

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

U.S. FOREIGN  
INTELLIGENCE  
SURVEILLANCE COURT

2013 SEP 17 PM 4:44

LEEANN FLYNN HALL  
CLERK OF COURT

IN RE MOTION FOR DECLARATORY JUDGMENT  
THAT LINKEDIN CORPORATION MAY REPORT  
AGGREGATE DATA REGARDING FISA ORDERS

Docket No. 13 - 07

**MOTION FOR DECLARATORY JUDGMENT  
THAT LINKEDIN CORPORATION MAY REPORT  
AGGREGATE DATA REGARDING FISA ORDERS**

Pursuant to 28 U.S.C. § 2201 and Rule 6(d) of the Rules of Procedure of the Foreign Intelligence Surveillance Court, LinkedIn Corporation (“LinkedIn”) hereby respectfully moves this Court for an order, judgment, or such other relief as this Court may deem appropriate, declaring that, for each provision of the Foreign Intelligence Surveillance Act (“FISA”), 50 U.S.C. § 1801 *et seq.* and the FISA Amendments Act (the “FAA”) pursuant to which LinkedIn may receive process, LinkedIn may, without violating any provision of law, publicly report the total number of compulsory requests it receives from the United States government and the total number of users or accounts encompassed within such requests.<sup>1</sup> Further, pursuant to Rule 17 of the Rules of Procedure, LinkedIn respectfully requests a public oral argument on this Motion.

**BACKGROUND**

LinkedIn is the world’s largest professional network, with over 238 million members. Among other things, through its website and mobile applications, LinkedIn provides its members with electronic communications services. Thus, LinkedIn’s business involves providing

---

<sup>1</sup> Nothing in this Motion is intended to, or does, confirm or deny that LinkedIn has received any requests under FISA or the FAA.

electronic communications services that, for certain purposes, are subject to FISA and the FAA. See 50 U.S.C. § 1805(c)(2)(B); 50 U.S.C. § 1881a(h).<sup>2</sup>

LinkedIn's mission is to connect the world's professionals to make them more productive and successful. As it represents to its members, one of LinkedIn's core values is "Members First." Critical to this mission and core value is LinkedIn's commitment to earning and retaining its members' trust. It earns this trust by being open and transparent with its members, and by providing members with the Three C's, as it relates to members' data: Clarity, Consistency and Control. LinkedIn is clear about what it will and will not do with member data. It is consistent with how it treats member data (*e.g.*, no retroactive default settings). And, finally, LinkedIn provides members control over their data. This applies to all data on LinkedIn, including communications. LinkedIn's members entrust LinkedIn with their data, upon which they have built their professional reputation. LinkedIn's success is based upon the trust its members have placed in the company; although that trust takes a long time to build, it can be broken with a snap of the fingers.

---

<sup>2</sup> Under the FAA, for example, the term "electronic communications service provider" is defined by reference to how that term is defined by the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701 *et seq.* See 50 U.S.C. 1881(b)(4)(C). However, the SCA regulates *only* the disclosure of stored electronic communications held by providers of electronic communication service ("ECS") and providers of remote computing service ("RCS"). Whether an entity acts as an ECS or an RCS is entirely context dependent; a determination of whether the SCA's ECS rules or RCS rules apply must occur based on the particular service or particular piece of an electronic communication at issue at a specific time. See *In re United States*, 665 F. Supp. 2d 1210, 1214 (D. Or. 2009); Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO.WASH. L. REV. 1208, 1215-16 & n.48 (2004) ("Kerr"). In other words, a provider such as LinkedIn can act as an ECS with respect to some communications, an RCS with respect to other communications, and neither an ECS nor an RCS with respect to other communications. Kerr at 1215-16 & n.48. Thus, nothing in this Motion is intended as an acknowledgement that LinkedIn is subject to the SCA for any and all purposes.

LinkedIn understands, supports and has the greatest respect for the critical work performed by the government to protect our national security. At the same time, recent news reports about government surveillance have given rise to significant concerns among both the American people and the global community about the privacy of individuals' communications, activities, and personal data on the Internet. For example, both *The Guardian* and *The Washington Post* newspapers have published extensive reports alleging that the government has far-reaching access to electronic communications of American citizens, particularly via providers of Internet communications services similar to those provided by LinkedIn.<sup>3</sup> As President Obama has noted, these are "revelations that have depleted public trust" in the privacy of electronic communications.<sup>4</sup> Indeed, the President has acknowledged that when those "outside of the intelligence community" read these news stories, "understandably, people would be concerned" and that he, "too," would be concerned if he "wasn't inside the government."<sup>5</sup> Other articles have falsely suggested that LinkedIn itself is the subject of extensive government surveillance and information gathering.<sup>6</sup> All of these reports clearly have the potential to cause significant harm to LinkedIn's reputation and to its business.

Under these circumstances, and in light of LinkedIn's mission and core value, LinkedIn is committed to disclosing to its members clear and accurate information about government

---

<sup>3</sup> See, e.g., <http://www.theguardian.com/world/2013/jun06/us-tech-giants-nsa-data>; [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](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).

<sup>4</sup> Remarks by the President in a Press Conference, Aug. 9, 2013, <http://www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference>.

<sup>5</sup> *Id.*

<sup>6</sup> See, e.g., <http://www.wnd.com/2013/06/prism-targets-worldwide-communications/> (stating that "LinkedIn and Twitter also are included in this information gathering" under government "PRISM" program).

requests for their data and communications, including the frequency and nature of government requests and the number of members affected. LinkedIn seeks to report this data in order to address its members' concerns about the privacy and security of their data, activities, and communications on the LinkedIn site; to correct any misimpressions members might have about the nature and frequency of government requests; and to inform the important and ongoing public debate regarding government surveillance.

To these ends, over the past several months, LinkedIn has engaged with the Federal Bureau of Investigation ("FBI") to try to reach an agreement regarding LinkedIn's reporting of information regarding the number and the type of government requests for information it has received, including national security-related requests under FISA and/or the FAA and National Security Letters ("NSLs"). LinkedIn understands and supports the government's increasingly difficult job of protecting our national security, but those national security interests must be balanced against the need for transparency. LinkedIn has never sought, and does not now seek, to disclose the substance of any such requests, the identity of the affected members, or the substance of any of LinkedIn's responses to the requests. Against the backdrop of these negotiations, on July 18, 2013, LinkedIn and dozens of other companies and nonprofit organizations and trade associations sent a letter to President Obama and congressional leadership urging greater transparency around national security-related requests by the United States government to Internet, telephone, and web-based service providers for information about their users and subscribers.

Unfortunately, despite extensive negotiations, LinkedIn and the FBI have recently reached an impasse and have been unable to agree on a reporting framework that would permit LinkedIn to provide its members and the public with an accurate and more transparent

understanding of the government's national security-related requests for its members' data and communications. Among other things, the FBI has taken the position that LinkedIn cannot report aggregate data regarding the number of FISA requests, NSLs, or other kinds of national security-related requests or the aggregate number of member accounts affected by such requests. The FBI has informed LinkedIn that it has two choices: (1) it may disclose the total number of government requests for information, excluding all national security-related requests, with the number of NSLs only in "buckets of 0 to 1,000" on an annual basis and without any information regarding the number of FISA requests; or (2) it may disclose the total number of all government requests, including national security-related requests, on a six-month basis but only in "buckets of 0 to 1,000" and without any breakdown or indication of the number of national security-related requests.

On September 17, 2013, LinkedIn published a global transparency report of government requests for members' data, covering the period January 1, 2013 – June 30, 2013. The report lists total U.S. government requests for member data, including subpoenas, search warrants, court orders, and other requests. As a result of the FBI's restrictions, however, the report does not include any data regarding national security-related requests, including requests issued under FISA and/or the FAA or NSLs.

The FBI continues to maintain that disclosing this information would harm unspecified national security interests despite the fact that, on August 29, 2013, at the direction of President Obama, the Director of National Intelligence ("DNI") instructed the intelligence community to report data regarding various requests for information related to national security, including: (1) orders under FISA based on probable cause; (2) orders under Section 702 of FISA; (3) orders to produce business records pursuant to Title V of FISA; (4) orders for Pen Registers

pursuant to Title IV of FISA; and (5) NSLs issued pursuant to 18 U.S.C. § 2709, among other statutes.<sup>7</sup> The DNI stated that, in each category, the intelligence community would release the “total number of orders” and the “number of targets affected by these orders.”<sup>8</sup>

The government’s restrictions on the information that LinkedIn can provide to its members and to the public lacks any support in the law and is inconsistent with the Constitution. Moreover, LinkedIn’s reputation and business have been and continue to be affected by the limitations on the information LinkedIn can disclose, particularly in light of the recent news reports of government surveillance activity and the false and misleading news reports suggesting that LinkedIn may itself be the subject of extensive government surveillance. Under these circumstances, LinkedIn hereby moves this Court for an order declaring that, for each provision of FISA and/or the FAA pursuant to which it may receive process,<sup>9</sup> LinkedIn may disclose, on a semi-annual basis, the total number of compulsory requests it received from the United States government issued during the prior six months and the total number of members or accounts encompassed within or affected by such requests (collectively, “the Aggregate Data”), without violating any provision of law. At a minimum, LinkedIn respectfully submits that it is entitled to report the total number of compulsory requests it has received pursuant to FISA and/or the FAA and the total number of members or accounts encompassed within or affected by such requests.

---

<sup>7</sup> See <http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/922-dni-clapper-directs-annual-release-of-information-related-to-orders-issued-under-national-security-authorities>.

<sup>8</sup> *Id.*

<sup>9</sup> These authorities include the provisions of FISA and the FAA authorizing (1) electronic surveillance orders, *see* 50 U.S.C. §§ 1801-1812; (2) physical search orders, *see* 50 U.S.C. §§ 1821-1829; (3) pen register and trap and trace orders, *see* 50 U.S.C. §§ 1841-1846; (4) business records orders, *see* 50 U.S.C. §§ 1861-1862; and (5) orders and directives targeting certain persons outside the United States, *see* 50 U.S.C. §§ 1881-1881g.

## ARGUMENT

At the President's direction, the government is "creating a website that will serve as a hub for further transparency" in order to "give Americans and the world the ability to learn more about what our intelligence community does and what it doesn't do, how it carries out its mission, and why it does so."<sup>10</sup> That is all LinkedIn seeks for itself, its members, and the public, and it is all that reporting the Aggregate Data would do. The government's limitations on the information that LinkedIn may disclose is unsupported by FISA, the FAA, or any other rule of law. It also violates the First Amendment by restricting LinkedIn's ability to communicate with its members and the broader public regarding the number of requests for member data it has received.

### **I. NO RULE OF LAW PROHIBITS LINKEDIN FROM REPORTING THE AGGREGATE DATA**

No provision of FISA or the FAA grants the government the authority it has arrogated to itself to limit LinkedIn's ability to report publicly the Aggregate Data. Among other things, neither statutory framework contains any provision authorizing the government to prevent the recipient of an order issued by this Court authorizing electronic surveillance from disclosing the existence of such an order. Nor does any provision of FISA or the FAA prohibit the recipient of an electronic surveillance order from disclosing the fact that the order has been received. Further, the plain text of the provisions of FISA and the FAA that refer to disclosure of this Court's orders makes clear that neither provision prohibits disclosure of the Aggregate Data.

The first such provision provides that this Court may order electronic communications providers to furnish "all information, facilities, or technical assistance necessary to accomplish

---

<sup>10</sup> Remarks by the President in a Press Conference, Aug. 9, 2013, *supra* note 4.

the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services” the provider is “providing that target of electronic surveillance.” 50 U.S.C. § 1805(c)(2)(B); *see also* 50 U.S.C. § 1824(c)(2)(B); § 1881b(h)(1)(A). Far from a perpetual gag order prohibiting the disclosure of the existence of surveillance the government already has undertaken, this provision simply ensures that communications providers will take steps to avoid alerting *targets* as to surveillance activities the government is carrying out or will carry out with respect to their communications. The provision requires a communications provider to minimize interference with the target’s service precisely because a significant disruption of service could alert the target. Likewise, because FISA defines “electronic surveillance” as “the *acquisition*” of data or communications, *see* 50 U.S.C. § 1801(f) (emphasis added), the phrase “accomplish the electronic surveillance in such manner as will protect its secrecy” simply means that a communications provider must not compromise the secrecy of planned surveillance of a particular target before the government can carry it out. That language does not prevent a communications provider from disclosing the number of requests for surveillance it already has received without disclosing the targets of that surveillance. Nothing in such a disclosure undermines the secrecy of the surveillance conducted against a particular target or alerts a target that is going to be the subject of surveillance.

Nor does the provision of FISA that requires electronic communications providers to “maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition or the aid furnished that such electronic communication service provider wishes to maintain” prohibit the reporting of the Aggregate Data. 50 U.S.C. § 1805(c)(2)(C); *see also* 50 U.S.C. § 1881a(h)(1)(B) (same). The provision is directed only at “records” that an electronic communications provider may maintain.



Here, LinkedIn is not seeking to disclose any records, *i.e.*, the identity of members or the substance of communications. LinkedIn merely seeks to report the Aggregate Data, which consists only of the number and type of requests without disclosing *any* information regarding the content of those requests.

In light of these statutory provisions, and the absence of any other provision that authorizes the government to impose limitations on the disclosure of the Aggregate Data, the restrictions imposed by the government are without legal basis, exceed the government's authority, and should be stricken down.

## **II. LINKEDIN HAS A FIRST AMENDMENT RIGHT TO REPORT THE AGGREGATE DATA**

For the reasons set forth above, no rule of law prevents LinkedIn from reporting the Aggregate Data. Any rule of law that could be interpreted to authorize the government to prevent LinkedIn from reporting the Aggregate Data would be unconstitutional under the First Amendment because LinkedIn has a free speech right to report such information to its members and to the public.

Judge Illston in the Northern District of California recently held that an explicit statutory provision prohibiting the disclosure of requests for national security-related information violated the First Amendment. *See In re Nat'l Sec. Letter*, No. C 11-02173 SI, 2013 WL 1095417 (N.D. Cal. Mar. 14, 2013), *appeal pending*, Nos. 13-15957, 13-16731 and 13-16732 (9th Cir.). The petitioner in that case was an electronic communications provider that received an NSL pursuant to 18 U.S.C. § 2709. In the letter, the FBI certified that disclosing the existence of the NSL could result in "a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person." *Id.* at \*2. Under the NSL

statute, the FBI's certification prohibited the petitioner from disclosing the NSL's existence. *See* 18 U.S.C. § 2709(c). The petitioner filed an action alleging that the nondisclosure provision violated the First Amendment. Judge Illston held that the government's "pervasive use of nondisclosure orders, coupled with the government's failure to demonstrate that a blanket prohibition on recipients' ability to disclose the mere fact of receipt of an NSL is necessary to serve the compelling need of national security, creates too large a danger that speech is being unnecessarily restricted." *In re Nat'l Sec. Letter*, 2013 WL 1095417, at \*10.

The same is true here where the government claims authority to prevent LinkedIn from reporting factual information regarding FISA orders. Like the NSL nondisclosure provision, a prohibition on reporting the Aggregate Data, whether or not statutory, "clearly restrains speech of a particular content—significantly, speech about government conduct." *In re Nat'l Sec. Letter*, 2013 WL 1095417, at \*6 (citing *John Doe, Inc. v. Mukasey*, 549 F.3d 861, 876, 878 (2d Cir. 2008)). The government's position, as in the NSL litigation, is that LinkedIn may be "prevented from speaking about [its] receipt" of any national security-related requests "and from disclosing, as part of the public debate on the appropriate use of" such requests its "own experiences." *Id.*

As a content-based restraint on speech, it is subject to strict scrutiny. *See, e.g., id.*; *Ysursa v. Pocatello Educ. Ass'n*, 555 U.S. 353, 358 (2009) ("Restrictions on speech based on its content are presumptively invalid and subject to strict scrutiny.") (quotation marks omitted). Indeed, the government previously has conceded that strict scrutiny would apply to a statute preventing the very kind of disclosure that the government has claimed the power to prevent here. *See Mukasey*, 549 F.3d at 877-78. Under strict scrutiny review, the government must demonstrate that the nondisclosure requirement is "narrowly tailored to serve a compelling

governmental interest.” *In re Nat’l Sec. Letter*, 2013 WL 1095417, at \*6; compare *United States v. Playboy Entm’t Grp., Inc.*, 529 U.S. 803, 813 (2000) (same).

Further, the government’s position is that it “has been given the unilateral power to determine, on a case-by-case basis, whether to allow [the] recipients” of national security-related requests “to speak about the” requests. *In re Nat’l Sec. Letter*, 2013 WL 1095417, at \*6. Judge Illston held that the First Amendment prohibited the government from exercising such power as to NSLs, *even where Congress had granted it*. *See id.* If no statute prohibits disclosure of the Aggregate Data, the government’s claimed authority would be even more constitutionally problematic. While this may not be a “typical” prior restraint, the government cannot exercise this kind of authority unless it can show the same “heightened justifications for sustaining prior-restraints” that apply to traditional prior restraints. *Id.*; *cf. New York Times Co. v. United States*, 403 U.S. 713, 723 (1971) (Douglas, J., concurring) (“The Government says that it has inherent powers to go into court and obtain an injunction to protect the national interest, which in this case is alleged to be national security. [We have] repudiated that expansive doctrine in no uncertain terms.”).

To be sure, the government’s interest in national security is vitally important as a general matter. *See Snepp v. United States*, 444 U.S. 507, 510 (1980) (*per curiam*) (“The Government has a compelling interest in protecting both the secrecy of information important to our national security and the appearance of confidentiality so essential to the effective operation of our foreign intelligence service”). However, a restraint on reporting that applies, “without distinction,” to “both the content of” a request for national security-related information “and to the very fact of having received one” is “not narrowly tailored” to the government’s interest in national security. *In re Nat’l Sec. Letter*, 2013 WL 1095417, at \*10.

That is because reporting only an aggregate *number* of requests (and the aggregate *number* of members affected) does not reveal anything about the substantive *content* of those requests. Disclosure of the number of requests does not reveal what information or threats the government is investigating, nor does it reveal who the information relates to or the member or members at issue. An aggregate number does not give anyone warning that he or she is under suspicion or the target of surveillance. And an aggregate number does not reveal whether this Court has issued any particular order or granted any particular government application. In short, unless a recipient has “only a handful of subscribers,” reporting whether a recipient has received a request for information related to national security does not reveal anything about the government’s strategy or tactics in protecting national security. *Id.* at \*11.

Nor can the government claim otherwise where it already has publicly reported aggregate data on requests under FISA.<sup>11</sup> Further, as set forth above, the DNI has directed the intelligence community to report data regarding various requests for information related to national security, including FISA orders and NSLs.<sup>12</sup> The DNI stated that, in each category, the intelligence community would release the “total number of orders” and the “number of targets affected by these orders.”<sup>13</sup>

Thus, LinkedIn’s reporting of the aggregate *number* of each such request it has received (and the aggregate number of members affected)—without disclosing the *contents* of any of these requests—would simply report a subset of information that the government itself has

---

<sup>11</sup> See Letter from Peter J. Kadzik, Principal Deputy Attorney General, U.S. Dep’t of Justice, to Hon. Senator Harry Reid, Majority Leader, Apr. 30, 2013, available at: [http://www.justice.gov/nsd/foia/foia\\_library/2012fisa-ltr.pdf](http://www.justice.gov/nsd/foia/foia_library/2012fisa-ltr.pdf).

<sup>12</sup> See *supra* note 7.

<sup>13</sup> *Id.*

reported and will continue reporting. The First Amendment simply does not permit the government to restrain LinkedIn from reporting a portion of information that the government itself already has disclosed.

On the contrary, a prior restraint on reporting the Aggregate Data would be “especially problematic in light of the active, continuing public debate” regarding government surveillance. *In re Nat’l Sec. Letter*, 2013 WL 1095417, at \*11. Indeed, the government has publicly stated on repeated occasions that it uses its powers under FISA and the FAA to collect information regarding Internet users’ activities and communications, and has weighed in on this public debate about the value of such programs.<sup>14</sup> The President has called for “a thoughtful fact-based debate” that is “guided by our Constitution, with reverence for our history as a nation of laws, and with respect for the facts.”<sup>15</sup> Reporting the Aggregate Data would provide LinkedIn members and the public with basic facts about the government’s requests to LinkedIn for information about its members. As such, it “occupies the highest rung of the hierarchy of First Amendment values, and is entitled to special protection.” *Snyder v. Phelps*, 131 S. Ct. 1207,

---

<sup>14</sup> See, e.g., Director of National Intelligence 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> (“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 3-4 (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](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.”).

<sup>15</sup> See Remarks by the President in a Press Conference, Aug. 9, 2013, *supra* note 4.

1215 (2011) (quotation marks omitted); *see also Mills v. Alabama*, 384 U.S. 214, 218 (1966) (“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.”); *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.”).

There is no justification for depriving LinkedIn of the protections provided by the First Amendment here. Reporting the Aggregate Data would not jeopardize national security and the government itself already has reported similar data. Accordingly, LinkedIn has a First Amendment right to report the Aggregate Data and any provision of law preventing such reporting is constitutionally infirm.

### **III. CONCLUSION**

For the foregoing reasons, LinkedIn respectfully requests that this Court issue an order, judgment, or such other relief as this Court may deem appropriate, declaring that LinkedIn may disclose the Aggregate Data without violating any provision of law.

Further, pursuant to Rule 17 of the Rules of Procedure, LinkedIn respectfully requests a public oral argument on this Motion. Given that the issues of transparency raised by this Motion are the subject of intense concern by and vigorous debate among the American people and their elected representatives, it is appropriate that those issues be adjudicated as transparently as possible.

\* \* \* \*

The undersigned counsel do not hold a security clearance.

Pursuant to Rule 7(h) and Rule 63, the undersigned counsel for LinkedIn hereby certify that Jerome C. Roth is licensed to practice law by the bar of California and the bar of New York, and is a member in good standing of the bars of the United States Courts of Appeals for the Second and Ninth Circuits and the United States District Courts for the Eastern, Central and Northern Districts of California and the Southern and Eastern Districts of New York.

Undersigned counsel further certify that Jonathan H. Blavin is licensed to practice law by the bar of California, and is a member in good standing of the bars of the United States Court of Appeals for the Ninth Circuit and the United States District Courts for the Eastern, Central and Northern Districts of California. Undersigned counsel certify that Justin P. Raphael is licensed to practice law by the bar of New York, and is a member in good standing of the bar of the United States District Court for the Southern District of New York.

Dated: September 17, 2013

  
Jerome C. Roth  
Jonathan H. Blavin  
Justin P. Raphael  
Munger, Tolles & Olson LLP  
560 Mission Street, 27th Floor  
San Francisco, CA 94105  
(415) 683-9100 (telephone)  
(415) 512-4077 (facsimile)  
Jerome.Roth@mto.com  
Jonathan.Blavin@mto.com  
Justin.Raphael@mto.com

*Attorneys for Movant LinkedIn Corporation*

**CERTIFICATE OF SERVICE**

I hereby certify this 17th of September, 2013, that the foregoing document was served via hand delivery on the following:

Christine Gunning  
Litigation Security Group  
United States Department of Justice  
2 Constitution Square  
145 N. St., NE, Suite 2W-115  
Washington, DC 20530

  
Jerome C. Roth  
Jonathan H. Blavin  
Justin P. Raphael  
Munger, Tolles & Olson LLP  
560 Mission Street, 27th Floor  
San Francisco, CA 94105  
(415) 512-4000 (telephone)  
(415) 512-4077 (facsimile)  
Jerome.Roth@mto.com  
Jonathan.Blavin@mto.com  
Justin.Raphael@mto.com

*Attorneys for Movant LinkedIn Corporation*