or other group”) (citation omitted).

7 DATED: September 2, 2016

8 By: /s/ Hayley L. Berlin
9 Michael A. Sussmann*
10 Hayley L. Berlin, WSBA #43566
11 Perkins Coie LLP
12 700 Thirteenth Street, N.W., Suite 600
13 Washington, D.C. 20005-3960
14 Telephone: (202) 654-6200
15 Facsimile: (202) 654-6211
16 Email: MSussmann@perkinscoie.com
17 HBerlin@perkinscoie.com

18 Orin S. Kerr*
19 Law Office of Orin S. Kerr
20 2000 H Street, NW
21 Washington, D.C. 20052
22 Telephone: (202) 994-4775
23 Facsimile: (202) 994-5654
24 Email: okerr@law.gwu.edu

25 **pro hac vice* application pending

26 *Attorneys for Twitter, Inc.*

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

CERTIFICATE OF SERVICE

I hereby certify that on September 2, 2016, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to the email addresses indicated on the Court’s Electronic Mail Notice List.

DATED: September 2, 2016

By: /s/Hayley L. Berlin
Hayley L. Berlin, WSBA No. 43566
Perkins Coie LLP
700 Thirteenth Street, N.W., Suite 600
Washington, D.C. 20005-3960
Telephone: (202) 654-6200
Facsimile: (202) 654-6211
Email: HBerlin@perkinscoie.com

Attorneys for Twitter, Inc.

THE HONORABLE JAMES L. ROBERT

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

MICROSOFT CORPORATION,

Plaintiff,

v.

THE UNITED STATES DEPARTMENT
OF JUSTICE, and LORETTA LYNCH, in
her official capacity as the Attorney
General of the United States,

Defendant.

No. 16-CV-00538JLR

BRIEF OF *AMICUS CURIAE* TWITTER,
INC. IN SUPPORT OF MICROSOFT
CORPORATION'S OPPOSITION TO
DEFENDANT'S MOTION TO DISMISS

TABLE OF CONTENTS

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

	Page
I. Statement of Interest of <i>Amicus Curiae</i>	1
II. Introduction.....	1
III. Disclosure Is Essential to Government Surveillance and Has Always Been the Standard Practice for Traditional Physical Searches	2
IV. Targets of Internet Surveillance Often Never Know That the Government Has Rifled Through Their Digital Lives	3
V. Gag Orders Under 18 U.S.C. § 2705(b) Are Trivially Easy to Obtain but Difficult to Challenge	6
VI. The Government’s Practice of Obtaining Indefinite Gag Orders Has Been Successfully Challenged, Including in the National Security Context	10
VII. Conclusion	12

TABLE OF AUTHORITIES

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

Page

CASES

Buckley v. Valeo,
424 U.S. 1 (1976).....2

Doe v. Holder,
703 F. Supp. 2d 313 (S.D.N.Y. 2010).....11

Grosjean v. Am. Press Co.,
297 U.S. 233 (1936).....2

Hudson v. Michigan,
547 U.S. 586 (2006).....2

In re Grand Jury Subpoena for: [Redacted]@yahoo.com,
79 F. Supp. 3d 1091 (N.D. Cal. 2015)8, 10

In re a Warrant to Search a Certain E-mail Account,
No. 14-2985, ___F.3d___, 2016 WL 3770056 (2d Cir. July 14, 2016)4

In re Application of the United States of America for an Order of Nondisclosure Pursuant to 18 U.S.C. § 2705(b), 45 F. Supp. 3d 1 (D.D.C. 2014)7, 8

In re Application of the United States for an Order Pursuant to 18 U.S.C. § 2705(b), 131 F. Supp. 3d 1266 (D. Utah. 2015)4

In re Grand Jury Subpoena, JK-15-029,
No. 15-35434, ___F.3d___, 2016 WL 3745541 (9th Cir. July 13, 2016)5

In re Nat’l Sec. Letter,
930 F. Supp. 2d 1064 (N.D. Cal. 2013)11

In re Nat’l Sec. Letter,
No. CIV. JKB-15-1180, ___ F. Supp. 3d ___, 2015 WL 10530413 (D. Md. Sept. 17, 2015)11

In re Nat’l Sec. Letters,
No. 16-518 (JEB), Memorandum Opinion and Order (D.D.C. July 25, 2016),
http://www.dcd.uscourts.gov/sites/dcd/files/16-518Opinion_Redacted.pdf11

TABLE OF AUTHORITIES
(continued)

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

<i>In re Nat'l Sec. Letters,</i> Nos. 11-cv-02173 SI, 3:11-cv-2667 SI, 3:13-mc-80089 SI, 3:13-cv-1165 SI, Order re: Renewed Petitions to Set Aside National Security Letters (N.D. Cal. Mar. 29, 2016), https://www.eff.org/files/2016/04/21/redactedorder42016.pdf	11
<i>In re Sealing & Non-Disclosure of Pen/Trap/2703(d) Orders,</i> 562 F. Supp. 2d 876 (S.D. Tex. 2008)	10
<i>In re Search Warrant for: [redacted]@hotmail.com,</i> 74 F. Supp. 3d 1184 (N.D. Cal. 2014)	10
<i>Merrill v. Lynch,</i> 151 F. Supp. 3d 342 (S.D.N.Y. 2015).....	11
<i>Twitter v. Lynch,</i> No. 14-04480-YGR (N.D. Cal.).....	1, 11
<i>United States v. Bach,</i> 310 F.3d 1063 (8th Cir. 2002)	4
<i>United States v. Bansal,</i> 663 F.3d 634 (3d Cir. 2011).....	5
<i>United States v. Freitas,</i> 800 F.2d 1451 (9th Cir. 1986)	3
<i>United States v. Warshak,</i> 631 F.3d 266 (6th Cir. 2010)	5
STATUTES	
18 U.S.C. § 2510(15)	1
18 U.S.C. § 2518(8)(d)	5
18 U.S.C. §§ 2701–12.....	4
18 U.S.C. § 2703(b)	5
18 U.S.C. § 2703(d)	8, 9
18 U.S.C. § 2705(b)	1, 2, 6, 7, 8, 9, 10

TABLE OF AUTHORITIES
(continued)

		Page
1		
2		
3	18 U.S.C. § 2705(b)(3)	7
4	18 U.S.C. § 2705(b)(5)	7
5	18 U.S.C. § 2709.....	11
6	18 U.S.C. § 2709(c)	11
7	18 U.S.C. § 3105.....	3
8	18 U.S.C. § 3123(d)	5, 10
9	18 U.S.C. § 3511.....	11
10		
11	RULES	
12	Fed. R. App. P. 29(c)(5).....	1
13	Fed. R. Crim. P. 41	5
14	Fed. R. Crim. P. 41(e)(2)(A)(ii).....	3
15	Fed. R. Crim. P. 41(f)(1)(B)–(C)	2
16	Fed. R. Crim. P. 41(f)(1)(C)	5
17	OTHER AUTHORITIES	
18	Louis D. Brandeis, <i>Other People’s Money and How the Bankers Use It</i> 62 (1933)	2
19	Orin S. Kerr, <i>The Next Generation Communications Privacy Act</i> , 162 U. Pa. L.	
20	Rev. 373 (2014)	6
21	Stephen Wm. Smith, <i>Gagged, Sealed & Delivered: Reforming ECPA’s Secret</i>	
22	<i>Docket</i> , 6 Harv. L. & Pol’y Rev. 313 (2012).....	4
23	U.S. Dep’t of Justice, <i>Searching and Seizing Computers and Obtaining Electronic</i>	
24	<i>Evidence in Criminal Investigations</i> 141 (2009),	
25	https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf	8
26	United States Courts, <i>Wiretap Report 2015</i> (last updated Dec. 31, 2015),	
	http://www.uscourts.gov/statistics-reports/wiretap-report-2015	5

I. Statement of Interest of *Amicus Curiae*¹

Twitter is a global information sharing and distribution network serving over 310 million monthly active users around the world. People using Twitter write short messages, called “Tweets,” of 140 characters or fewer, which are public by default and may be viewed all around the world instantly. As such, Twitter gives a public voice to anyone in the world—people who inform and educate others, who express their individuality, who engage in all manner of political speech, and who seek positive change.

Twitter is firmly committed to providing meaningful transparency to its users and the public regarding governmental demands for user records. To that end, Twitter has filed a second amended complaint in a lawsuit against the Department of Justice and the FBI challenging indefinite gags on its ability to discuss or describe orders issued pursuant to the Foreign Intelligence Surveillance Act. *Twitter v. Lynch*, No. 14-cv-4480-YGR, Second Amended Complaint (N.D. Cal. May 24, 2016). Twitter is an electronic communications service provider as that term is defined in the Electronic Communications Privacy Act, 18 U.S.C. § 2510(15), and is therefore subject to nondisclosure orders issued pursuant to Section 2705(b) and other governmental requests for account information.

II. Introduction

The challenged provision in this case, 18 U.S.C. § 2705(b), is the linchpin for secret government surveillance under the Stored Communications Act and it should trouble every Internet user. This brief explains why Section 2705(b) is at odds with the notice afforded in traditional physical-world searches and why its application in practice reduces user notice far beyond what is necessary. Providing meaningful notice to those whose information is accessed is critical to any system of government surveillance.¹ Although meaningful notice is the norm in physical search cases, Internet investigations are different, as the law rarely requires investigators

¹ No party or other person authored this brief, in whole or in part, or contributed funds for its preparation and submission. *See* Fed. R. App. P. 29(c)(5).

1 to notify subjects of Internet surveillance. And under Section 2705(b), investigators can and do
2 routinely gag Internet service providers from disclosing to their customers the fact of
3 government access. The gag orders are very easy to get and very difficult to challenge.
4 Therefore, Section 2705(b) is the key that allows the government to rifle through a suspect's
5 digital life without the suspect ever knowing the government was there.

6 **III. Disclosure Is Essential to Government Surveillance and Has Always Been the** 7 **Standard Practice for Traditional Physical Searches**

8 Disclosure is an essential component of any system of government surveillance.
9 “[I]nformed public opinion is the most potent of all restraints upon misgovernment.” *Grosjean v.*
10 *Am. Press Co.*, 297 U.S. 233, 250 (1936). “Sunlight is said to be the best of disinfectants; electric
11 light the most efficient policeman.” *Buckley v. Valeo*, 424 U.S. 1, 67 (1976) (quoting Louis D.
12 Brandeis, *Other People's Money and How the Bankers Use It* 62 (1933)). When government
13 surveillance remains hidden, the public cannot know what the government is doing on its behalf.
14 Meaningful notice thereby enables the identification and correction of government overreach.

15 In the context of traditional physical-world searches, disclosure is required both by
16 physics and by law. First, physical searches provide their own disclosure. When the police raid a
17 house, residents and neighbors can watch the search occur. They can see what the officers took
18 because seizing physical property requires its removal. Neighbors can see the officers cart the
19 property away. Even if no one is home, the signs of physical entry usually are clear. Residents
20 can know what the government took by cataloging what property is missing.

21 The law governing search warrants has long helped to make that physical disclosure
22 effective. It is an “ancient” principle of the common law, recognized by the Fourth Amendment,
23 “that law enforcement officers must announce their presence and provide residents an
24 opportunity to open the door” when executing a warrant. *Hudson v. Michigan*, 547 U.S. 586, 589
25 (2006). Officers must leave a copy of the warrant together with an inventory of what was taken
26 so targets can know what was taken and who took it. *See* Fed. R. Crim. P. 41(f)(1)(B)–(C).

1 Officers ordinarily must search in the daytime, which is a time they can be more easily observed.
2 *See* Fed. R. Crim. P. 41(e)(2)(A)(ii). The officers must be present to execute the warrant and
3 ordinarily cannot delegate the task to others. *See* 18 U.S.C. § 3105.

4 It is true that notice for physical searches may sometimes be delayed. *See, e.g., United*
5 *States v. Freitas*, 800 F.2d 1451, 1456 (9th Cir. 1986) (permitting so-called “sneak and peek”
6 warrants). However, the Ninth Circuit has made clear that the period of delay must be very short:
7 “[E]xcept upon a strong showing of necessity,” notice cannot exceed seven days. *Id.* The limited
8 period of delay reflects the universally-recognized importance of notice in the physical search
9 context:

10 [S]urreptitious searches and seizures of intangibles strike at the
11 very heart of the interests protected by the Fourth Amendment.
12 The mere thought of strangers walking through and visually
13 examining the center of our privacy interest, our home, arouses our
passion for freedom as does nothing else. That passion, the true
source of the Fourth Amendment, demands that surreptitious
entries be closely circumscribed.

14 *Id.*

15 **IV. Targets of Internet Surveillance Often Never Know That the Government Has 16 Rifled Through Their Digital Lives**

17 Disclosure of online government surveillance is strikingly different from disclosure of
18 physical surveillance. When the government obtains a target’s e-mail instead of mail, or when it
19 rifles through a suspect’s virtual locker instead of his physical locker, the subjects of the searches
20 usually never know about it. American citizens can have their entire digital lives sifted through
21 by government agents and will never know they were even suspects.

22 This is true for reasons of both technology and law. First, Internet technology renders
23 online evidence collection invisible to everyone but investigators who obtain court orders and the
24 companies required by law to execute them. The Internet equivalent of our homes consists of
25 storage space on computer servers run by third-party providers such as Dropbox, Google,
26 Microsoft and Twitter. When investigators wish to search virtual homes to seize private

1 information, they typically go to the providers that store the information rather than the users
2 who own it. *See, e.g., United States v. Bach*, 310 F.3d 1063 (8th Cir. 2002).

3 Instead of executing the searches themselves, investigators in Internet cases obtain
4 warrants ordering the providers to act on their behalf. *See generally In re a Warrant to Search a*
5 *Certain E-mail Account*, No. 14-2985, ___F.3d___, 2016 WL 3770056 (2d Cir. July 14, 2016).
6 The searches can occur far away from users, and communications are seized by merely taking
7 copies of them rather than by removing the original communications. *See id.* In this way, the
8 technology allows government access to remain shielded from view.

9 Because of this technological reality, individual users who are subject to government
10 searches will receive notice only if the government or the companies provide it. But in contrast
11 to the law of physical searches, the law of digital searches makes disclosure of government
12 access the exception rather than the rule. As Magistrate Judge Stephen Smith (S.D. Tex.) has
13 explained, after the government obtains its court orders, those orders can “all but vanish into a
14 legal void:”

15 It is as if they were written in invisible ink—legible to the phone
16 companies and Internet service providers who execute them, yet
17 imperceptible to unsuspecting targets, the general public, and even
18 other arms of government, most notably Congress and the
19 appellate courts.

20 Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA’s Secret Docket*, 6 Harv. L.
21 & Pol’y Rev. 313, 314 (2012).

22 Existing law almost never requires the government to notify users of searches and
23 seizures of their Internet communications. The primary statutory means to obtain a user’s
24 communications, the Stored Communication Act (“SCA”), 18 U.S.C. §§ 2701–12, imposes no
25 notice requirement on the government. When the government compels non-content information,
26 or when it compels content and obtains the warrant required by the Fourth Amendment, the SCA
does not require user notice. *See In re Application of the United States for an Order Pursuant to*

1 18 U.S.C. § 2705(b), 131 F. Supp. 3d 1266, 1271 (D. Utah. 2015) (summarizing the notice
2 requirements of the SCA).

3 The SCA requires notice only in one idiosyncratic situation: when the government
4 compels contents of communications without a warrant. 18 U.S.C. § 2703(b). This amounts to no
5 notice requirement at all, however, as this procedure has been ruled unconstitutional. *See United*
6 *States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010). *See also In re Grand Jury Subpoena, JK-*
7 *15-029*, No. 15-35434, ___F.3d___, 2016 WL 3745541, at *5 (9th Cir. July 13, 2016) (“[E]mails
8 are to be treated as closed, addressed packages for expectation-of-privacy purposes”). Federal
9 Rule of Criminal Procedure 41 (“Rule 41”) does not require notice to the user, either. Rule 41
10 has a notice provision mandating notice “to the person from whom, or from whose premises, the
11 property was taken.” Fed. R. Crim. P. 41(f)(1)(C). Courts have held that this requirement is met
12 by alerting the third-party provider that it must assist with the execution of the warrant. If Rule
13 41 applies, it does not require notice to the customer. *See United States v. Bansal*, 663 F.3d 634,
14 662–63 (3d Cir. 2011) (holding Rule 41 satisfied when “the warrant was provided to the internet
15 service providers upon whom the search warrants were executed”).

16 When the government conducts real-time surveillance of communications instead of
17 accessing stored communications under the SCA, notice is required only when the government
18 intercepts the *contents* of communications pursuant to a Wiretap Act order. *Compare* 18 U.S.C.
19 § 2518(8)(d), *with* 18 U.S.C. § 3123(d) (imposing sealing requirements and gag orders for non-
20 content surveillance using pen registers and/or trap and trace devices). The Wiretap Act
21 generally requires that the subjects of monitoring be informed about the court order and whether
22 their communications were monitored. *See* 18 U.S.C. § 2518(8)(d). This requirement is more
23 theoretical than real, however, because wiretaps for electronic communications are relatively
24 rare. *See United States Courts, Wiretap Report 2015* (last updated Dec. 31, 2015),
25 <http://www.uscourts.gov/statistics-reports/wiretap-report-2015> (reporting that in 2015, federal
26 and state governments nationwide obtained only 32 Wiretap Orders to intercept electronic

1 communications). Because electronic communications are often saved and stored, the
2 government can and usually does evade the burdensome requirements of the Wiretap Act
3 (including its notice requirement) by instead obtaining orders for stored communications under
4 the SCA. *See* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. Pa. L.
5 Rev. 373, 393–94 (2014).

6 **V. Gag Orders Under 18 U.S.C. § 2705(b) Are Trivially Easy to Obtain but Difficult to**
7 **Challenge**

8 In light of the foregoing, the only way most users will receive notice of government
9 access under the SCA is if the providers give it. Twitter notifies affected users of requests for
10 their account information prior to disclosure unless prohibited or the request falls into one of the
11 exceptions to Twitter’s user notice policy.² Twitter may also provide post-disclosure notice to
12 affected users when prior notice is prohibited. Disclosure is essential to customer trust, and
13 providers value the relationship of trust with their customers. Notice is essential to allow
14 customers to raise legal privileges against disclosure or to challenge government overreach. But
15 providers can notify users only if they are legally permitted to do so. Section 2705(b) thus
16 provides the linchpin for secrecy under the SCA by making gag orders trivially easy for the
17 government to obtain and correspondingly difficult for providers to challenge.

18 Consider the low legal standard for obtaining gag orders. Under Section 2705(b), the
19 government can obtain an order forbidding providers to disclose legal process if there is “reason
20 to believe” that notice will result in one of five harms:

- 21 (1) endangering the life or physical safety of an individual;
- 22 (2) flight from prosecution;
- 23 (3) destruction of or tampering with evidence;
- 24 (4) intimidation of potential witnesses; or
- 25 (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

26 ² Exceptions include exigent or counterproductive circumstances (*e.g.*, emergencies; account compromises).

1 The gag order can be imposed “for such period as the court deems appropriate,” without any
2 statutorily imposed limit. 18 U.S.C. § 2705(b). The procedure is undertaken *ex parte*, and the
3 provider who will be gagged is not invited to participate. *See In re Application of the United*
4 *States of America for an Order of Nondisclosure Pursuant to 18 U.S.C. § 2705(b)*, 45 F. Supp.
5 3d 1, 5–6 (D.D.C. 2014).

6 This statutory standard is so low that the government can meet it in nearly any
7 investigation. Because the government is not required to notify targets of surveillance, most
8 targets of surveillance will not know that the government is watching them. Tipping off a suspect
9 that they are being watched will almost always create a “reason to believe” that the target will
10 somehow respond in a manner described in Section 2705(b). For example, the target may
11 respond by taking steps to avoid future surveillance, thus “seriously jeopardizing” the
12 investigation, 18 U.S.C. § 2705(b)(5), or a target who has engaged in wrongdoing may delete or
13 alter potentially incriminating files, thus “tampering with evidence,” *id.* § 2705(b)(3). Gag orders
14 are therefore readily obtained as a matter of routine.

15 The government’s motion to dismiss in this case practically concedes as much:

16 [B]ecause . . . requests for information under 2703 are often made
17 at early stages of a case . . . , [and] the evidence involved is
18 electronic and therefore can be altered, or destroyed easily, it is
19 unsurprising that the Government frequently may point to
20 destruction of evidence as a likely outcome if an order is disclosed
21 to a user.

22 Motion to Dismiss at 18 n.13. “[T]he absence of case specific facts” is common because the
23 reasons for the gag order are generic and “the manner in which these harms inure from disclosure
24 in one case may parallel another.” *Id.* In Twitter’s experience, when presented with facts that
25 would suggest that notice would not present danger—such as the target of the investigation
26 already being aware of the investigation because of news coverage—the government has
27 nonetheless maintained the need for nondisclosure. The norm is secrecy, and the standard of
28 Section 2705(b) is so low that no specific facts are needed to maintain the secrecy norm.

1 Because the government can meet this standard in nearly any investigation, it can simply
2 add a routine request for a gag order to its application for a search warrant or production order
3 under Section 2703(d). Indeed, the Justice Department’s guide to the Stored Communications
4 Act recommends this practice. “If the relevant process is a 2703(d) order or 2703 warrant,” it
5 explains, “agents can simply include appropriate language in the application and proposed order
6 or warrant.” U.S. Dep’t of Justice, Searching and Seizing Computers and Obtaining Electronic
7 Evidence in Criminal Investigations 141 (2009) (“DOJ Manual”),
8 <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf>.
9 The DOJ Manual offers the following entirely generic “appropriate language” as a model to
10 include in the government’s application:

11 The United States requests that pursuant to the preclusion of notice
12 provisions of 18 U.S.C. § 2705(b), ISPCCompany be ordered not to
13 notify any person (including the subscriber or customer to which
14 the materials relate) of the existence of this Order for such period
15 as the Court deems appropriate. The United States submits that
16 such an order is justified because notification of the existence of
17 this Order would seriously jeopardize the ongoing investigation.
18 Such a disclosure would give the subscriber an opportunity to
19 destroy evidence, change patterns of behavior, notify confederates,
20 or flee or continue his flight from prosecution.

21 *Id.* at 218–19.

22 Finally, a gag order is difficult to challenge once in place. Certainly the government will
23 not do so: “[W]hat reason would the government ever have to request lifting the order?” *In re*
24 *Grand Jury Subpoena for: [Redacted]@yahoo.com*, 79 F. Supp. 3d 1091, 1094 (N.D. Cal. 2015).
25 A provider may wish to notify its users as soon as possible, but it will lack the necessary facts.
26 *See id.* (noting that the government “uniquely has access to the underlying facts of the
investigation” that justify Section 2705(b) notice). The provider will not know whether the
investigation has reached a point at which disclosure no longer serves the statutory standard. *See*
In re Application of the United States, 45 F. Supp. 3d at 6 (“Because the government controls the

1 scope of the criminal investigation, the government is better equipped to provide information
2 about potential compromises to the ongoing criminal investigation than is the service provider.”).

3 In sum, the government routinely employs Section 2705(b) to prohibit service providers
4 from giving their users notice that they have been the targets of government surveillance—notice
5 that is crucial to monitoring the *government’s* conduct. The standard for an unlimited gag order
6 is so low that it can be met in almost every case. Once entered, the gag order will tend to stay in
7 place. The government lawyer that knows enough to challenge the order will not, while the
8 provider that will want to challenge the order usually will not know enough to do so.

9 Twitter’s experience echoes these concerns. In the period combining 2015 and the first
10 half of 2016, Twitter received legal process to compel customer information under the Stored
11 Communications Act a total of 6,432 times. Of those, 3,315 were accompanied by gag orders
12 under Section 2705(b). Another 784 were accompanied by gag orders under state authorities
13 such as state equivalents of the Stored Communications Act. In other words, legal process
14 seeking to compel disclosure was accompanied by a gag order 64% of the time, with 52% of
15 legal process coming with a gag order specifically under Section 2705(b).

16 Further, when the government obtained gag orders under Section 2705(b), the non-
17 disclosure was indefinite in duration 47% of the time, reflecting 1,565 out of 3,315 cases. This
18 rate varied depending on the type of compelled legal process received under the Stored
19 Communications Act. Gag orders under Section 2705(b) were indefinite 63% of the time that
20 they accompanied search warrants (83/131); 33% of the time that they accompanied 18 U.S.C.
21 § 2703(d) court orders (146/436); and 49% of the time that they accompanied subpoenas
22 (1,336/2,748).³ The high percentage of Section 2705(b) orders accompanying subpoenas is
23 particularly noteworthy because the government, which can otherwise issue subpoenas without
24 the court’s approval, must separately seek a court order mandating nondisclosure. As these
25

26 ³ These numbers do not account for all non-binding requests to not provide user notice that Twitter received from the government.

1 numbers show, gag orders are the norm rather than the exception. And about as often as not, the
2 orders are imposed for an indefinite duration.

3 **VI. The Government’s Practice of Obtaining Indefinite Gag Orders Has Been**
4 **Successfully Challenged, Including in the National Security Context**

5 Microsoft’s challenge to Section 2705 is just one example of a number of recent
6 challenges to a broader governmental practice of seeking gag orders of unlimited duration related
7 to electronic surveillance. Many of these challenges have succeeded, with courts finding that
8 unlimited gags run afoul of the First Amendment.

9 In a number of recent cases, judges have rejected government requests for indefinite
10 nondisclosure obligations under Section 2705. *See In re Grand Jury Subpoena for:*
11 *[Redacted]@yahoo.com*, 79 F. Supp. 3d at 1091 (“[R]ather than requesting that Yahoo! be
12 gagged for 60 days, 90 days or some other fixed period, the government wants Yahoo! gagged
13 ‘until further order of the Court.’ Because such an indefinite order would amount to an undue
14 prior restraint of Yahoo!’s First Amendment right to inform the public of its role in searching
15 and seizing its information, the court DENIES the government’s [Section 2705(b)]
16 application.”); *In re Search Warrant for: [redacted]@hotmail.com*, 74 F. Supp. 3d 1184, 1186
17 (N.D. Cal. 2014) (denying application under Section 2705 for nondisclosure of unlimited
18 duration, and holding that federal law “clearly requires the court to define some end. That end
19 could come in less than 90 days, 90 days exactly or even more than 90 days”); *In re Sealing &*
20 *Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F. Supp. 2d 876, 877–78, 895 (S.D. Tex.
21 2008) (holding that “neither 18 U.S.C. § 2705(b) nor § 3123(d) may be interpreted to permit a
22 gag order of unlimited duration,” and noting that “[a]s a rule, sealing and non-disclosure of
23 electronic surveillance [demands] must be neither permanent nor, what amounts to the same
24 thing, indefinite”).

25 Service providers have successfully challenged unlimited gag orders associated with
26

1 national security letters (“NSLs”) issued pursuant to 18 U.S.C. § 2709.⁴ *See, e.g., In re Nat’l Sec.*
 2 *Letters*, No. 16-518 (JEB), Memorandum Opinion and Order (D.D.C. July 25, 2016),
 3 http://www.dcd.uscourts.gov/sites/dcd/files/16-518Opinion_Redacted.pdf (rejecting government
 4 request for nondisclosure of unlimited duration, and instead imposing triennial review of NSL
 5 nondisclosure provisions); *In re Nat’l Sec. Letters*, Nos. 11-cv-02173 SI, 3:11-cv-2667 SI, 3:13-
 6 mc-80089 SI, 3:13-cv-1165 SI, Order re: Renewed Petitions to Set Aside National Security
 7 Letters (N.D. Cal. Mar. 29, 2016), <https://www.eff.org/files/2016/04/21/redactedorder42016.pdf>
 8 (lifting nondisclosure provision relating to one NSL upon finding that the government failed to
 9 meet its burden for continued nondisclosure under 18 U.S.C. § 3511); *In re Nat’l Sec. Letter*, No.
 10 CIV. JKB-15-1180, ___ F. Supp. 3d ___, 2015 WL 10530413 (D. Md. Sept. 17, 2015)
 11 (modifying NSL nondisclosure provision to avoid nondisclosure provision of “infinite duration,”
 12 which the court found to be “problematic”); *Merrill v. Lynch*, 151 F. Supp. 3d 342 (S.D.N.Y.
 13 2015) (lifting nondisclosure requirement relating to attachment to an NSL upon finding that the
 14 government failed to meet its burden for continued nondisclosure under 18 U.S.C. § 3511); *Doe*
 15 *v. Holder*, 703 F. Supp. 2d 313 (S.D.N.Y. 2010) (permitting disclosure of two categories of
 16 information contained in attachment to NSL).

17 Finally, Twitter has challenged nondisclosure orders of unlimited duration associated
 18 with orders issued under the Foreign Intelligence Surveillance Act (“FISA”) in a case currently
 19 pending in the Northern District of California.⁵ *See Twitter v. Lynch*, No. 14-cv-4480-YGR,

20 _____
 21 ⁴ The FBI can issue NSLs to service providers with nondisclosure orders of unlimited duration unilaterally
 22 and without judicial review. 18 U.S.C. § 2709(c). These nondisclosure orders apply both to the contents of the NSL
 23 and to the very fact of having received an NSL. *See In re Nat’l Sec. Letter*, 930 F. Supp. 2d 1064, 1075, 1077 (N.D.
 24 Cal. 2013). According to transparency reports issued by the Office of the Director of National Intelligence, the FBI
 25 issued 19,212 NSLs in 2013, 16,348 NSLs in 2014, and 12,870 NSLs in 2015. DNI Transparency Reports, Exs. 1–3.

26 ⁵ Five subsections of FISA (“Titles”) permit the government to seek real-time surveillance or disclosure of
 stored records from a service provider: Title I (electronic surveillance of the content of communications and all
 communications metadata); Title III (disclosure of stored content and noncontent records); Title IV (provisioning of
 pen register and trap and trace devices to obtain dialing, routing, addressing, and signaling information); Title V
 (disclosure of certain “business records”) (also referred to as “Section 215 of the USA PATRIOT Act”); and Title
 VII (surveillance of non-U.S. persons located beyond U.S. borders). According to transparency reports issued by the
 Office of the Director of National Intelligence, in 2013, 2014, and 2015, the government issued, under Titles I, III,
 IV, and VII, over 1,500 FISA orders annually, and over 90,000 targets were affected by those orders each year. DNI

1 Second Amended Complaint (N.D. Cal. May 24, 2016) (ongoing litigation challenging
2 government prohibitions on speech regarding the amount of national security legal process
3 received from the Foreign Intelligence Surveillance Court, including FISA nondisclosure orders
4 of unlimited duration).

5 These legal challenges, and the decisions recognizing the unconstitutionality of
6 nondisclosure obligations of unlimited duration, stand as testament for the need to stem the
7 government's routine practice of unlimited gagging when engaging in electronic surveillance.

8 **VII. Conclusion**

9 The Court should deny the government's Motion to Dismiss.

10
11 DATED: September 2, 2016

12 By: /s/ Hayley L. Berlin

13 Michael A. Sussmann*

14 Hayley L. Berlin, WSBA #43566

15 Perkins Coie LLP

16 700 Thirteenth Street, N.W., Suite 600

17 Washington, D.C. 20005-3960

18 Telephone: (202) 654-6200

19 Facsimile: (202) 654-6211

20 Email: MSussmann@perkinscoie.com

21 HBerlin@perkinscoie.com

22 Orin S. Kerr*

23 Law Office of Orin S. Kerr

24 2000 H Street, NW

25 Washington, D.C. 20052

26 Telephone: (202) 994-4775

Facsimile : (202) 994-5654

Email: okerr@law.gwu.edu

**pro hac vice application pending*

Attorneys for Twitter, Inc.

25 Transparency Reports, Exs. 1–3. A target is defined as “an individual person, a group, or an organization composed
26 of multiple individuals or a foreign power that possesses or is likely to communicate foreign intelligence
information that the U.S. government is authorized to acquire” under FISA. *Id.* These numbers do not take into
account applications submitted under Title V of FISA, which were numerous (178 in 2013, 170 in 2014, and 142 in
2015) and affected hundreds of individuals each year. *Id.*

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

CERTIFICATE OF SERVICE

I hereby certify that on September 2, 2016, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to the email addresses indicated on the Court’s Electronic Mail Notice List.

DATED: September 2, 2016

By: /s/Hayley L. Berlin
Hayley L. Berlin, WSBA No. 43566
Perkins Coie LLP
700 Thirteenth Street, N.W., Suite 600
Washington, D.C. 20005-3960
Telephone: (202) 654-6200
Facsimile: (202) 654-6211
Email: HBerlin@perkinscoie.com

Attorneys for Twitter, Inc.

Exhibit 1

~~TOP SECRET//NOFORN~~



Office of the Director of National Intelligence

Statistical Transparency Report Regarding use of
National Security Authorities

Annual Statistics for Calendar Year 2013

~~Classified By: 2381928
Derived From: ODNI COL T-12
Reason:
Declassify On: 20391231~~

~~TOP SECRET//NOFORN~~

Statistical Transparency Report Regarding use of National Security Authorities

June 26, 2014

Introduction.

In June 2013, President Obama directed the Intelligence Community to declassify and make public as much information as possible about certain sensitive U.S. Government surveillance programs while protecting sensitive classified intelligence and national security information. Over the past year, the Director of National Intelligence (DNI) has declassified and authorized the public release of thousands of pages of documents relating to the use of critical national security authorities. Today, and consistent with the DNI's directive on August 29, 2013, we are releasing information related to the use of these important tools, and will do so in the future on an annual basis. Accordingly, the DNI has declassified and directed the release of the following information for calendar year 2013.

Annual Statistics for Calendar Year 2013 Regarding Use of Certain National Security Legal Authorities.

Titles I, III, IV, and VII of FISA.

Legal Authority	Annual Number of Orders	Estimated Number of Targets Affected
FISA Orders based on probable cause (Title I and III of FISA, Sections 703 and 704 of FISA)	1,767 orders	1,144
Section 702 of FISA	1 order	89,138
FISA Pen Register/Trap and Trace (Title IV of FISA)	131 orders	319

It is important to provide some additional context to the above statistics.

- **Targets.** Within the Intelligence Community, the term "target" has multiple meanings. For example, "target" could be an individual person, a group, or an organization composed of multiple individuals or a foreign power that possesses or is likely to communicate foreign intelligence information that the U.S. government is authorized to acquire by the above-referenced laws. Some laws require that the government obtain a Court order specifying the communications facilities used by a "target" to be subject to intelligence collection. Although the government may have legal authority to conduct intelligence collection against multiple communications facilities used by the target, the user of the facilities - the "target" - is only counted once in the above figures.

~~TOP SECRET//NOFORN~~

- **702 Targets.** In addition to the explanation of target above, in the context of Section 702 the term “target” is generally used to refer to the act of intentionally directing intelligence collection at a particular person, a group, or organization. For example, the statutory provisions of Section 702 state that the Government “may not *intentionally target any person* known at the time of the acquisition to be located in the United States” (emphasis added), among other express limitations. Under Section 702, the Foreign Intelligence Surveillance Court (FISC) approves Certifications as opposed to individualized orders. Thus, the number of 702 “targets” reflects an estimate of the number of known users of particular facilities (sometimes referred to as selectors) subject to intelligence collection under those Certifications. This estimate is based on the information readily available to the Intelligence Community to identify unique targets – users, whose identity may be unknown, but who are reasonably believed to use the particular facility from outside the United States and who are reasonably believed to be non-United States persons. For example, foreign intelligence targets often communicate using several different email accounts. Unless the Intelligence Community has information that multiple email accounts are used by the same target, each of those accounts would be counted separately in these figures. On the other hand, if the Intelligence Community is aware that the accounts are all used by the same target, as defined above, they would be counted as one target.
- **Relationship of Orders to Targets.** In some cases, one order can by its terms affect multiple targets (as with Section 702). Alternatively, a target may be the subject of multiple orders, as noted below.
- **Amendments and Renewals.** The FISC may amend an order one or more times after it has been issued. For example, an order may be amended to add a newly discovered account used by the target. To avoid redundant counting, these statistics do not count such amendments separately. Moreover, some orders may be renewed multiple times during the calendar year (for example, the FISA statute provides that a Section 704 FISA Order against a U.S. person target may last no longer than 90 days but permits the order to be renewed). The statistics count each such renewal as a separate order.

Title V of FISA (Business Records).

We are reporting information about the Government’s use of the FISA Business Records provision (Title V) separately because this authority has been used in two distinct ways – collection of business records to obtain information about a specific subject and collection of business records in bulk. Accordingly, in the interest of transparency, we have decided to clarify the extent to which individuals are affected by each use. In addition, instead of reporting on the number of Business Record orders, the government is reporting on the number of *applications* submitted to the Foreign Intelligence Surveillance Court because the FISC may issue several orders to different recipients based upon a particular application.

~~TOP SECRET//NOFORN~~

Legal Authority	Annual Number of Applications	Estimated Number Affected
FISA Business Records (Title V of FISA)	178	172: The number of individuals, entities, or foreign powers subject to a business records application to obtain information about a specific subject
		423: The number of selectors approved to be queried under the NSA telephony metadata program
		248: The number of known or presumed U.S. persons who were the subject of queries of information collected in bulk or who were subject to a business records application.

National Security Letters.

Finally, we are reporting information on the Government’s use of National Security Letters (NSLs). On April 30, 2014, the Department of Justice released its Annual Foreign Intelligence Surveillance Act Report to Congress. That report, which is [available here](#) reports on the number of requests made for certain information concerning different United States persons pursuant to NSL authorities during calendar year 2013. In addition to those figures, today we are reporting (1) the total number of NSLs issued for all persons, and (2) the total number of requests for information contained within those NSLs. For example, one NSL seeking subscriber information from one provider may identify three e-mail addresses, all of which are relevant to the same pending investigation and each is considered a “request.”

We are reporting the annual number of requests rather than “targets” for multiple reasons. First, the FBI’s systems are configured to comply with Congressional reporting requirements, which do not require the FBI to track the number of individuals or organizations that are the subject of an NSL. Even if the FBI systems were configured differently, it would still be difficult to identify the number of specific individuals or organizations that are the subjects of NSLs. One reason for this is that the subscriber information returned to the FBI in response to an NSL may identify, for example, one subscriber for three accounts or it may identify different subscribers for each account. In some cases this occurs because the identification information provided by the subscriber to the provider may not be true. For example, a subscriber may use a fictitious name or alias when creating the account. Thus, in many instances, the FBI never identifies the actual subscriber of a facility. In other cases this occurs because individual

~~TOP SECRET//NOFORN~~

subscribers may identify themselves differently for each account, e.g., inclusion of middle name, middle initial, etc., when creating an account.

We also note that the actual number of individuals or organizations that are the subject of an NSL is different than the number of NSL requests. The FBI often issues NSLs under different legal authorities, e.g., 12 U.S.C. § 3414(a)(5), 15 U.S.C. §§ 1681u(a) and (b), 15 U.S.C. § 1681v, and 18 U.S.C. § 2709, for the same individual or organization. The FBI may also serve multiple NSLs for an individual for multiple facilities, e.g., multiple e-mail accounts, landline telephone numbers, cellular phone numbers, etc. The number of requests, consequently, is significantly larger than the number of individuals or organizations that are the subjects of the NSLs.

Legal Authority	Annual Number of NSLs Issued	Annual Number of Requests for Information
National Security Letters issued pursuant to 12 U.S.C. § 3414(a)(5), 15 U.S.C. §§ 1681u(a) and (b), 15 U.S.C. § 1681v, and 18 U.S.C. § 2709	19,212	38,832

This information will be available at the website of the Office of the Director of National Intelligence (ODNI); and ODNI's public website dedicated to fostering greater public visibility into the intelligence activities of the Government, ICOntheRecord.tumblr.com.

~~TOP SECRET//NOFORN~~

Exhibit 2

UNCLASSIFIED

Statistical Transparency Report Regarding use of National Security Authorities

April 22, 2015

Introduction.

In June 2013, President Obama directed the Intelligence Community to declassify and make public as much information as possible about certain sensitive U.S. government surveillance programs while protecting sensitive classified intelligence and national security information. Since then, the Director of National Intelligence (DNI) has declassified and authorized the public release of thousands of pages of documents relating to the use of critical national security authorities. In addition to declassifying and publicly releasing these documents, the DNI and the Intelligence Community have published several reports regarding these authorities, including a first-of-its-kind report on June 26, 2014, presenting statistics on how often the government used certain authorities during calendar year 2013.

Today, and consistent with the Intelligence Community's *Principles of Intelligence Transparency*, we are releasing our second annual report presenting statistics on how often the government uses these important authorities. Accordingly, the DNI has declassified and directed the release of the following information covering calendar year 2014.

Annual Statistics for Calendar Year 2014 regarding Use of Certain National Security Legal Authorities.

Titles I, III, IV, and VII of FISA.

Legal Authority	Annual Number of Orders	Estimated Number of Targets Affected
FISA Orders based on probable cause (Title I and III of FISA, Sections 703 and 704 of FISA)	1519 orders	1562
Section 702 of FISA	1 order	92707
FISA Pen Register/Trap and Trace (Title IV of FISA)	135 orders	516

UNCLASSIFIED

It is important to provide some additional context to the above statistics.

- **Targets.** Within the Intelligence Community, the term “target” has multiple meanings. For example, a “target” could be an individual person, a group, or an entity composed of multiple individuals or a foreign power that possesses or is likely to communicate foreign intelligence information that the U.S. government is authorized to acquire by the above-referenced laws. Some laws require that the government obtain a court order specifying the communications facilities (e.g., a telephone number, an email address) used by a “target” to be subject to intelligence collection. Although the government may have legal authority to conduct intelligence collection against multiple communications facilities used by the target, the user of the facilities – the “target” – is only counted once in the above figures.
- **702 Targets.** In addition to the explanation of target above, in the context of Section 702 the term “target” is generally used to refer to the *act* of intentionally directing intelligence collection at a particular person, a group, or entity. For example, the statutory provisions of Section 702 state that the Government “may not *intentionally target any person* known at the time of the acquisition to be located in the United States” (emphasis added), among other express limitations. Under Section 702, the Foreign Intelligence Surveillance Court (FISC) approves Certifications as opposed to individualized orders. In the Section 702 context, the Intelligence Community targets a particular person, group, or entity by “tasking” selectors, pursuant to targeting procedures approved by the FISC. Selectors are specific communications facilities assessed to be used by a target (e.g., an email address or telephone number). Given the restrictions of Section 702, only selectors used by non-U.S. persons reasonably believed to be located outside the United States and who possess, or who are likely to communicate or receive, foreign intelligence information that is covered by an approved certification may be tasked.

The number of 702 “targets” therefore reflects an estimate of the number of known users of particular selectors. This estimate is based on the information readily available to the Intelligence Community to identify unique targets – users whose identity may be unknown but who are reasonably believed to use the particular selector from outside the United States and who are reasonably believed to be non-United States persons. For example, foreign intelligence targets often communicate using several different email accounts. Each email account is a different selector, so unless the Intelligence Community has information that multiple email accounts are used by the same target, each of those accounts, i.e., selectors, would be counted separately in these figures. On the other hand, if the Intelligence Community is aware that multiple accounts, i.e. selectors, are all used by the same target, as defined above, they would be counted as one target. This method of estimating helps ensure that the Intelligence Community does not inadvertently understate the number of discrete persons targeted pursuant to Section 702.

UNCLASSIFIED

UNCLASSIFIED

- **Relationship of Orders to Targets.** In some cases, one order can by its terms affect multiple targets (as with Section 702). Alternatively, a target may be the subject of multiple orders, as noted below.
- **Amendments and Renewals.** The FISC may amend an order one or more times after it has been issued. For example, an order may be amended to add a newly discovered account used by the target. To avoid redundant counting, these statistics do not count such amendments separately. Moreover, some orders may be renewed multiple times during the calendar year (for example, the FISA statute provides that a Section 704 FISA order against a U.S. person target may last no longer than 90 days but permits the order to be renewed). Unlike amendments, the statistics count each such renewal as a separate order.

Title V of FISA (Business Records).

We are reporting information about the government's use of the FISA Business Records provision (Title V) separately because this authority has been used in two distinct ways – collection of business records to obtain information about a specific subject and collection of business records in bulk. Accordingly, in the interest of transparency, we have decided to clarify the extent to which individuals are affected by each use. In addition, instead of reporting on the number of Business Records orders, the government is reporting on the number of approved *applications* submitted to the FISC because the FISC may issue several orders to different recipients based upon a particular application.

UNCLASSIFIED

UNCLASSIFIED

Legal Authority	Annual Number of Approved Applications	Estimated Number Affected
FISA Business Records (Title V of FISA)	170	160: The number of individuals, entities, or foreign powers subject to a business records application to obtain information about a specific subject.
		161: The number of selectors approved by the FISC to be queried under the NSA telephony metadata program.
		227: The number of known or presumed U.S. persons who were the subject of queries of information collected in bulk or who were subject to a business records application.

National Security Letters.

Finally, we are reporting information on the government's use of National Security Letters (NSLs). On April 21, 2015, the Department of Justice released its [Annual Foreign Intelligence Surveillance Act Report](#) to Congress. That report provides the number of requests made for certain information concerning different United States persons pursuant to NSL authorities during calendar year 2014. In addition to those figures, today we are reporting (1) the total number of NSLs issued for all persons, and (2) the total number of requests for information contained within those NSLs. For example, one NSL seeking subscriber information from one provider may identify three e-mail addresses, all of which are relevant to the same pending investigation and each is considered a "request."

We are reporting the annual number of requests rather than "targets" for multiple reasons. First, the FBI's systems are configured to comply with Congressional reporting requirements, which do not require the FBI to track the number of individuals or organizations that are the subject of an NSL. Second, even if the FBI systems were configured differently, it would still be difficult to identify the number of specific individuals or organizations that are the subjects of NSLs. One reason for this is that the subscriber information returned to the FBI in response to an NSL may identify, for example, one subscriber for three accounts or it may identify different subscribers for each account. In some cases this occurs because the identification information provided by the subscriber to the provider may not be true. For example, a subscriber may use

UNCLASSIFIED

UNCLASSIFIED

a fictitious name or alias when creating the account. Thus, in many instances, the FBI never identifies the actual subscriber of a facility. In other cases this occurs because individual subscribers may identify themselves differently for each account (e.g., by including a middle name or middle initial) when creating an account.

We also note that the actual number of individuals or organizations that are the subject of an NSL is different than the number of NSL requests. The FBI often issues NSLs under different legal authorities, e.g., 12 U.S.C. § 3414(a)(5), 15 U.S.C. §§ 1681u(a) and (b), 15 U.S.C. § 1681v, and 18 U.S.C. § 2709, for the same individual or organization. The FBI may also serve multiple NSLs for an individual for multiple facilities (e.g., multiple e-mail accounts, landline telephone numbers, or cellular phone numbers). The number of requests, consequently, is significantly larger than the number of individuals or organizations that are the subjects of the NSLs.

Legal Authority	Annual Number of NSLs Issued	Annual Number of Requests for Information
National Security Letters issued pursuant to 12 U.S.C. § 3414(a)(5), 15 U.S.C. §§ 1681u(a) and (b), 15 U.S.C. § 1681v, and 18 U.S.C. § 2709	16,348	33,024

This information will be available at the website of the Office of the Director of National Intelligence (ODNI); and ODNI's public website dedicated to fostering greater public visibility into the intelligence activities of the government, IContheRecord.tumblr.com.

UNCLASSIFIED

Exhibit 3

Statistical Transparency Report Regarding Use of National Security Authorities

April 30, 2016

Annual Statistics for Calendar Year 2015 regarding Use of Certain National Security Legal Authorities.

In June 2013, President Obama directed the Intelligence Community (IC) to declassify and make public as much information as possible about certain sensitive U.S. government surveillance programs while protecting sensitive classified intelligence and national security information. Since then, the Director of National Intelligence (DNI) has declassified and authorized the public release of thousands of pages of documents relating to the use of critical national security authorities, including the Foreign Intelligence Surveillance Act (FISA). In addition to declassifying and publicly releasing these documents, the Intelligence Community has published several reports regarding these authorities, including the *Statistical Transparency Report Regarding use of National Security Authorities* (hereafter the DNI's annual transparency report), presenting metrics related to the use of certain authorities for calendar years [2013](#) and [2014](#).

On June 2, 2015, the [USA FREEDOM Act](#) was enacted, codifying many of the statistics reported in the DNI's annual transparency reports. The Act also expanded the scope of the information included in the reports by requiring the DNI to report information concerning United States person search terms and queries of certain unminimized, FISA-acquired information, as well as information concerning unique identifiers used to communicate information collected pursuant to certain FISA orders.¹ The IC implemented the USA Freedom Act on November 30, 2015.²

Today, consistent with the USA FREEDOM Act and the IC's [Principles of Intelligence Transparency](#), we are releasing our third annual transparency report presenting statistics on how often the government uses certain national security authorities. The DNI has declassified and directed the release of the applicable statistics covering calendar year 2015.

This information is available at the [website of the Office of the Director of National Intelligence](#) (ODNI); and ODNI's public website dedicated to fostering greater public visibility into the intelligence activities of the United States government, [icontheRecord.tumblr.com](#).

It is important to provide some additional context to the numbers included in this report:

- **Types of Orders.** There are several different types of orders that the Foreign Intelligence Surveillance Court (FISC) may issue in connection with FISA cases: orders granting or modifying the government's authority to conduct intelligence collection; orders directing electronic communication service providers to provide any technical assistance necessary to implement the authorized intelligence collection; supplemental orders and briefing orders requiring the government to take a particular action or provide the court with specific information; and so on.

Under Section 702, rather than issuing an individual order authorizing the government to target each non-U.S. person reasonably believed to be located outside the United States who possesses, or who is likely to communicate or receive, foreign intelligence information, the FISC

¹ See 50 U.S.C. § 1873(b).

² Although the USA FREEDOM Act was not implemented until November 30, 2015, the metrics provided in this report represent the full 2015 calendar year except where otherwise stated.

issues a single order³ approving certifications that describe *categories* of foreign intelligence information to be acquired through the targeting of non-U.S. persons reasonably believed to be located outside the United States.

Unless otherwise indicated, only the orders *granting authority to conduct intelligence collection* under the applicable FISA section are counted in this report; the other types of orders (e.g., modification orders) are not included.

- **Amendments and Renewals.** The FISC may amend an order one or more times after it has been issued. For example, an order may be amended to add a newly discovered account used by the target. This report *does not count such amendments* separately.

Moreover, some orders may be renewed multiple times during the calendar year (e.g., the FISA statute provides that a Section 704 FISA order against a U.S. person target may last no longer than 90 days but permits the order to be renewed). Unlike amendments, this report *does count each such renewal* as a separate order.

- **Targets.** Within the IC, the term “target” has multiple meanings. With respect to the statistics provided in this report, the term “target” is defined as the individual person, group, entity comprised of multiple individuals, or foreign power that uses the selector, such as a telephone number or email address. If a target were known to use four different selectors, the IC would count one target, not four. Alternatively, if four targets were known to use a one selector, the IC would count four targets.

The term “target” can also be used as a verb. Under Section 702, for example, the IC “targets” a particular non-U.S. person, group, or entity reasonably believed to be located outside the United States and who possesses, or who is likely to communicate or receive, foreign intelligence information, by “*tasking*” selectors that are assessed to be used by such non-U.S. person, group or entity, pursuant to targeting procedures approved by the FISC.

The number of 702 “targets” reflects an estimate of the number of known users of tasked selectors. This estimate is based on the information readily available to the IC. Unless and until the IC has information that links multiple selectors to a single foreign intelligence target, each individual selector is counted as being associated with a separate target in this report. On the other hand, where the IC is aware that multiple selectors are used by the same target, the IC counts the user of those selectors as a single target. This method of estimating helps ensure that the IC does not inadvertently understate the number of discrete persons *targeted* pursuant to Section 702.

- **Title V of FISA.** The IC implemented the USA FREEDOM Act’s Title V provisions on November 30, 2015, resulting in one additional month’s worth of data for calendar year 2015. Because statistical information tied to a particular FISA authority for a particular month remains

³ Note that, in its own transparency report, which is also required pursuant to Sec. 603 of the USA FREEDOM Act, the Director of the Administrative Office of the United States Courts (AOUSC) counted each Section 702 certification as being associated with its own order. Because the number of the government’s Section 702 certifications remains a classified fact, the government requested that the AOUSC redact the number of certifications and the number of modified orders from its transparency report prior to publicly releasing it.

classified, Title V data specifically associated with December 2015 – i.e., the information required under Section 603 (b)(4)(A) and (B) and 603 (b)(5)(A), (B) and (C) – is included only in the classified annex to this report that has been provided to Congress.

- **U.S. Persons.** In calculating the metrics in this report, the IC applied the broader definition of the term “U.S. Person” used in FISA, rather than USA FREEDOM Act’s narrower “U.S. Person” definition. Section 603(e)(4) of the USA FREEDOM Act defines “U.S. Person” as “a citizen of the United States or an alien lawfully admitted for permanent residence (as defined in section 101(a) of the Immigration and Nationality Act (8 U.S.C. § 1101(a))).” This definition is narrower than FISA’s, which defines “U.S. Person” as a citizen of the United States or an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in 50 U.S.C. § 1801(a)(1), (2), or (3). Because the broader FISA definition is the one that governs how U.S. person queries are conducted pursuant to the relevant minimization procedures, it also governs how those queries are counted. It is not possible to isolate U.S. person search terms that only meet the USA FREEDOM Act’s narrower definition.
- **“Unique identifiers used to communicate information collected pursuant to such orders.”** This language describes metrics included in the Title IV (PR/TT) portion of the report and in the Title V information covered in the classified annex to the report. The House Report on the USA FREEDOM Act states that “[t]he phrase ‘unique identifiers used to communicate information collected pursuant to such orders’ means the total number of, for example, email addresses or phone numbers that have been collected as a result of these particular types of FISA orders--not just the number of target email addresses or phone numbers.” H. Rept. 114-109 Part I.

The remainder of this page is intentionally left blank.

<u>Titles I and III and Sections 703 and 704 of FISA</u>	
Total number of orders	1,585
Estimated number of targets of such orders	1,695

The remainder of this page is intentionally left blank.

Section 702 of FISA	
Total number of orders	1
Estimated number of targets of such orders	94,368
Estimated number of search terms concerning a known U.S. person used to retrieve the unminimized contents of communications obtained under Section 702 (excluding search terms used to prevent the return of U.S. person information) ^a	4,672 ^b
Estimated number of queries concerning a known U.S. person of unminimized noncontents information obtained under Section 702 (excluding queries containing information used to prevent the return of U.S. person information) ^c	23,800 ^d

- a. Pursuant to 50 U.S.C. § 1873(d)(2)(A), this metric does not apply to queries conducted by the FBI.
- b. This metric includes some duplicative or recurring queries conducted using the same term.
- c. Pursuant to 50 U.S.C. § 1873(d)(2)(A), this metric does not apply to queries conducted by the FBI.
- d. One IC element is currently not able to provide this information. See the DNI's certification as to the estimated number of queries concerning a known U.S. person of unminimized noncontents information obtained under Section 702.

The remainder of this page is intentionally left blank.

RESPONSE TO PCLOB RECOMMENDATION 9(5)

In response to Recommendation 9(5) of the Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, prepared by the Privacy and Civil Liberties Oversight Board, the National Security Agency (NSA) provides the following additional information regarding the dissemination of Section 702 intelligence reports that contain U.S. person information.

Section 702 only permits the targeting of non-U.S. persons reasonably believed to be located outside the United States to acquire foreign intelligence information. Such targets, however, may on occasion communicate information of or about U.S. persons. Where appropriate, NSA may disseminate such information concerning U.S. persons. NSA only generates signals intelligence reports in response to a specific intelligence requirement, regardless of whether the proposed report contains U.S. person information. NSA's minimization procedures expressly prohibit dissemination of information about U.S. persons in any NSA report unless that information is necessary to understand foreign intelligence information or assess its importance, contains evidence of a crime, or indicates a threat of death or serious bodily injury. Even if one of these conditions applies, NSA often will mask the information and will, under any circumstance, include no more than the minimum amount of U.S. person information necessary to understand the foreign intelligence or to describe the crime or threat. In certain instances, however, NSA makes a determination prior to releasing its original report that the U.S. person's identity is appropriate to disseminate in the first instance using the same standards discussed above. In 2015, NSA disseminated 4,290 FAA Section 702 intelligence reports that included U.S. person information. Of those 4,290 reports, the U.S. person information was masked in 3,168 reports and unmasked in 1,122 reports.

Recipients of NSA reporting can request that NSA provide the true identity of a masked U.S. person referenced in an intelligence report, but this information is released only if the recipient has a legitimate need to know the identity and dissemination of the U.S. person's identity has been determined to be necessary to understand foreign intelligence information or assess its importance, contains evidence of a crime, or indicates a threat of death or serious bodily injury. Under NSA policy, NSA is allowed to unmask the identity for the specific requesting recipient only under certain conditions and where specific additional controls are in place to preclude its further dissemination, and additional approval has been provided by a designated NSA official. In 2015, NSA released 654 U.S. person identities in response to such requests.

Finally, as part of their regular oversight reviews, the Department of Justice and the Office of the Director of National Intelligence review disseminations of information about U.S. persons that NSA obtained pursuant to Section 702 to ensure that the disseminations were performed in compliance with the minimization procedures. For additional information, see page 7 of the NSA Director of Civil Liberties and Privacy Office Report, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702.

<u>Title IV of FISA</u> PR/TT FISA	
Total number of orders	90
Estimated number of targets of such orders	456
Estimated number of unique identifiers used to communicate information collected pursuant to such orders ^a	134,987 ^b

- a. Pursuant to Section 1873(d)(2)(B), this metric does not apply to orders resulting in the acquisition of information by the FBI that does not include electronic mail addresses or telephone numbers.
- b. This number represents information the government received from provider(s) electronically for the entire 2015 calendar year. The government does not have a process for capturing unique identifiers received by other means (such as hard-copy or portable media).

The remainder of this page is intentionally left blank.

<u>Title V of FISA</u>	
Annual number of approved applications	142 ^a
The number of individuals, entities, groups, or foreign powers subject to a business records application to obtain information about a specific subject	134
The number of selectors approved by the FISC to be queried either under the NSA telephony metadata program or by NSA under Section 501(b)(2)(C) of the USA FREEDOM Act	56 ^b
The number of known or presumed U.S. persons who were the subject of queries of information collected in bulk prior to the effective date of the business record provisions of the USA FREEDOM Act, or who were subject to a business records application at any point in 2015	183 ^c

- a. This metric consists of the total number of approved applications, or orders issued, prior to the effective date of the business records provisions of the USA FREEDOM Act, as well as the approved applications, or orders issued, under Sections 501(b)(2)(B) and 501(b)(2)(C), as required by Section 603(b)(4) and 603(b)(5) of the USA FREEDOM Act.
- b. This metric reflects the number of selectors approved by the FISC as meeting the reasonable articulable suspicion standard.
- c. This metric includes some duplicative or recurring queries conducted using the same identifier. There may also be some duplication to the extent that some of the U.S. persons who were the subject of queries of information collected in bulk were also subject to a business records application.

The remainder of this page is intentionally left blank.

National Security Letters (NSLs)^a	
Annual number of NSLs issued	12,870
Annual number of Requests for Information (ROI) ^b	48,642

- a. On April 29, 2016, the Department of Justice released its Annual Foreign Intelligence Surveillance Act Report to Congress. That report is available [\[here\]](#).
- b. For example: one NSL seeking subscriber information from one provider may identify three e-mail addresses, all of which are relevant to the same pending investigation; each is considered a separate “request.”

The remainder of this page is intentionally left blank.

THE HONORABLE JAMES L. ROBART

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

MICROSOFT CORPORATION,

Plaintiff,

v.

THE UNITED STATES DEPARTMENT
OF JUSTICE, and LORETTA LYNCH, in
her official capacity as the Attorney
General of the United States,

Defendant.

No. 16-CV-00538JLR

[PROPOSED] ORDER GRANTING
STIPULATED MOTION FOR LEAVE TO
FILE BRIEF *AMICUS CURIAE* OF
TWITTER, INC. IN SUPPORT OF
MICROSOFT CORPORATION'S
OPPOSITION TO DEFENDANT'S
MOTION TO DISMISS

The Court has reviewed the Stipulated Motion for Leave to File Brief *Amicus Curiae* of Twitter, Inc. in Support of Microsoft Corporation's Opposition to Defendant's Motion to Dismiss.

The Court **ORDERS** that the Motion is approved. The Clerk shall accept for filing the Brief *Amicus Curiae* of Twitter, Inc. In Support of Microsoft Corporation's Opposition to Defendant's Motion to Dismiss.

Dated this ____ day of _____, 2016.

HON. JAMES L. ROBART
United States District Judge

1 Presented by:

2
3 By: /s/ Hayley L. Berlin
4 Michael A. Sussmann*
5 Hayley L. Berlin, WSBA #43566
6 Perkins Coie LLP
7 700 Thirteenth Street, N.W., Suite 600
8 Washington, D.C. 20005-3960
9 Telephone: (202) 654-6200
10 Facsimile: (202) 654-6211
11 Email: MSussmann@perkinscoie.com
12 HBerlin@perkinscoie.com

13
14 Orin S. Kerr*
15 Law Office of Orin S. Kerr
16 2000 H Street, NW
17 Washington, D.C. 20052
18 Telephone: (202) 994-4775
19 Facsimile: (202) 994-5654
20 Email: okerr@law.gwu.edu

21
22 **pro hac vice* application pending

23
24 *Attorneys for Twitter, Inc.*

CERTIFICATE OF SERVICE

I hereby certify that on September 2, 2016, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to the email addresses indicated on the Court's Electronic Mail Notice List.

DATED: September 2, 2016

By: /s/Hayley L. Berlin
Hayley L. Berlin, WSBA No. 43566
Perkins Coie LLP
700 Thirteenth Street, N.W., Suite 600
Washington, D.C. 20005-3960
Telephone: (202) 654-6200
Facsimile: (202) 654-6211
Email: HBerlin@perkinscoie.com

Attorneys for Twitter, Inc.