

**Court of Appeals Case Nos. 13-15957, 13-16731 and 13-16732**

---

**UNITED STATES COURT OF APPEALS  
FOR THE NINTH CIRCUIT**

IN RE NATIONAL SECURITY LETTER

---

Appeal from the United States District Court  
for the Northern District of California  
The Honorable Susan Illston, United States District Judge

---

**BRIEF OF *AMICUS CURIAE* LINKEDIN CORPORATION  
SUPPORTING APPELLEE AND URGING AFFIRMANCE**

---

JEROME C. ROTH  
JONATHAN H. BLAVIN  
JOHN P. MITTELBAACH  
MUNGER, TOLLES & OLSON LLP  
560 Mission Street, 27th Floor  
San Francisco, California 94105  
(415) 512-4000

*Counsel for Amicus Curiae  
LinkedIn Corporation*

## **CORPORATE DISCLOSURE STATEMENT**

Pursuant to Rules 26.1 and 29(c)(1) of the Federal Rules of Appellate

Procedure:

*Amicus* LinkedIn Corporation certifies that it is a publicly held  
company.

# TABLE OF CONTENTS

	<b>Page</b>
CORPORATE DISCLOSURE STATEMENT .....	i
INTEREST OF AMICUS CURIAE .....	1
SUMMARY OF ARGUMENT .....	1
BACKGROUND .....	6
A.    LinkedIn’s Business and Its Commitment to Trust and Transparency .....	6
B.    Recent Reports of Government Surveillance Have Raised Serious Issues of Public Mistrust .....	8
C.    The FBI’s Recent Proposals to LinkedIn Only Exacerbate the Problem and Would Not Provide Transparency .....	11
ARGUMENT .....	14
A.    The Non-Disclosure Provision Threatens LinkedIn and Other American Internet Companies’ Vital Interests in Transparency And User Trust .....	14
B.    The Non-Disclosure Provision Undermines The First Amendment Interests of LinkedIn, Its Members, and the Public to Engage In An Informed Debate On An Issue of Substantial Public Importance .....	18
CONCLUSION.....	23
CERTIFICATE OF COMPLIANCE WITH FEDERAL RULE OF APPELLATE PROCEDURE 32.....	24
CERTIFICATE OF SERVICE.....	25

## TABLE OF AUTHORITIES

Page(s)

### FEDERAL CASES

<i>Bartnicki v. Vopper</i> , 532 U.S. 514 (2001).....	19
<i>Mills v. Alabama</i> , 384 U.S. 214 (1971).....	19, 20
<i>Snepp v. United States</i> , 444 U.S. 507 (1980).....	21
<i>Snyder v. Phelps</i> , 131 S. Ct. 1207 (2011).....	19
<i>The Florida Star v. B.J.F.</i> , 491 U.S. 524 (1989).....	19
<i>In re Nat'l Sec. Letter</i> , No. C 11-02173 SI, 2013 WL 1095417 (N.D. Cal. Mar. 14, 2013).....	passim
<i>In re United States</i> , 665 F. Supp. 2d 1210 (D. Or. 2009).....	6

### FEDERAL STATUTES

18 U.S.C. §§ 2701 <i>et seq.</i> .....	6
18 U.S.C. § 2709.....	3, 13
18 U.S.C. § 2709(a) .....	6
18 U.S.C. § 2709(c) .....	9
18 U.S.C. § 2709(c)(1).....	3, 10

### FEDERAL RULES

Fed. R. App. P. 29(a) .....	1
-----------------------------	---

**TABLE OF AUTHORITIES**  
**(continued)**

	<b>Page(s)</b>
Fed. R. App. P. 29(c)(5).....	1
Fed. R. App. P. 32.....	24
Fed. R. App. P. 32(a)(5).....	24
Fed. R. App. P. 32(a)(6).....	24
Fed. R. App. P. 32(a)(7)(B) .....	24
Fed. R. App. P. 32(a)(7)(B)(iii) .....	24
 <b>OTHER AUTHORITIES</b>	
Federal Trade Commission Staff, “Mobile Privacy Disclosures: Building Trust Through Transparency,” February 2013.....	16
Kerr, Orin S., <i>A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It</i> , 72 GEO.WASH. L. REV. 1208 (2004).....	6
Remarks by the President in a Press Conference, Aug. 9, 2013 .....	16
Internet Policy Task Force, Department of Commerce, “Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework,” December 16, 2010 .....	15
Shah, Dharmesh, “The Surprising Brilliance of the LinkedIn Influencers Program” .....	19

## **INTEREST OF *AMICUS CURIAE***

*Amicus Curiae* LinkedIn Corporation (“LinkedIn”) respectfully submits this brief with the consent of all parties.<sup>1</sup> Fed. R. App. P. 29(a).

LinkedIn is an Internet company that hosts the world’s largest professional network, with over 238 million members. LinkedIn’s mission is to connect the world’s professionals to enable them to be 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 by being open, transparent, responsive, and clear regarding the privacy and security of their personal data on LinkedIn. LinkedIn therefore has a strong and direct interest in the rules governing public disclosure of government requests for national security-related data.

## **SUMMARY OF ARGUMENT**

A bedrock principle of the American Internet industry is earning and maintaining user trust. The industry flourishes based on the confidence users have in the secure, transparent manner in which their data will be handled. As the world’s largest professional network, LinkedIn is

---

<sup>1</sup> Pursuant to Rule 29(c)(5), LinkedIn states that (i) no counsel for a party has written this brief in whole or in part and (ii) no person or entity other than LinkedIn has made a monetary contribution that was intended to fund the preparation or submission of this brief.

committed to preserving the trust that it has built with its over 238 million members by providing them with clear, accurate, consistent, and transparent reporting about how LinkedIn handles and protects its members' personal data.

LinkedIn's commitment to transparency and member trust is all the more critical in the wake of recent revelations in the press and elsewhere regarding alleged secret government surveillance programs of American Internet and telecommunications companies and their users' data and communications. These reports have shaken the public's confidence in the privacy and security of personal information. This potential erosion of user trust threatens the entire Internet and technology sector, which has been the economic bright spot in America's struggling economy for the last several years.

Under these circumstances, it is vital that LinkedIn and similar companies have the right to communicate to their members and to the public basic information about government access to member data. This basic information includes the aggregate numbers regarding government requests for data, including requests related to national security. Such disclosure would not reveal substantive information about the identity of the members at issue or the type or content of information requested. But it would

provide members and the public with important information about the nature and extent of government access to data on LinkedIn and other Internet sites and would afford the transparency that members demand – and deserve – in deciding whether, when, and how they use the Internet.

Specifically with respect to so-called National Security Letters (“NSLs”) issued under 18 U.S.C. § 2709, the non-disclosure orders that accompany virtually every NSL pursuant to the statutory non-disclosure provision, 18 U.S.C. § 2709(c)(1) (the “Non-Disclosure Provision”), make disclosure of this basic information impossible. The non-disclosure orders prohibit companies like LinkedIn from providing any information about the NSLs. The companies are barred from confirming that they have even received an NSL in the first place. As a result, they cannot disclose the number of such requests or responses so that users and the public can understand the extent of the disclosure of information being sought by the government and can have confidence, based on actual numbers, that their data is not being put at risk.

This secretive environment and the information the government has shrouded also invites unfounded speculation that American Internet companies are part of expansive government surveillance activities. Such public misperception can have devastating effects on those companies’

reputations and can eviscerate the trust and transparency that they have worked so hard to develop with their users.

The district court properly held that the blanket restriction on the disclosure of the fact that a company has received an NSL violates the First Amendment on the ground that it is not “necessary to serve the compelling need of national security” and “creates too large a danger that speech is being unnecessarily restricted.” *In re Nat’l Sec. Letter*, No. C 11–02173 SI, 2013 WL 1095417, at \*10 (N.D. Cal. Mar. 14, 2013).<sup>2</sup>

Furthermore, recent government proposals for stopgap measures that would permit companies to report NSL numbers in so-called “buckets” or ranges of 0 to 1,000 NSLs would only exacerbate the problem. Although the government’s one-size-fits-all approach may work for some Internet companies that receive thousands or tens of thousands of NSLs, it does not work for companies that receive smaller numbers or even only a handful of NSLs, as the prescribed disclosure would create the false impression that the number of NSLs was potentially far more substantial. The information permitted under these measures would be misleading, would distort the public’s understanding of the actual number of government requests

---

<sup>2</sup> The district court also held the Non-Disclosure Provision was not severable from the rest of the substantive provisions of the NSL statute, and therefore declared the entire statute unconstitutional. 2013 WL 1095417, at \*15.

received, would reduce rather than increase transparency, and would deplete rather than enhance trust in the companies, the industry, and the government.

LinkedIn urges this Court to affirm the district court's order holding that the Non-Disclosure Provision is an unconstitutional restraint on speech. Upholding the order will help ensure that LinkedIn can provide its members with transparency regarding their personal data and maintain the resulting trust it has spent years developing among its members. It further will allow the Internet industry to continue to grow and flourish, to the benefit of all Americans.

Affirmance of the district court's order also would enable LinkedIn and similarly-situated companies to disseminate relevant information to the public, as guaranteed by the First Amendment, and to participate in the ongoing, intense national debate on the vital issues arising from the government's national security-related requests for data. Accurate aggregate data regarding the national security-related requests received by companies such as LinkedIn and the responses to those requests would significantly inform that debate and allow more active, fruitful engagement by LinkedIn, other companies, their members, and the public more generally.

## BACKGROUND

### A. LinkedIn's Business and Its Commitment to Trust and Transparency

LinkedIn is the world's largest professional network, with over 238 million members worldwide and over 84 million members in the United States. Among other things, through its website and mobile applications, LinkedIn provides its members with electronic communications services. Thus, for certain purposes, LinkedIn is an "electronic communications services provider" that is subject to the statutory provisions governing NSLs. *See* 18 U.S.C. § 2709(a).<sup>3</sup>

---

<sup>3</sup> The term "electronic communications service provider" is defined in the Stored Communications Act ("SCA"), which includes provisions governing NSLs. *See* 18 U.S.C. §§ 2701 *et seq.* 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 Brief is intended as an acknowledgement that LinkedIn is subject to the SCA for any and all purposes.

LinkedIn's mission is to connect the world's professionals to make them more productive and successful. Through its proprietary platform, LinkedIn members are able to create, manage, and share their professional identity online, build and engage with their professional network, access shared knowledge and insights, and find business opportunities, enabling them to be more productive and successful. At the core of LinkedIn's platform is its members, who create individual profiles that serve as their professional profiles and are accessible by any other member, as well as (unless a member chooses otherwise) anyone with an Internet connection.

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. LinkedIn earns this trust by being open and transparent with its members and by providing members with what it refers to as 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 (for example, there are no retroactive default settings). And, finally, LinkedIn provides members with control over their data: members decide who can see their data and what it will be used for. This applies to all data on LinkedIn, including communications between and among members.

LinkedIn's members entrust LinkedIn with their data, upon which those members have built their professional reputation. LinkedIn's success is based upon taking steps to make sure the trust that its members have placed in the company is well-deserved and that member data is protected.

**B. Recent Reports of Government Surveillance Have Raised Serious Issues of Public Mistrust**

LinkedIn understands and respects the important work performed by the government to protect our national security. At the same time, recent news reports about government surveillance for national security purposes have given rise to significant concerns among both the American people and the global community regarding 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 United States government has far-reaching access to electronic communications of American citizens, including a recently disclosed NSA program known as "PRISM," which reportedly has allowed the NSA to obtain "direct access" to Internet services.<sup>4</sup> Amid the swirl of resulting press attention and public outcry, other news reports have falsely

---

<sup>4</sup> *E.g.*, <http://www.theguardian.com/world/2013/jun06/us-tech-giants-nsa-data>; *see also* [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). LinkedIn did not participate in the PRISM program.

suggested that LinkedIn itself is the subject of extensive government surveillance and information gathering.<sup>5</sup> The concern that these reports have generated threatens the reputation and business of LinkedIn and other American Internet companies, which have spent time, money and effort to develop trust among their members and the public.

Under these circumstances, and in light of LinkedIn's mission and core value, LinkedIn believes that it is critical to provide its members, and the public, with clear and accurate information about the number and nature of government requests for their data and communications.

LinkedIn has never sought to disclose the substance of any national security-related requests, the identity of affected members, or the substance of any of LinkedIn's responses, nor does it do so now. Instead, LinkedIn has advocated for the ability to disclose periodic, aggregate data concerning the number of such requests: the total number of NSLs, the total number responded to, and the total number of members affected by such requests during the prior six-month period.

---

<sup>5</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).

The scope of the Non-Disclosure Provision, set out in 18 U.S.C. § 2709(c), makes that impossible with respect to NSLs.<sup>6</sup> Under the Non-Disclosure Provision, the recipient of an NSL cannot provide any information about the NSL – including confirming that the company received an NSL in the first place – if the Director of the FBI or his designee certifies that the information sought “may result [in] a danger to”:

1. the national security of the United States;
2. interference with a criminal, counterterrorism, or counterintelligence investigation;
3. interference with diplomatic relations; or
4. the life or physical safety of any person.

18 U.S.C. § 2709(c)(1).

Given the FBI’s practice of invoking the Non-Disclosure Provision in essentially all of its NSL requests,<sup>7</sup> companies like LinkedIn are effectively barred from providing their members with any aggregate information about the number of NSLs they have received or responded to, if any. More

---

<sup>6</sup> The government’s use of NSLs has increased dramatically over the past decade. In 2000, the total number of NSL requests was approximately 8,500; from 2003-2005, the total number of requests was 143,074. <http://epic.org/privacy/nsl/>.

<sup>7</sup> See *In re Nat’l Sec. Letter*, 2013 WL 1095417, at \*9 (“[T]ens of thousands of NSLs are issued each year—and by the government’s own estimate, 97% of them may come with a nondisclosure order.”).

broadly, the Non-Disclosure Provision eliminates LinkedIn’s ability to provide the public with accurate information necessary to engage in an informed discussion on the increasingly pervasive use of NSLs, which as the district court observed, is a “subject that has engendered extensive public and academic debate.”<sup>8</sup>

**C. The FBI’s Recent Proposals to LinkedIn Only Exacerbate the Problem and Would Not Provide Transparency**

Over the past several months, LinkedIn has engaged with the Federal Bureau of Investigation (“FBI”) to try to reach an agreement so that LinkedIn could provide basic, aggregate data regarding the number and the type of government requests for information that it has received, including national security-related requests such as NSLs, if any. LinkedIn understands and supports the government’s increasingly-difficult job of protecting our national security, but also believes that these national security interests must be balanced against the need for transparency. Against the backdrop of these negotiations, on July 18, 2013, LinkedIn and dozens of other companies, 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

---

<sup>8</sup> See *In re Nat’l Sec. Letter*, 2013 WL 1095417 at \*9 (citing examples).

government to Internet, telephone, and web-based service providers for information about their users and subscribers.

Unfortunately, despite extensive discussions, LinkedIn's negotiations with the FBI reached an impasse in early September 2013. Among other things, the FBI has taken the position that LinkedIn cannot report aggregate data regarding the number of NSLs and other kinds of national security-related requests or the total number of member accounts affected by such requests. Instead, the government has informed LinkedIn that it has only two choices: (1) it may disclose the total number of government requests for information on an annual basis excluding all national security-related requests, and may disclose the number of NSLs only in "buckets of 0 to 1,000" (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.

The FBI's proposal does not make sense and is counterproductive. It does not provide for meaningful transparency; on the contrary, it exacerbates LinkedIn's concerns about not being able to provide accurate information regarding the NSLs that it receives. The FBI's proposed reporting in

“buckets of 0 to 1,000” would distort the actual number of requests received and would further public misinformation and confusion. By way of example, if a company like LinkedIn hypothetically received 100 non-security related requests and 10 NSLs in any given year, it could report the 100 requests but then state only that the number of NSLs it received was between 0 and 1,000. This would leave the company’s members and the public with the entirely false impression that the number of NSLs was potentially very substantial and might dwarf the number of other requests – when exactly the opposite would be true.

On September 17, 2013, LinkedIn published its most recent 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 emergency requests. As a result of the FBI’s restrictions, however, this report does not include any data regarding national security-related requests, including requests issued via NSLs, if any.

The FBI has claimed that disclosing such information would harm 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 NSLs issued pursuant to 18 U.S.C. § 2709, among other statutes.<sup>9</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>10</sup> LinkedIn simply seeks the right to report the same information regarding requests it has received from the government.

The proposal by the FBI is unworkable and only heightens concern about the lack of transparency engendered by the Non-Disclosure Provision. It would do nothing to mitigate the negative effects on public trust and transparency and nothing to mitigate the infringement of the First Amendment interests of LinkedIn, its members, or the general public.

## **ARGUMENT**

### **A. The Non-Disclosure Provision Threatens LinkedIn and Other American Internet Companies’ Vital Interests in Transparency And User Trust**

Critical to the success and contributions of LinkedIn and the broader American Internet sector is the trust and confidence that users have placed in the industry. The inability of LinkedIn and other companies to provide accurate information regarding the aggregate number of NSLs and other

---

<sup>9</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>10</sup> *Id.*

national security-related requests that they receive undermines that trust and threatens to disrupt millions of customer relationships.

A core principle of LinkedIn's commitment to its members is being transparent about what LinkedIn will and will not do with member data, how it treats member data, and providing members with control over their data. Although this trust takes a long time to build, it can be broken with a snap of the fingers.

Indeed, user trust is an integral and critical component of the entire American Internet industry. User data is a commodity that has the potential to be exploited and misused at the expense of consumer privacy.

Accordingly, American Internet companies strive not only to protect and secure that data, but to be transparent with their users as to how their data is used. As the Internet Policy Task Force of the Department of Commerce noted in a recent report on data privacy and innovation in the Internet economy,

Privacy protections are crucial to maintaining consumer trust, which is necessary to secure full use of the Internet as a political, educational, cultural, and social medium. Trust—the belief that someone or something will behave as expected, and not another way—is of central importance to the Internet.<sup>11</sup>

---

<sup>11</sup> Internet Policy Task Force, Department of Commerce, “Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework,” December 16, 2010, at 13, at [http://www.ntia.doc.gov/files/ntia/publications/iptf\\_privacy\\_greenpaper\\_121](http://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_121)

The Federal Trade Commission similarly has urged American Internet companies to adopt and maintain policies that offer greater transparency “about their collection and use of consumers’ information,” which “enhanc[es] the consumer trust that is so vital to companies operating” in the Internet and mobile space.<sup>12</sup> LinkedIn has worked valiantly for years to earn and maintain the trust its members place in it. The primacy of user trust is essential to the success of the entire Internet industry in the United States.

This trust in the industry has been badly shaken in the wake of recent news stories describing sweeping Internet surveillance measures that the U.S. government purportedly has been implementing in secret with the alleged assistance and collaboration of American Internet companies. These stories have the potential to tarnish those companies’ reputations as entities committed to protecting their users’ data and right to privacy. As President Obama has noted, these are “revelations that have depleted public trust” in the privacy of electronic communications.<sup>13</sup> Indeed, the President has

---

62010.pdf.

<sup>12</sup> Federal Trade Commission Staff, “Mobile Privacy Disclosures: Building Trust Through Transparency,” February 2013, at 6, 29, at <http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf>.

<sup>13</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>.

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>14</sup>

The potential erosion of consumer trust puts at risk the entire Internet and technology industry, which has been the bright spot in America’s struggling economy for the last several years. Internet companies have been a source of dynamic innovation and job creation in a largely stagnant economy. The foundation of that economic success has been the trust and confidence that Internet users have placed in companies like LinkedIn.

Consistent with that trust, and similar to other Internet companies, LinkedIn publishes periodic transparency reports, which disclose to its members and the broader public data about government requests for member data. As a result of the Non-Disclosure Provision, however, LinkedIn and other companies have been unable to disclose accurate aggregate figures regarding NSLs. This both prevents those companies from informing and educating their users about the extent of government surveillance and, in some instances, from dispelling widespread but false rumors about their involvement with and participation in government surveillance. As the district court stated in correctly concluding that the Non-Disclosure

---

<sup>14</sup> *Id.*

Provision is a content-based restriction subject to strict scrutiny review under the First Amendment, under the statute “recipients are prevented from speaking about their receipt of NSLs and from disclosing, as part of the public debate on the appropriate use of NSLs or other intelligence devices, their own experiences.” *In re Nat’l Sec. Letter*, 2013 WL 1095417, at \*6. This has interfered with the efforts of LinkedIn and other American Internet companies to ensure the transparency to which they are committed.

**B. The Non-Disclosure Provision Undermines The First Amendment Interests of LinkedIn, Its Members, and the Public to Engage In An Informed Debate On An Issue of Substantial Public Importance**

The proper balance between efforts to ensure national security and the privacy interests of American citizens is widely recognized to be one of the most important policy considerations of our time. The scope, manner, and frequency of the government’s use of NSLs to obtain data from electronic service providers like LinkedIn regarding Internet use lies at the center of that debate. As the district court observed, the fact that nearly every recipient of an NSL is prevented from ever disclosing that they received such a request “is especially problematic in light of the active, continuing public debate over NSLs, which has spawned a series of Congressional hearings, academic commentary, and press coverage.” *In re Nat’l Sec. Letter*, 2013 WL 1095417, at \*11.

LinkedIn is committed to engaging and facilitating informed public debate on a wide range of important issues. For example, in October 2012, LinkedIn launched its “Influencers” program, which has engaged leaders in a variety of business and policy fields to share their ideas with the millions of LinkedIn members and to facilitate thought, discussion, and new ideas. The program has been extraordinarily successful. Today there are over 300 LinkedIn Influencers – including Michael Bloomberg, Richard Branson, David Cameron, and Bill Gates – with top Influencer postings receiving hundreds of thousands and even millions of views and eliciting a diverse range of responses and comments.<sup>15</sup>

Reflecting its dedication to encouraging such an exchange of ideas among its members, LinkedIn is committed to transparency by informing the public regarding the government’s use of national security inquires such as NSLs – a commitment that lies at the heart of the First Amendment and is entitled to “special protection.” *Snyder v. Phelps*, 131 S. Ct. 1207, 1215 (2011); *see also, e.g., Mills v. Alabama*, 384 U.S. 214, 218 (1971) (speech related to the “manner in which government is operated or should be

---

<sup>15</sup> *See* Dharmesh Shah, “The Surprising Brilliance of the LinkedIn Influencers Program,” at <http://www.linkedin.com/today/post/article/20130806143440-658789-the-brilliance-of-the-linkedin-influencers-program> (last visited September 14, 2013).

operated” is at the very core of the First Amendment); *Bartnicki v. Vopper*, 532 U.S. 514, 533-34 (2001) (noting that challenged measure “implicates the core purposes of the First Amendment because it imposes sanctions on the publication of truthful information of public concern”); *cf. The Florida Star v. B.J.F.*, 491 U.S. 524, 533-34 (1989) (discussing constitutional protection afforded for dissemination of lawfully obtained truthful information concerning matters of public significance). Indeed, there is “practically universal agreement” that the First Amendment’s protections are at their highest when applied to “the free discussion of governmental affairs.” *Mills*, 384 U.S. at 218.

To engage in an informed debate, the public must be provided with accurate information about the frequency and scope of NSLs issued to companies like LinkedIn. As a result of the Non-Disclosure Provision, the public does not have access to any information other than the fact that the government is issuing tens of thousands of NSLs each year. The wave of public concern that has understandably swelled from the recent revelations of secret government surveillance makes it increasingly important that the public in general and Internet users in particular have access to more information about the extent of government surveillance of Internet companies.

The non-disclosure orders that accompany virtually every NSL issued make that impossible. Companies like LinkedIn have no way to provide their members or the public with even basic, aggregate data on the number of NSLs that the companies receive or the number of their members that are implicated by such requests. The public has no way to know, for example, whether LinkedIn receives only a handful of NSLs or instead receives hundreds.

LinkedIn of course appreciates and supports the vital importance of the government's interest in national security. *See Snepp v. United States*, 444 U.S. 507, 509 (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, as the district court correctly found, 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.<sup>16</sup> In short, as the district court recognized, 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.

Therefore, LinkedIn requests that this Court affirm the district court’s order holding that the Non-Disclosure Provision indiscriminately prohibits any communication regarding NSLs and is therefore overbroad and violates the First Amendment.

//

---

<sup>16</sup> LinkedIn is not taking a position regarding whether the government has met, or can meet, its burden to require NSL recipients to keep the substantive contents of the NSLs, or responses to those requests, secret.

## CONCLUSION

For these reasons, LinkedIn urges the Court to affirm the district court's order holding the Non-Disclosure Provision unconstitutional.

DATED: September 17, 2013

Respectfully submitted,

  
JEROME C. ROTH  
MUNGER, TOLLES & OLSON LLP  
560 Mission Street, 27th Floor  
San Francisco, California 94105  
(415) 512-4000  
*Counsel for Amicus Curiae  
LinkedIn Corporation*

**CERTIFICATE OF COMPLIANCE WITH FEDERAL RULE OF  
APPELLATE PROCEDURE 32**

Pursuant to Rule 32 of the Federal Rules of Appellate Procedure, I  
certify that:

1. This brief complies with the type-volume limitation of Rule 32(a)(7)(B) of the Federal Rules of Appellate Procedure because this brief 4,615 words (based on the Microsoft Word word-count function), excluding the parts of the brief exempted by Rule 32(a)(7)(B)(iii); and

2. This brief complies with the typeface requirements of Rule 32(a)(5) and the type style requirements of Rule 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2003 in 14 point Times New Roman type.

Dated: September 17, 2013

  
JEROME C. ROTH  
MUNGER, TOLLES & OLSON LLP  
560 Mission Street, 27th Floor  
San Francisco, California 94105  
(415) 512-4000  
*Counsel for Amicus Curiae  
LinkedIn Corporation*

## CERTIFICATE OF SERVICE

I hereby certify that on this 17th day of September 2013, a true and correct copy of the foregoing Brief for *Amicus Curiae* LinkedIn Corporation Supporting Appellee and Urging Affirmance was served on counsel of record by US Mail at the addresses below, because filing by ECF pursuant to Ninth Circuit Rule 25-5(f) was not available as this case is under seal.

Cindy A. Cohn  
Lee Tien  
Matthew Zimmerman  
Jennifer Lynch

Electronic Frontier Foundation  
454 Shotwell Street  
San Francisco, CA 94110

Richard R. Wiebe  
Law Office of Richard R. Wiebe  
1 California Street, Suite 900  
San Francisco, CA 94111

*Counsel for Petitioner*

Stuart F. Delery  
Melinda Haag  
Arthur R. Goldberg  
Steven Y. Bressler

U.S. Department of Justice  
P.O. Box 883  
Washington, D.C. 20044

*Counsel for the United States  
Department of Justice,  
the Attorney General, and the  
Federal Bureau of Investigation*

Dated: September 17, 2013

  
JEROME C. ROTH