United States
Foreign Intelligence Surveillance Court
Washington, D.C.

In re Motion to Disclose Aggregate Data Regarding FISA Orders	)	Docket No. Misc. 13-04

Microsoft Corporation's First Amended Motion for Declaratory Judgment or Other Appropriate Relief Authorizing Disclosure of Aggregate Data Regarding Any FISA Orders It Has Received

Pursuant to 28 U.S.C. § 2201 and Rule 6(d) of the Rules of Procedure of the United States Foreign Intelligence Surveillance Court ("FISC"), Microsoft Corporation ("Microsoft") respectfully moves this Court for an order, judgment, or such other relief as the Court may deem appropriate declaring that Microsoft may lawfully disclose aggregate statistics concerning any orders and/or directives that Microsoft may have received under the Foreign Intelligence Surveillance Act ("FISA") and/or FISA Amendments Act ("FAA").[1] Microsoft further respectfully requests that the Court hear oral argument on this Motion.[2]

I. Background

Microsoft, a corporation organized under the laws of the State of Washington with its principal place of business in Redmond, Washington, is a provider of electronic communication services and remote computing storage services to individual users, enterprises, educational institutions and governments worldwide. It is accordingly subject to orders and directives under FISA and the FAA seeking data hosted in the United States. *See* 50 U.S.C. §§ 1805(c)(2)(B);

---

[1] Nothing in this First Amended Motion is intended to confirm or deny that Microsoft has received any orders or directives issued pursuant to FISA or the FAA.

[2] The parties are today filing a motion for a proposed briefing order separate from this First Amended Motion.

1881a(h). As set forth in Microsoft's 2012 Law Enforcement Requests Report ("LERR"), *available at:* http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/, Microsoft receives a variety of lawful, compulsory process from U.S. federal, state, and local law enforcement authorities seeking user content and records. The LERR includes information about the number, within ranges, of National Security Letters ("NSLs") issued to Microsoft pursuant to 18 U.S.C. § 2709. Microsoft consulted the FBI before including NSL-related data in the LERR, and the FBI agreed that this information could be disclosed (in ranges) consistent with the NSL statute's non-disclosure obligations.

Since early June 2013, Microsoft and other electronic communication service providers have been the subject of intensive media coverage concerning an alleged U.S. Government surveillance program called "PRISM." *See* The Guardian, *NSA Prism Program Taps In To User Data of Apple, Google and Others* (June 6, 2013), *available at:* http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data; The Washington Post, *U.S., British Intelligence Mining Data From Nine U.S. Internet Companies in Broad Secret Program* (June 6, 2013), *available at:* http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html. The media has erroneously reported that the alleged PRISM program enables the U.S. Government to "tap[] directly into the central servers" of electronic communication service providers, including Microsoft, to collect information about their users.

In the months following the initial disclosure of the alleged PRISM program, the media has continued to report extensively on U.S. national security-related surveillance programs and the supposed role of technology and communications companies, including Microsoft, in such programs. *See, e.g.*, The Guardian, *NSA Paid Millions to Cover Prism Compliance Costs for Tech Companies* (Aug. 22, 2013), *available at:* http://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-

tech-companies-paid; The Washington Post, *NSA Gathered Thousands of Americans' E-mails Before Court Ordered It to Revise Its Tactics* (Aug. 21, 2013), *available at:* http://www.washingtonpost.com/world/national-security/nsa-gathered-thousands-of-americans-e-mails-before-court-struck-down-program/2013/08/21/146ba4b6-0a90-11e3-b87c-476db8ac34cd_story.html; The Guardian, *XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet'* (July 31, 2013), *available at:* http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

Microsoft has sought—and continues to seek—to correct the misimpression, furthered by inaccurate media reporting, that it provides the United States Government with direct access to its servers and network infrastructure and, thereby, indiscriminately discloses Microsoft users' information to the Government. As it had done in connection with its earlier disclosure of NSL-related statistics in the LERR, following the initial disclosures about the alleged PRISM program, Microsoft entered into discussions with the FBI concerning what information it could disclose relating to FISA orders and/or FAA directives that may have been served on Microsoft, if any. The FBI partially approved Microsoft's request to disclose information relating to FISA orders and/or FAA directives, subject to defined parameters. Specifically, the FBI informed Microsoft that it would not

> seek enforcement[1] of the non-disclosure provisions associated with any legal process, including FISA orders, so long as Microsoft agrees to aggregate data for all of the legal process it received in intervals of six months, beginning with the period ending December 31, 2012, from any and all government entities in the United States (including local, state, and federal, and including criminal and national security-related requests) into bands of 1000, starting at zero, and broken down into two categories: the number of requests and the number of user accounts for which data was requested.

(Letter from Andrew Weissmann, General Counsel, FBI, to John Frank, Vice President & Deputy General Counsel, Microsoft Corporation, June 14, 2013 (footnote omitted) (attached hereto as Exhibit A).)

Accordingly, on June 14, 2013, John Frank, Vice President & Deputy General Counsel for Microsoft, published the following statement on Microsoft's blog:

> This afternoon we are publishing additional information about the volume of law enforcement and national security orders served on Microsoft. For the first time, we are permitted to include the total volume of national security orders, which may include FISA orders, in this reporting. We are still not permitted to confirm whether we have received any FISA orders, but if we were to have received any they would now be included in our aggregate volumes.
>
> Earlier this week, along with others in the industry, we called for greater transparency about the volume and scope of the national security orders, including FISA orders, which require the disclosure of some customer content. We believe this would help the community understand and debate these important issues. Since then, we have worked with the FBI and U.S. Department of Justice to try and secure permission to do this.
>
> This afternoon, the FBI and DOJ have given us permission to publish some additional data, and we are publishing it straight away. However, we continue to believe that what we are permitted to publish continues to fall short of what is needed to help the community understand and debate these issues.
>
> Here is what the data shows: For the six months ended December 31,2012, Microsoft received between 6,000 and 7,000 criminal and national security warrants, subpoenas and orders affecting between 31,000 and 32,000 consumer accounts from U.S. governmental entities (including local, state and federal). This only impacts a tiny fraction of Microsoft's global customer base.
>
> We are permitted to publish data on national security orders received (including, if any, FISA Orders and FISA Directives), but only if aggregated with law enforcement requests from all other U.S. local, state and federal law enforcement agencies; only for the six-month period of July 1, 2012 thru December 31, 2012; only if the totals are presented in bands of 1,000; and all Microsoft consumer services had to be reported together. [. . .]

Available at: http://blogs.technet.com/b/microsoft_on_the_issues/archive/2013/06/14/microsoft-s-u-s-law-enforcement-and-national-security-requests-for-last-half-of-2012.aspx.

To promote additional transparency concerning the Government's lawful access to Microsoft's customer data, Microsoft sought permission to report more specific aggregate information about FISA orders and FAA directives, separate and apart from all other local, state, and federal law enforcement demands. The FBI and the Department of Justice denied Microsoft's

request. Accordingly, on June 19, 2013, Microsoft filed in this Court a Motion for Declaratory Judgment or Other Appropriate Relief seeking a judicial declaration authorizing the publication of the total number of orders and/or directives (if any) received under FISA and/or the FAA, as well as the total number of accounts affected by any such orders and/or directives.

Thereafter, the Court established a briefing schedule (*see* Order of June 20, 2013) and subsequently extended the Government's deadline to respond to Microsoft's motion six times so that the parties could engage in settlement discussions. (*See* Orders of July 3, 2013; July 23, 2013; August 1, 2013; August 7, 2013; August 13, 2013; and August 19, 2013.) Those discussions were unsuccessful. Microsoft now files this First Amended Motion and respectfully requests that the Court issue an order declaring that Microsoft may disclose, for each provision of FISA and/or the FAA pursuant to which Microsoft may receive process,[3] the following aggregate figures: (1) the number of orders and/or directives (if any) received that require the production of only non-content data, and the number of accounts affected by any such orders and/or directives; and (2) the total number of orders and/or directives (if any) received that require the production of content *and* non-content data, and the number of accounts affected by any such orders and/or directives (together, the "Aggregate Data").

Microsoft respectfully submits that there is no statutory basis under FISA or the FAA for precluding Microsoft from disclosing the Aggregate Data. Further, to the extent FISA, the FAA, or any other law or rule could be construed to bar such disclosure, such a construction would constitute a content-based restriction on speech and thus would impose a heavy burden on the Government to demonstrate that the restraint satisfies strict scrutiny—*i.e.*, that it is narrowly tailored

---

[3] These authorities could include electronic surveillance orders, *see* 50 U.S.C. §§ 1801-1812; physical search orders, *see* 50 U.S.C. §§ 1821-1829; pen register and trap and trace orders, *see* 50 U.S.C. §§ 1841-1846; business records orders, *see* 50 U.S.C. §§ 1861-1862; and orders and directives targeting certain persons outside the United States, *see* 50 U.S.C. §§ 1881-1881g.

to serve a compelling state interest. While the preservation of national security is undoubtedly a compelling interest, the Government has not demonstrated—and on the facts of this case, cannot establish—that restraining Microsoft from disclosing the Aggregate Data is narrowly tailored to serve that compelling interest. Without such a showing, a restraint on Microsoft's disclosure of the Aggregate Data violates the First Amendment.

II. FISA and the FAA Do Not Prohibit Microsoft From Disclosing the Aggregate Data.

FISA and the FAA do not prohibit providers from disclosing aggregated information about the number of FISA orders and/or FAA directives they receive. To the extent FISA or the FAA imposes on providers an obligation of secrecy with respect to individual FISA orders or FAA directives—and, in turn, to the extent such an obligation is incorporated into the language of any particular order or directive—the clear purpose of such an obligation is to prevent the specific targets of such orders or directives from becoming aware of the required search or surveillance. *See* 50 U.S.C. § 1805(c)(2)(B) (providers may be ordered to "furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier... is providing that target of electronic surveillance."); *see also* 50 U.S.C. § 1824(c)(2)(B) (imposing the same obligation in the context of a FISA physical search order); 50 U.S.C. § 1881a(h)(1)(A) (same with respect to a directive issued under Section 702 of the FAA).[4] As the statutory language makes clear, FISA's non-disclosure obligations are target-specific. The statute does not purport to impose on providers the obligation to remain silent about the fact that they

[4] The provisions of FISA and the FAA that require providers to maintain "records concerning the surveillance" under "security procedures approved by the Attorney General and Director of National Intelligence" have the same purpose—protecting the secrecy of particular FISA orders and FAA directives—and do not bar Microsoft from disclosing the Aggregate Data. 50 U.S.C. § 1805(c)(2)(C); *see also* 50 U.S.C. § 1881a(h)(1)(B).

receive FISA orders *generally*, nor does it purport to limit providers' ability to disclose the aggregate number of any such orders they may receive and the accounts that are affected.

Disclosure of the Aggregate Data would not plausibly jeopardize the secrecy of any particular FISA order or FAA directive that Microsoft may have received. Microsoft is a large provider of electronic communication services with millions of customers. Given the size of Microsoft's user base, and the tiny fraction of user accounts that are affected by any type of compulsory legal process served on Microsoft (whether issued pursuant to traditional law enforcement or national security authorities), the Government cannot reasonably contend that disclosure of the Aggregate Data could lead any particular individual user to infer that he or she had been targeted.

III. To the Extent FISA or the FAA Bars Microsoft's Disclosure of the Aggregate Data, Such a Restraint on Speech Violates the First Amendment.

As set forth above, FISA and the FAA do not prohibit providers such as Microsoft from disclosing the Aggregate Data. If, however, FISA, the FAA, or any other statute or rule were construed to prohibit such a disclosure, such a restraint would be unconstitutional as applied to Microsoft. *See Boddie v. Connecticut*, 401 U.S. 371, 379 (1971) ("Our cases further establish that a statute or a rule may be held constitutionally invalid as applied when it operates to deprive an individual of a protected right although its general validity as a measure enacted in the legitimate exercise of state power is beyond question.").

Any law prohibiting Microsoft from disclosing the Aggregate Data would be a content-based restriction on speech—*i.e.*, a rule forbidding speech about the fact that Microsoft has received process under FISA or the FAA—and thus subject to strict scrutiny. *See Doe v. Mukasey*, 549 F.3d 861, 878 (2d Cir. 2008) (noting, in the context of an analogous challenge to the non-disclosure provisions of the NSL statute, 18 U.S.C. § 2709, that "the Government has conceded that strict scrutiny is the applicable standard"). "Under strict scrutiny review, the Government must

demonstrate that the nondisclosure requirement is 'narrowly tailored to promote a compelling Government interest.'" *Id.* (quoting *United States v. Playboy Entm't Grp., Inc.*, 529 U.S. 803, 813 (2000)).

The Government has not, and cannot, establish that a prohibition against the disclosure of the Aggregate Data is "narrowly tailored" to promote the admittedly compelling Government interests in enforcing FISA orders and FAA directives, for three reasons.

First, as noted above, a bar to disclosing the Aggregate Data is not narrowly tailored because it does not promote the Government's interest in maintaining the secrecy of national security investigations or foreign intelligence collection. As one court explained when analyzing the non-disclosure provision of the NSL statute, "[i]t is not hard to surmise situations where recipients would appropriately be precluded from disclosing their receipt of an NSL. For example, if a[] [provider] has only a handful of subscribers, disclosure could compromise a national security investigation." *In re Nat'l Sec. Letter*, --- F. Supp. 2d. --- , 2013 WL 1095417, at *11 (N.D. Cal. Mar. 14, 2013). Microsoft, however, offers electronic communications services to many millions of users, none of whom could plausibly infer from the disclosure of the Aggregate Data that he or she has been targeted by a FISA order or FAA directive. That the First Amendment might permit a different result for a small provider with few customers does not justify the blanket imposition of a non-disclosure rule on Microsoft. *See Members of City Council of City of L.A. v. Taxpayers for Vincent*, 466 U.S. 789, 803 n.22 (1984) ("The fact that the ordinance is capable of valid applications does not necessarily mean that it is valid as applied to these litigants."); *United States v. Nat'l Treasury Emps. Union*, 513 U.S. 454, 478 (1995) ("In this case, granting full relief [under the First Amendment] to respondents—who include all Executive Branch employees below grade GS-16—does not require passing on the applicability of [the challenged honoraria ban] to Executive Branch employees above grade GS-15....").

Second, a prohibition against disclosure of the Aggregate Data is not narrowly tailored because the Government already discloses detailed aggregate data regarding surveillance activities undertaken pursuant to FISA. Under 50 U.S.C. § 1807, for example, the Attorney General is directed to transmit to Congress "a report setting forth with respect to the preceding calendar year... [1] the total number of applications made for orders and extensions of orders approving electronic surveillance under this subchapter; and [2] the total number of such orders and extensions either granted, modified, or denied." These reports are released to the public. *See* Letter to Majority Leader Harry Reid, United States Senate from Peter J. Kadzik, Principal Deputy Assistant Attorney General (Apr. 30, 2013), *available at:* http://www.justice.gov/nsd/foia/foia_library/2012fisa-ltr.pdf (noting, for example, that during calendar year 2012, (1) the Government made 1,856 applications to the FISC for authority to conduct electronic surveillance and/or physical searches for foreign intelligence purposes; and (2) the FISC did not deny any applications in whole or in part.)

The Government also has recently undertaken to release voluntarily even more detailed aggregate data about its use of FISA and the FAA. On August 29, 2013, the Director of National Intelligence ("DNI") announced that the Intelligence Community ("IC") would release annually the total number of orders issued during the prior year and the number of targets affected by those orders for each of the following categories of national security authorities: (i) FISA orders based on probable cause (Titles I and III of FISA, and sections 703 and 704); (ii) Section 702 of FISA; (iii) FISA Business Records (Title V of FISA); (iv) FISA Pen Register/Trap and Trace (Title IV of FISA); and (v) NSLs. *See* Office of the DNI, *DNI Clapper Directs Annual Release of Information Related to Orders Issued Under National Security Authorities*, IC on the Record (Aug. 29, 2013), *available at* http://icontherecord.tumblr.com/post/59719173750/dni-clapper-directs-annual-release-of-information. The fact that the Government already releases aggregate data about the number of FISA orders issued annually—and plans to release even more detailed aggregate information in

voluntary annual reports—refutes any notion that a prohibition on Microsoft's disclosure of its Aggregate Data is necessary to protect the secrecy of national security investigations or foreign intelligence collection. To the contrary, the Government's own speech on these issues supports Microsoft's claim that it should be permitted to disclose the fact that it has or has not received national security-related orders under specific statutory authorities, and how often.

Third, a rule barring Microsoft from disclosing the Aggregate Data fails strict scrutiny because of the significant public debate and interest over the use of FISA and the FAA to collect information from electronic communication services providers. The fact that the Government uses FISA and the FAA to collect information from electronic communication service providers is already a matter of public record as a result of statements made by the President, the DNI, and other high-ranking Government officials, as well as from documents that the Government recently has declassified. *See, e.g.*, Office of the DNI, *DNI Statement on Activities Authorized Under Section 702 of FISA* (June 6, 2013), *available at:* http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/869-dni-statement-on-activities-authorized-under-section-702-of-fisa ("*The Guardian* and *The Washington Post* articles refer to collection of communications pursuant to Section 702 of [FISA] ... Information collected under this program is among the most important and valuable foreign intelligence information we collect, and is used to protect our nation from a wide variety of threats."); U.S. Dep't of Justice & Office of the DNI, *The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act*, at 3 (marked "Top Secret" and transmitted to Congress on May 4, 2012; declassified on August 21, 2013), *available at:* http://www.dni.gov/files/documents/Ltr%20to%20HPSCI%20Chairman%20Rogers%20and%20Ranking%20Member%20Ruppersberger_Scan.pdf ("Once a target has been approved, NSA uses two means to acquire [redacted] electronic communications. First, [redacted], it acquires such communications directly from U.S.-based ISPs. This is known as PRISM collection.... Second, in

addition to collection directly from ISPs, NSA collects telephone and electronic communications as they transit the Internet 'backbone' within the United States. This is known as 'upstream' collection.").

In light of these statements, and the extensive public reporting on this subject, a prohibition against Microsoft's disclosure of the Aggregate Data cannot be narrowly tailored to promote the Government's national security interests. As *amici* point out, disclosure of the Aggregate Data constitutes truthful speech about Microsoft's actions taken under government compulsion, a subject at the core of what the First Amendment is intended to protect. *See* Br. of First Amendment Coalition *et al.*, at 6-8 & n.5 (citing *Mills v. Alabama*, 384 U.S. 214, 218 (1971) ("Whatever differences may exist about interpretations of the First Amendment, there is practically universal agreement that a major purpose of that Amendment was to protect the free discussion of governmental affairs."), and *Bartnicki v. Vopper*, 532 U.S. 514, 533-34 (2001) ("The enforcement of [the challenged measure] in these cases ... implicates the core purposes of the First Amendment because it imposes sanctions on the publication of truthful information of public concern.")). Particularly where, as here, the Government itself has decided to engage actively in an ongoing public debate on an issue of great importance to Microsoft's customers, shareholders, and the public, the First Amendment does not permit the Government to bar Microsoft from speaking about the very same subject.

* * *

For the foregoing reasons, Microsoft respectfully requests that the Court issue an order declaring that Microsoft may disclose the Aggregate Data.

Pursuant to Rule 7(i) of the FISC Rules of Procedure, Microsoft states that the following responsible employee of Microsoft holds a security clearance: John Frank, Vice President and Deputy General Counsel (DOD-Top Secret). This clearance was granted for the purpose of facilitating Microsoft's interaction with the Government concerning classified matters. Microsoft

further states that its undersigned counsel have security clearances as follows: James M. Garland (FBI-Top Secret), David N. Fagan (FBI-Top Secret), and Alexander A. Berengaut (FBI-Top Secret). These clearances were granted so as to permit counsel to advise their clients concerning any classified legal process they might receive.

Dated: September 9, 2013

Respectfully submitted,

MICROSOFT CORPORATION

James M. Garland, D.C. Bar # 475509
David N. Fagan, D.C. Bar # 474518
Alexander A. Berengaut, D.C. Bar # 989222
COVINGTON & BURLING LLP
1201 Pennsylvania Avenue, NW
Washington, DC 20004-2401
Tel: (202) 662-5337
Fax: (202) 778-5337

CERTIFICATE OF SERVICE

I hereby certify that at or before the time of filing this submission, the Government (care of the Security and Emergency Planning Staff, United States Department of Justice) has been served with a copy of this motion pursuant to Rule 8(a) of the FISC Rules of Procedure.

Dated: September 9, 2013

James M. Garland, D.C. Bar # 475509
David N. Fagan, D.C. Bar # 474518
Alexander A. Berengaut, D.C. Bar # 989222
COVINGTON & BURLING LLP
1201 Pennsylvania Avenue, NW
Washington, DC 20004-2401
Tel: (202) 662-5337
Fax: (202) 778-5337

EXHIBIT A

U.S. Department of Justice

Federal Bureau of Investigation

Office of the General Counsel

Washington, D.C. 20535

June 14, 2013

Mr. John Frank
Vice President/Deputy General Counsel
Office of the General Counsel
Microsoft Corporation
1 Microsoft Way
Redmond, WA 98052

Re: Microsoft's Pending Transparency Report

Dear Mr. Frank:

We appreciate your discussions with us about your proposal to disclose certain information about the volume of legal process Microsoft receives.

As we discussed during our phone call on June 14, 2013, we do not intend to seek enforcement[1] of the non-disclosure provisions associated with any legal process, including FISA orders, so long as Microsoft agrees to aggregate data for all of the legal process it received in intervals of six months, beginning with the period ending December 31, 2012, from any and all government entities in the United States (including local, state, and federal, and including criminal and national security-related requests) into bands of 1000, starting at zero, and broken down into two categories: the number of requests and the number of user accounts for which data was requested.

This position is an exercise of FBI discretion in light of current circumstances and the precise contours of this letter. Accordingly, our decision does not reflect the FBI's position with respect to potential disclosures by Microsoft that differ in any respect from the disclosures outlined in this letter. Nor is our decision a precedent for disclosures by any other company that is in receipt of such process, even if the disclosures were made in the manner that is proposed in this letter. The national security implications of disclosures related to the receipt of such process may vary depending on the identity of the company that is making the disclosure and the overall number of disclosures by different companies. For this reason, if other companies also seek to disclose information about the volume of such process that they receive, that may alter our

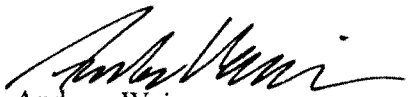
[1] The FBI does not have the authority to negate a court order, nor can we bind state or local authorities.

calculus about the implications of disclosures by Microsoft. In addition, our current determination is based on our prediction about the potential national security consequences of the disclosures and as such we may in the future revise our position as circumstances change or as we evaluate the actual impact of your disclosures on national security.

This letter further commits Microsoft to coordinate with us before making any additional public disclosures about the volume of legal process you receive, beyond the contours outlined in this letter. If we revise our position, we will notify you. We would retain the right to bring an appropriate enforcement action with respect to any future disclosures you make after you receive a notification of our change in position.

Thank you again for coordinating your proposal with us. We appreciate your efforts to reach an agreement that promotes transparency without jeopardizing our national security responsibilities to the public.

Sincerely,



Andrew Weissmann
General Counsel