United States Foreign Intelligence Surveillance Court

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

Microsoft Corporation's 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]

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); 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/,

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

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.

In recent weeks, 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.guardian.co.uk/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 Microsoft and other electronic communication service providers to collect information about their users.

Microsoft has sought—and continues to seek—to correct the misimpression, furthered by such 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, 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 approved Microsoft's request subject to specific parameters

under which Microsoft could make a public disclosure. 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 seeks to report aggregate information about FISA orders and FAA directives separately from all other local, state, and federal law enforcement demands. Despite

further efforts, however, Microsoft has not received permission from the FBI and the Department of Justice to disclose additional aggregate figures relating to any orders and/or directives it may have received under FISA or the FAA, 50 U.S.C. §§ 1801-1881g. Specifically, the Government has denied Microsoft's request to disclose the following two aggregate figures: (1) the total number of orders and/or directives (if any) received under FISA and/or the FAA; and (2) the total number of accounts affected by any such orders and/or directives (together, the "Aggregate Data").

As set forth below in greater detail, 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 or the FAA could be construed to bar such disclosure, such a construction would constitute a content-based restriction on speech that fails to satisfy strict scrutiny, in violation of 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 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).

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, 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 FISA or the FAA were to prohibit such a disclosure, however, the statutes would be unconstitutional.

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*, 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. 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*, 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.

Second, a prohibition against disclosure of the Aggregate Data is not narrowly tailored because FISA already provides for public disclosure of the aggregate number of applications made and orders issued under the law. Under 50 U.S.C. § 1807, 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 fact that the Government already releases aggregate data about the number of FISA orders issued annually refutes any notion that a prohibition against Microsoft's disclosure of the Aggregate Data is necessary to promote the Government's interest in protecting the secrecy of national security investigations.

Third, a construction of FISA and the FAA that would bar 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 Director of National Intelligence, among others. *See, e.g.,* Director of National Intelligence Statement on Activities Authorized Under Section 702 of FISA (June 6, 2013) ("*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."), *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.

In light of these statements, and the extensive public reporting on this subject, a statutory prohibition against Microsoft's disclosure of the Aggregate Data cannot be narrowly tailored to promote the Government's national security interests. The First Amendment does not permit the Government to bar Microsoft from speaking about an issue of great importance to its customers, shareholders, and the public while, simultaneously, senior Government officials are speaking publicly 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: June 19, 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: 202.662.6000
Fax: 202.662.6291

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 by hand delivery with a copy of this motion pursuant to Rule 8(a) of the FISC Rules of Procedure.

Dated: June 19, 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: 202.662.6000
Fax: 202.662.6291