No. 13-16732
UNDER SEAL

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNDER SEAL,

PETITIONER- APPELLANT,

v.

ERIC H. HOLDER, Jr., Attorney General; UNITED STATES DEPARTMENT OF JUSTICE; FEDERAL BUREAU OF INVESTIGATION,

RESPONDENTS-APPELLEES.

On Appeal From the United States District Court
for the Northern District of California
Case No. 13-cv-1165 SI
Honorable Susan Illston, District Court Judge

BRIEF OF *AMICI CURIAE* CONGRESSWOMAN ZOE LOFGREN (D-CA), CONGRESSMAN THOMAS MASSIE (R-KY), CONGRESSMAN JARED POLIS (D-CO), AND CONGRESSWOMAN ANNA G. ESHOO (D-CA) IN SUPPORT OF PETITIONER

Marcia Hofmann
25 Taylor Street
San Francisco, CA 94102
Telephone: (415) 830-6664
marcia@marciahofmann.com

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

CONSTITUTIONAL PROVISIONS

FEDERAL RULES OF CRIMINAL PROCEDURE

LEGISLATIVE MATERIALS

OTHER AUTHORITIES

STATEMENT OF INTEREST OF *AMICI CURIAE*

Congresswoman Zoe Lofgren represents California's Nineteenth District in the 113th Congress. She was elected to her first term in 1994. She serves on the House Committee on the Judiciary, the Committee on Science, Space, and Technology, and the Committee on House Administration. Congresswoman Lofgren champions government oversight and transparency. She introduced H.R. 3035, the Surveillance Order Reporting Act of 2013, and co-sponsors H.R. 3361, the USA FREEDOM Act.

Congressman Thomas Massie represents Kentucky's Fourth District in the 113th Congress. He was elected to his first term in 2012. He serves on the House Committee on Transportation and Infrastructure, the Committee on Science, Space, and Technology, and the Committee on Oversight and Government Reform. Congressman Massie is a staunch defender of the Constitution and an unwavering advocate for individual liberty and privacy rights. He is a co-sponsor of the Surveillance Order Reporting Act and the USA FREEDOM Act.

Congressman Jared Polis represents Colorado's Second District in the 113th Congress. He was elected to his first term in 2008. He serves on the House Committee on Education and the Workforce and the Committee on Rules. Prior to being elected to Congress, Representative Polis was an Internet entrepreneur, starting several successful businesses and gaining an appreciation for the importance of government transparency in the creation and implementation of laws and regulations. Representative Polis has introduced the Email Privacy Act to enhance privacy

protections for information stored by electronic communication service providers. He is also a co-sponsor of the USA FREEDOM Act.

Congresswoman Anna G. Eshoo represents California's Eighteenth District in the 113th Congress. She was elected to her first term in 1992. She is a senior member of the House Energy and Commerce Committee and is the Ranking Member of the Communications and Technology Subcommittee. Congresswoman Eshoo served on the House Permanent Select Committee on Intelligence from 2003-2009, and, in the 113th Congress, she is a cosponsor of the Email Privacy Act and the USA FREEDOM Act.[1]

[1] This brief is filed with the consent of all parties. It was not written in whole or part by current counsel for any party, though the undersigned attorney served as counsel for one of the petitioners in the district court while employed as a senior staff attorney at the Electronic Frontier Foundation. She currently holds an honorary, uncompensated position as Special Counsel to EFF. No person or entity other than undersigned counsel or *amici* has made a monetary contribution to the preparation or submission of this brief.

INTRODUCTION

This case concerns the constitutionality of 18 U.S.C. §§ 2709 and 3511, which allow the Federal Bureau of Investigation to issue national security letters (NSLs) in counterintelligence investigations to demand non-content information from telecommunications and Internet service providers. These letters are issued directly by the Bureau without any prior judicial review, and are almost always accompanied by a non-disclosure order barring the recipient from revealing anything about the demand.

Petitioner argues that sections 2709 and 3511 violate the First Amendment, both facially and as applied. *Amici* urge this Court to agree.

NSLs are profoundly problematic because the FBI has extraordinary discretion to issue these demands unilaterally and shroud them in secrecy. Indeed, the Department of Justice Inspector General has documented widespread misuse of this investigative tool. Because Congress must depend on information reported by the FBI to conduct oversight, and NSL recipients are barred from disclosing even the most basic information about these demands, it is exceedingly difficult to evaluate the Bureau's use of this controversial power.

Moreover, section 2709's speech restrictions violate the free expression rights of communications service providers that want to be more transparent and forthright with their users, Congress, and the public. *Amici* support the rights of these companies to disclose aggregate statistics about the national security process they receive, and have sponsored legislation toward that end.

NSLs undermine the ability of Congress to perform its key government oversight role, as well as the public's ability to engage in informed debate about matters of public importance. For this reason, *amici* respectfully ask that this Court find sections 2709 and 3511 facially unconstitutional.

ARGUMENT

I. National Security Letters Raise Special Oversight Concerns Because, Unlike Other Forms of Investigative Process, They are Issued Directly by the FBI, Are Not Subject to Prior Judicial Review, and are Almost Always Accompanied by a Permanent Non-Disclosure Order.

Together, 18 U.S.C. §§ 2709 and 3511 authorize the FBI to demand information about a service provider's customers without any prior judicial review, and to impose indefinite non-disclosure orders forbidding the provider to reveal anything about the demand.[2] No other form of legal process leaves so much discretion to the Executive branch, which makes it uniquely ripe for abuse.

[2] Section 2709 is not the only legal authority that permits the FBI to issue NSLs. Though not challenged in this case, several other statutes allow the FBI to serve NSLs on particular types of businesses. *See, e.g.*, 12 U.S.C. § 3414, 15 U.S.C. §§ 1681(u) and 1691(v), 50 U.S.C. § 3162. *See also* Charles Doyle, Senior Specialist, American Law Division, Congressional Research Service, *National Security Letters in Foreign Intelligence Investigations: A Glimpse at the Legal Background* 6-7 (Jan. 3, 2014), *available at* https://www.fas.org/sgp/crs/intel/RS22406.pdf.

A. The USA PATRIOT Act's Expansion of Section 2709 Resulted in the FBI's Systematic Misuse of National Security Letters and Undermined Congress' Ability to Oversee the Bureau's Use of This Tool.

Section 2709 was enacted in 1986 as part of the Electronic Communications Privacy Act, 18 U.S.C. §§ 2501 et seq. As originally drafted, section 2709 permitted the FBI to issue an NSL only if it was authorized by an official at the level of Deputy Assistant Director or higher at FBI headquarters, and only where that official certified there were "specific and articulable facts giving reason to believe that the customer or entity whose records are sought is a foreign power or an agent of a foreign power." 18 U.S.C. § 2709(b) (1986); *see also Liberty and Security in a Changing World: Report and Recommendations from the President's Review Group on Intelligence and Communications Technologies* 90 (Dec. 12, 2013) ("President's Review Group").[3]

In 2001, the USA PATRIOT Act substantially expanded the FBI's authority to issue these legal demands in several ways. Pub. L. No. 107-56, 115 Stat. 272. First, the law gave more FBI officials the power to approve NSLs. No longer restricting this activity to senior-level officials at Bureau headquarters, the law now permits Special Agents in Charge of any FBI field office to authorize an NSL. 18 U.S.C. § 2709(b).

Second, the USA PATRIOT Act loosened the basic standard for issuing an NSL. Prior to the passage of the Act, high-level officials were required to certify that "specific and articulable facts" existed "giving reason to believe that the customer or

[3] Available at http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

entity whose records are sought is a foreign power or an agent of a foreign power." 18 U.S.C. § 2709(b) (1986). The USA PATRIOT Act lowered this bar, permitting the FBI to issue NSLs whenever records are "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities." 18 U.S.C. § 2709(b).

In the USA PATRIOT Improvement and Reauthorization Act of 2005, Congress directed the Department of Justice Office of the Inspector General to review the FBI's use of NSLs, which it documented in two reports issued in 2007 and 2008. *A Review of the Federal Bureau of Investigation's Use of National Security Letters* (March 2007) ("2007 OIG Report"); *A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006* (March 2008) ("2008 OIG Report").[4]

Not surprisingly, the Inspector General found the FBI's issuance of NSLs increased sharply after the USA PATRIOT Act made this form of legal process easier to use. In 2000, the year before the USA PATRIOT Act became law, the FBI issued about 8,500 NSL requests. This number skyrocketed to approximately 39,000 requests in 2003, after the USA PATRIOT Act's changes went into effect, and jumped again to

[4] Available at http://www.usdoj.gov/oig/special/s0703b/final.pdf & http://www.usdoj.gov/oig/special/s0803b/final.pdf.

more than 48,106 requests in 2006.[5] 2007 OIG Report at 120; 2008 OIG Report at 107. But many of these figures are simply the Inspector General's best estimate, as the FBI's NSL recordkeeping practices were poor during the time period covered by the reports, and the available data "significantly understated" the FBI's NSL requests. 2007 OIG Report at 34.

Based on the available data, the Inspector General exhaustively documented illegal and improper use of NSLs. 2007 OIG Report at 66-102; 2008 OIG Report at 131-155. These findings revealed a broad array of infractions, including:

- Issuing NSLs after the FBI's authority to conduct an underlying investigation had ended;
- Using NSLs to collect email subscriber information and telephone billing records about the wrong people;
- Gathering subscriber information beyond what was requested in the NSL;
- Gathering subscriber information beyond the time limits of the NSL;
- Seeking information beyond the scope of what a particular NSL statute would permit, *e.g.*, issuing a section 2709 NSL to access an investigative target's educational records; and

[5] Note the distinction between NSL "requests" and NSL "letters." One NSL letter may include multiple requests for subscriber information. *See* 2007 OIG Report at 120. For example, in one investigation, the FBI issued nine NSL letters seeking subscriber information related to 11,100 phone numbers. *Id.* at 36. The precise number of NSL requests issued under each of the separate NSL authorities remains non-public, but the FBI issued the "overwhelming majority" pursuant to section 2709. *Id.* at 36-37; 2008 OIG Report at 107.

- Using NSLs to obtain subscriber information not relevant to an authorized national security investigation.[6]

The Inspector General noted, however, that the "overwhelming majority" of possible NSL misuses had never been identified or reported through the internal oversight channels established within the FBI, and so were never documented. 2007 OIG Report at 84; 2008 OIG Report at 132.

In an additional report issued in 2010, the Inspector General determined that the FBI had improperly collected "community of interest" or "calling circle" information through more than 250 NSLs (and other means). *A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records* 75 (Jan. 2010).[7] These requests were made without a proper assessment of whether the telephone numbers were relevant to authorized national security investigations. *Id.* at 75-76. They were also sometimes issued on the basis of First Amendment-protected activity, and were used to gather reporters' and news organizations' toll billing records and calling information. *Id.* at 6, 89-122.

The Inspector General also determined the FBI had issued 11 "blanket" NSLs in an attempt to legitimize the collection of records it had already acquired through informal requests with no basis in law—including records related to many telephone numbers that were not relevant to any national security investigation. *Id.* at 165-68,

[6] 2007 OIG Report at 66-67; 2008 OIG Report at 131, 140-41.

[7] Available at http://www.justice.gov/oig/special/s1001r.pdf.

203-208. The FBI also issued after-the-fact NSLs regularly to paper over its collection of information through improper processes. *Id.* at 211-212. The Inspector General again attributed these problems to a lack of oversight within the agency. *Id.* at 213-214, 279-285.

The FBI has reportedly taken steps to mitigate the many problems identified by the Inspector General between 2007 and 2010.[8] But it has been four years since that office reviewed the FBI's use of NSL authority, which makes it difficult to gauge the Bureau's progress.

Congress does have one measuring stick: section 2709(e) requires the Bureau to "fully inform" Congress twice a year about its use of NSL power. But this form of oversight relies on the FBI's self-reported data—which means Congress' information is only as accurate and complete as the FBI's. Thanks to the Inspector General's reports, we know the Bureau's own internal oversight has left much to be desired. Given this history, Congress cannot—and should not—be forced to rely exclusively on the Bureau to understand the effectiveness and shortcomings of the NSL regime.

[8] In 2008, the Inspector General concluded it was too soon to know "whether the new guidance, training, and systems put into place by the FBI in response to our first NSL report will fully eliminate the problems with the use of NSLs that we identified and that the FBI confirmed in its own reviews. At the same time, we believe that the FBI has made significant progress in addressing these issues and that the FBI's senior leadership is committed to addressing misuse of NSLs." 2008 OIG Report at 49.

B. National Security Letters are a Uniquely Problematic Form of Legal Process Because They Permit Investigators to Demand Information and Silence Recipients With No Prior Judicial Oversight.

The Bureau's checkered history of NSL misuse might have been avoided from the outset if national security letters were subject to judicial oversight before approval. But section 2709 lacks this fundamental check, which contributes to its constitutional failings.

This investigative capability is also wholly unnecessary. The government enjoys a host of law enforcement tools to compel service providers to disclose information about their customers under the proper circumstances, including probable cause warrants; grand jury subpoenas; criminal trial subpoenas; administrative subpoenas; 18 U.S.C. § 2703(d) court orders; and orders issued under the Foreign Intelligence Surveillance Act (FISA). *See Doe v. Ashcroft*, 334 F. Supp. 2d 471, 484-91 (S.D.N.Y. 2004) (discussing the differences between NSLs and other information-gathering authorities), *vacated sub nom. Doe v. Gonzales*, 449 F.3d 415 (2d Cir. 2006).

There is a crucial difference between the NSLs challenged in this case and other forms of legal process. NSLs are issued directly by investigators who are also empowered to impose never-ending non-disclosure orders on recipients—without any prior judicial approval. No other legal process operates this way. For example:

(1) Federal Rule of Criminal Procedure 41 warrants. As a general rule, warrants issue only upon a showing of probable cause to a neutral magistrate. *Johnson v. United States*,

333 U.S. 10, 14 (1948); *see also California v. Acevedo*, 500 U.S. 565, 586-88 (1991) (Stevens, J. dissenting) (discussing the deeply rooted line of Supreme Court precedent requiring a judicial officer to issue warrants, reflecting a policy judgment that privacy interests outweigh the burdens on law enforcement).

Unlike an FBI field office issuing an NSL, law enforcement agents serving a warrant have no direct authority to impose a non-disclosure order on an Internet service provider. Rather, a *court* may, under certain narrow circumstances, order a provider not to disclose the existence of a warrant for a period the court "deems appropriate." 18 U.S.C. § 2705(b); *see also* Department of Justice, Criminal Division, Computer Crime and Intellectual Property Section, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 259 (2009) (model "nondisclosure and sealing" request to be presented to a magistrate in a warrant application).

(2) Grand jury subpoenas. While a grand jury subpoena does not require prior approval of a court, a prosecutor must authorize its issuance in the context of a grand jury investigation—which itself is meant to be a procedural protection against excessive government power. *President's Review Group* at 91 n.76; Charles Doyle, Senior Specialist, American Law Division, Congressional Research Service, *Administrative Subpoenas in Criminal Investigations* 5 (March 17, 2006) ("Administrative Subpoenas") (the grand jury is "a buffer against the abuse of government authority.").[9] Moreover, a

[9] Available at https://www.fas.org/sgp/crs/intel/RS22407.pdf.

witness may ask a judge to quash a grand jury subpoena that is "unreasonable or oppressive." Fed. Rule Crim. P. 17(c)(2); *United States v. R. Enters., Inc.*, 498 U.S. 292, 299 (1991). And grand jury witnesses and subpoena recipients are generally free to speak about the fact they received a grand jury subpoena. Fed. Rule Crim. P. 6(e)(2)(A); *see also Butterworth v. Smith*, 494 U.S. 624, 626 (1990).

(3) Criminal subpoenas. Federal Rule of Criminal Procedure 17(c) authorizes law enforcement agencies to issue subpoenas for potential evidence in criminal proceedings. As is the case with grand jury subpoenas, a recipient may ask a court to quash an "unreasonable or oppressive" criminal trial subpoena. Fed. Rule Crim. P. 17(c)(2). And far from being shrouded in secrecy, criminal trial proceedings are presumptively public. *Doe v. Ashcroft*, 334 F. Supp. 2d at 486 (citing U.S. CONST. AMEND. VI); *see also Press-Enter. Co. v. Superior Ct.*, 478 U.S. 1, 13 (1986) (the public enjoys a qualified First Amendment right of access even to preliminary criminal proceedings).

(4) Administrative subpoenas. Executive agencies can issue administrative subpoenas to carry out investigative and administrative duties under a range of authorities. Administrative Subpoenas at 6.[10] Agencies can issue these subpoenas without prior judicial approval, but are able to enforce them only through the authority of a court. *Id.* at 7-8; *see also United States v. Powell*, 379 U.S. 48, 57-58 (1964).

[10] Available at https://www.fas.org/sgp/crs/intel/RS22407.pdf.

In rare instances, some administrative subpoena authorities permit agencies to issue non-disclosure orders. *See, e.g.*, 20 U.S.C. § 1232g(b)(1)(J)(ii). But most of these authorities do not include such restrictions, or instead provide for a court to issue a non-disclosure order under appropriate circumstances.[11]

(5) Section 2703(d) orders. Under the Electronic Communications Privacy Act, investigators may seek a court order to compel a service provider to disclose the contents of communications or other subscriber information in a criminal investigation. 18 U.S.C. § 2703(d). The court may prevent the provider from disclosing the existence of the order under certain narrow circumstances, but the investigative agency does not have this authority. *Id.* § 2705(b).

(6) Foreign Intelligence Surveillance Act orders. Finally, the government takes the position that it can obtain records from a communications service provider under the Foreign Intelligence Surveillance Act, which (among other things) authorizes the collection of "any tangible things" related to an authorized investigation. 50 U.S.C. § 1861 (as amended by the USA PATRIOT Act, Pub. L. No. 107-56, § 215, 115 Stat. 272). To obtain such an order, the FBI must apply and make a requisite showing to the Foreign Intelligence Surveillance Court or a United States magistrate judge. 50

[11] For a comprehensive list of administrative subpoena authorities and a summary of their provisions, see Department of Justice, Office of Legal Policy, *Report to Congress on the Use of Administrative Subpoena Authorities by Executive Branch Agencies and Entities* (2002), available at http://www.justice.gov/archive/olp/rpt_to_congress.htm.

U.S.C. § 1861(b). The recipient is generally not allowed to disclose the order's existence (with some narrow exceptions). *Id.* § 1861(d).

Only one investigative tool gives the FBI carte blanche to issue national security legal process under its own authority and unilaterally impose a permanent secrecy requirement on the recipient: the national security letter. NSLs are a truly unusual form of legal process because they leave exceptional discretion in the FBI's hands. As the President's Review Group has noted, there is "no principled reason" why the FBI should have this extraordinary latitude when it has other, less problematic forms of national security-related process at its disposal. President's Review Group at 92-93.

II. The Open-Ended Non-Disclosure Orders That Accompany National Security Letters Raise Substantial First Amendment Concerns Because They Bar Recipients From Disclosing Important Information to Their Customers, Congress, and the Public.

In addition to permitting the FBI to compel a service provider to disclose certain subscriber information, section 2709(c) allows the FBI to impose an unlimited non-disclosure order to prevent the service provider from discussing the NSL publicly—including the very fact that it received an NSL—upon a certification that "there may result 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." 18 U.S.C. § 2709(c)(1). And the FBI almost always makes this certification: non-

disclosure orders accompany 97 percent of all NSLs issued by the FBI. President's Review Group at 92; *see also In re Nat'l Sec. Letter*, 930 F. Supp. 2d 1064, 1073 (N.D. Cal. 2013).

Section 3511 allows recipients to file a petition to modify or set aside an NSL or an accompanying non-disclosure order. But a court may grant the petition only under limited conditions, and must treat the FBI's certifications as conclusive unless made in bad faith. 18 U.S.C. §§ 3511(b)(2)-(3). Thus, an NSL recipient must fight a steep uphill battle to challenge a speech restriction.

The Second Circuit recognized in *Doe v. Mukasey* that this burden creates serious First Amendment problems, striking down the provisions of section 3511(b) that require a court to treat the FBI's certifications as conclusive. 549 F.3d 861, 885 (2d Cir. 2008). That court salvaged section 2709(c) by interpreting it to require the government to initiate judicial review if an NSL recipient decides to contest a non-disclosure requirement. *Id.* at 881. The district court here went further, finding sections 2709(c) and 3511(b)(2)-(b)(3) facially unconstitutional. *In re Nat'l Sec. Letter*, 930 F. Supp. 2d at 1081 (No. 13-15957).

The President's Review Group has also noted the critical First Amendment concerns raised by everlasting non-disclosure requirements. The committee suggested that the law be changed to ensure that non-disclosure orders accompanying a range of national security demands—including NSLs—should issue only upon judicial

approval, and should last only 180 days unless a court renews the order. President's Review Group at 122-123.

The non-disclosure requirements of section 2709(c) do not sit well with NSL recipients—far from it. Last year, several major communications service providers began reporting aggregate numbers of national security legal process they receive, including NSLs—but the Justice Department allowed them to do so only in broad number ranges such as 0-999.[12] Since then, several major Internet companies have negotiated with the Obama Administration for the right to publicly disclose this data in greater detail. *See, i.e.*, Reform Government Surveillance, https://www.reformgovernmentsurveillance.com (last visited March 27, 2014) (a campaign in which AOL, Apple, Dropbox, Facebook, Google, LinkedIn, Microsoft,

[12] *See, e.g.*, Google, *Transparency Report: Shedding More Light on National Security Letters* (March 5, 2013), http://googleblog.blogspot.com/2013/03/transparency-report-shedding-more-light.html; Apple, *Update on National Security and Law Enforcement Orders* (Jan. 27, 2014), http://images.apple.com/pr/pdf/140127upd_nat_sec_and_law_enf_orders.pdf; Dropbox, *2013 Transparency Report*, https://www.dropbox.com/transparency (last visited April 11, 2014); *Verizon Transparency Report*, http://transparency.verizon.com/us-data (last visited April 11, 2014); Brad Smith, General Counsel and Executive Vice President, Legal & Corporate Affairs, Microsoft, *Providing Additional Transparency on US Government Requests for Data* (Feb. 3, 2014), http://blogs.technet.com/b/microsoft_on_the_issues/archive/2014/02/03/providing-additional-transparency-on-us-government-requests-for-customer-data.aspx; LinkedIn, *Transparency Report 1H 2013* (Feb. 3, 2014), http://help.linkedin.com/app/answers/detail/a_id/41878/ft/eng; Facebook, *Global Government Requests Report*, https://www.facebook.com/about/government_requests (last visited April 11, 2014); Kenneth R. Carter, CloudFlare, *CloudFlare Transparency Report on National Security Orders* (Jan. 27, 2014), http://blog.cloudflare.com/cloudflare-transparency-report-on-national-security-orders.

Twitter, and Yahoo have called on the government to allow them to "publish the number and nature of government demands for user information.").

When these negotiations failed to yield results, Google Facebook, Microsoft, and Yahoo asked the Foreign Intelligence Surveillance Court to declare that they have a First Amendment right to publish basic aggregate data about the various types of national security process they receive, including NSLs. *See* Ryan Gallagher, *Tech Giants United in Court to Fight Against Government Surveillance Secrecy*, Slate, Sept. 10, 2013.[13]

In response to this pressure, the Justice Department recently agreed to allow companies to report national security process in two new ways. Letter From James M. Cole, Deputy Attorney General, Department of Justice, to General Counsels of Facebook, Google, LinkedIn, Microsoft, and Yahoo, Jan. 27, 2014.[14] The first option is to report aggregate data about distinct categories of legal process—including the number of NSLs received and number of user accounts affected by NSLs—as a single number in bands of 1000. *Id.* at 2-3. Alternatively, these companies may choose to report the total number of all national security requests received, including all NSLs and FISA orders, and the total number of all "customer selectors" targeted by all national process, as single figures in bands of 250. *Id.* at 3.

---

[13] http://www.slate.com/blogs/future_tense/2013/09/10/yahoo_google_facebook_microsoft_fight_for_permission_to_release_data_about.html.

[14] Available at http://www.justice.gov/iso/opa/resources/366201412716018407143.pdf.

While this middle ground is a step in the right direction, it does not resolve the companies' fundamental free speech concerns. As Twitter has pointed out:

> We think the government's restriction on our speech not only unfairly impacts our users' privacy, but also violates our First Amendment right to free expression and open discussion of government affairs. We believe there are far less restrictive ways to permit discussion in this area while also respecting national security concerns. . . . We are also considering legal options we may have to seek to defend our First Amendment rights."

Jeremy Kessel, Manager, Global Legal Policy, *Fighting for more #transparency* (Feb. 6, 2014).[15]

Amici strongly support the rights of these companies to be open and honest with their customers and the general public about the number of national security demands they receive. Toward this end, 21 senators and 142 members of Congress sponsored bipartisan bills in the House and Senate seeking to ensure communications service providers can issue quarterly aggregate reports to the public about NSLs and other national security demands from the government. *See* the Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection, and Online Monitoring Act (USA FREEDOM Act), H.R. 3361, 113th Cong. (introduced Oct. 29, 2013); S. 1599, 113th Cong. (introduced Oct. 29, 2013).[16]

[15] https://blog.twitter.com/2014/fighting-for-more-transparency.

[16] Congresswoman Lofgren has also introduced the Surveillance Order Reporting Act of 2013, bipartisan legislation that would similarly ensure communications providers have the right to reports aggregate statistics to the public about national security

These bills would allow electronic service providers to reveal an estimate of the national security demands they receive from the government, as well as estimates of the number of users or accounts affected by those demands, in numbers rounded to the nearest 100 (rather than 1000). Providers could also publish an estimate of the number of demands with which they comply, rounded to the nearest 100. And the legislation would allow providers who have not received any national security demands to disclose that basic fact.

Companies should have the freedom to divulge statistics about the number of national security demands they get from the government. Restrictions on such disclosures not only impinge upon their First Amendment rights, but also keep them from being truthful and upfront with their customers, Congress, and the public.

Amici also believe these statistics are an important counterpoint to the self-reported data they receive from the Executive branch about its use of controversial investigative tools in national security matters. This information will help Congress keep the Executive branch accountable, and inform meaningful public debate about our government's investigative powers.

---

demands received from the government. H.R. 3035, 113th Cong. (introduced Aug. 2, 2013).

CONCLUSION

Amici respectfully ask that this Court reverse the district court's ruling in 13-16732.

Dated: April 11, 2014

/s/ *Marcia Hofmann*
Marcia Hofmann
25 Taylor Street
San Francisco, CA 94102
Telephone: (415) 830-6664
marcia@marciahofmann.com

Counsel for Amici Curiae Congresswoman Zoe Lofgren, Congressman Thomas Massie, Congressman Jared Polis, and Congresswoman Anna G. Eshoo

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION, TYPEFACE REQUIREMENTS, AND TYPE STYLE REQUIREMENTS

Pursuant to Federal Rule of Appellate Procedure 32(a)(7)(C), I certify as follows:

1. This brief is 4,427 words, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(a)(7)(B)(iii). It therefore complies with the type-volume limitation of Federal Rule of Appellate Procedure 32(a)(7)(B).

2. This brief's type size and typeface comply with Federal Rule of Appellate Procedure 32(a)(5) and (6). It was written in Garamond typeface with 14-point font.

Dated: April 11, 2014

/s/ *Marcia Hofmann*
Marcia Hofmann

CERTIFICATE OF SERVICE

I certify that I filed the foregoing *amici* brief with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit in accordance with the Chief Deputy Clerk's Instructions for Prospective *Amici*.

I further certify that I sent this brief via FedEx to the Court at the below address on April 11, 2014:

Susan Soong, Chief Deputy Clerk - Operations
U.S. Court of Appeals for the Ninth Circuit
95 7th Street
San Francisco, CA 94103

The court will effect service on the parties.

Dated: April 11, 2014

/s/ *Marcia Hofmann*
Marcia Hofmann