Case No. 13-16732

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

IN RE NATIONAL SECURITY LETTER

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

BRIEF OF *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) IN SUPPORT OF PETITIONER

Marc Rotenberg
Counsel of Record
Alan Butler
David Husband
Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
Telephone: (202) 483-1140

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1 and 29(c), *Amicus Curiae* Electronic Privacy Information Center ("EPIC") is a District of Columbia corporation with no parent corporation. No publicly held company owns 10% or more of EPIC stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

INTEREST OF AMICUS

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other Constitutional values.[1] EPIC maintains two of the most popular web sites in the world concerning privacy, epic.org and privacy.org.

For twenty years, the Electronic Privacy Information Center has routinely provided information to the public about the government's electronic surveillance activities, based on the annual reports, required by statute, provided by the Administrative Office of the U.S. Courts and the Attorney General. EPIC reviews these reports, prepares charts and graphs, and publishes news items comparing the most recent data with the earlier so as to determine significant changes in the surveillance practices of federal and state governments. EPIC has attempted to provide similar information to the public about the government's use of National Security Letter authority. However, the statutory provisions before this Court have made such evaluation impossible. Without additional information about the use of

[1] The parties consent to the filing of this brief. In accordance with FRAP 29, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

National Security Letters, EPIC and others will be limited in their ability to inform the public about the scope of government surveillance activities.

SUMMARY OF THE ARGUMENT

The government's use of National Security Letters to collect sensitive personal information is a matter of substantial public controversy. The Inspector General has determined that this authority has been used improperly and many questions remain about the full scope of this investigative technique. Information about the use and effectiveness of this authority is necessary to prevent misuse and ensure accountability. The provisions currently before this Court prevent necessary disclosure that would enable public oversight and should be overturned. Comprehensive statistical reports on the use of surveillance authorities by law enforcement have been provided for decades without compromising individual investigations. For organizations such as EPIC, the availability of this information is critical to assess government surveillance programs that impact personal privacy. However, the current NSL provisions do not permit the necessary disclosures to enable meaningful analysis. Separate from the provider's right to speak freely about the government's requests for customer information without fear of criminal prosecution is the public's right to know about the government's extensive collection of the public's personal information. The NSL "gag order" provision frustrates this fundamental right.

ARGUMENT

National Security Letter ("NSL") authorities currently allow the Federal Bureau of Investigation to collect an extraordinary amount of sensitive personal information on American citizens from private companies without meaningful judicial review, notice to a potential target, or public reporting on the activity. *See* 18 U.S.C. § 2709 (Electronic Communications Privacy Act); 12 U.S.C. § 3414(a)(5) (Right to Financial Privacy Act); 15 U.S.C. §§ 1681u-1681v (Fair Credit Reporting Act); 50 U.S.C. § 3162 (National Security Act of 1947). Under these NSL provisions, companies are compelled to disclose their customers' private records and, in almost every case, are simultaneously prohibited from disclosing any details about (even the mere existence of) the government's requests.

These blanket prohibitions on disclosure of information about the use of NSLs not only infringe the First Amendment rights of recipients, they also impact the public's ability to know about the collection of their information and the conduct of their government. The public's concern about this particular activity is well founded. The Department of Justice's Inspector General has uncovered significant abuses in the use of NSL authority, and recent reports by expert panels have recommended significant reform of NSL authority. But these reforms cannot

be achieved if those who are subject to these provisions face criminal prosecution for even discussing such cases.

I. The "Gag Order" Provision Frustrates Accountability and Is Inconsistent with Reporting Requirements Found Elsewhere in Federal Law

Under the current National Security Letter authority, the FBI and other federal agencies obtain the private financial and communications records of U.S. consumers and simultaneously prohibit the recipients of NSLs from revealing even the existence of these requests. The nondisclosure provision does not differentiate between the release of case-specific information and the aggregate data that has historically been released about the government's use of surveillance authorities without compromising individual investigations. As a result, there is no effective means for the public to evaluate the use and efficacy of the authorities that were significantly expanded in the USA PATRIOT Act. Such restrictions have raised substantial First Amendment concerns as to the speech of those receiving the request. Prior to the amendments adopted in the USA Patriot Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (Mar. 9, 2006), NSL recipients were prohibited from disclosing any information about the letters they received, even where disclosure was necessary to obtain legal advice or to implement the order. 1 David S. Kris & J. Douglas Wilson, *National Security Investigations & Prosecutions 2d* § 20:10, at 752 (2012). These provisions were ruled unconstitutional under the First Amendment, *Doe v. Ashcroft*, 334 F. Supp.

2d 471 (S.D.N.Y. 2004), *vacated*, 449 F.3d 415 (2d Cir. 2006), and were subsequently amended by Congress. The amended nondisclosure provisions were again ruled unconstitutional, *Doe v. Gonzales*, 500 F. Supp. 2d 379 (S.D.N.Y. 2007),[2] before being narrowly construed by the Court of Appeals for the Second Circuit in *Doe v. Mukasey*. 549 F.3d 861, 883-85 (2d Cir. 2008). But the current FBI procedures, adopted subsequent to *Mukasey*, are not sufficiently narrow to permit aggregate reporting from NSL recipients. Without a carve-out for public transparency reports, the NSL nondisclosure provisions shield the use of NSLs from meaningful scrutiny.

Under the amended statute, the FBI may prohibit an NSL recipient from disclosing any information about the letter as long as an authorized official certifies that disclosure "may 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." 18 U.S.C. § 2709(c)(1).[3] And even though the nondisclosure requirements are no longer imposed by default, the FBI has asserted them in nearly every case. *See* U.S. Dep't of Justice, Office of the Inspector Gen.,

[2] The case never reached a final resolution on appeal because Congress passed new NSL provisions under the Patriot Reauthorization Act. Pub. L. No. 109-177, § 116, 120 Stat. 192 (Mar. 9, 2006).

[3] *See also* 15 U.S.C. § 1681u(d)(1); 15 U.S.C. § 1681v(c)(1); 12 U.S.C. § 3414(a)(3)(A); 50 U.S.C. § 3162(b)(1).

A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006 10 (2008) [hereinafter *2008 IG Report*] ("97% of the NSLs in the random sample imposed non-disclosure and confidentiality obligations on recipients").[4]

The statute does not require that the official identify the harm that will result or identify the scope of the disclosure that would cause harm. There is a narrow exception in the statute to allow disclosure as "necessary to comply with the request" or to "an attorney to obtain legal advice or legal assistance with respect to the request." 18 U.S.C. § 2709(c)(1). But even where disclosure is necessary to comply with the letter, the FBI may require that the recipient notify the agency and provide the identities of those notified.[5]

The recipient of an NSL may request that a court modify or set aside the nondisclosure order that accompanies an NSL. 18 U.S.C. § 3511(b). *See generally* 1 Kris & Wilson § 20:10, at 755. If the petition is filed within one year of the date the recipient receives the NSL, the court may modify the order only if it finds that "there is no reason to believe that disclosure may endanger the national security of

[4] *Available at* http://www.justice.gov/oig/special/s0703b/final.pdf.
[5] 18 U.S.C. § 2709(c)(4); 15 U.S.C. § 1681u(d)(4); 15 U.S.C. § 1681v(c)(4); 12 U.S.C. § 3414(a)(3)(D); 50 U.S.C. § 3162(b)(4).

the United States" or other enumerated interests.[6] 18 U.S.C. § 3511(b)(2). In making this determination, the court must treat an official certification as "conclusive unless the court finds that the certification was made in bad faith." *Id*. If the petition is filed more than one year after receipt of the NSL then the government must either "terminate the nondisclosure requirement or re-certify that disclosure may result in danger to national security" within 90 days. 18 U.S.C. § 3511(b)(3).

After Congress enacted these amended nondisclosure provisions, they were ruled unconstitutional in *Doe v. Gonzales*. 500 F. Supp. 2d 379 (S.D.N.Y. 2007). On appeal, in *Doe v. Mukasey*, 549 F. 3d 861 (2d Cir. 2008), the Second Circuit affirmed in part and only upheld the remaining provisions after it imposed new constraints on the FBI's ability to authorize and enforce its nondisclosure orders. *Id.* at 879-82. The court made clear that the government bears the burden of persuading "a district court that there is a good reason to believe that disclosure may result in one of the enumerated harms." *Id.* at 876. But the injunction issued by the court in *Doe* does not apply outside the Second Circuit. And even under these new constraints, the nondisclosure orders are not narrow enough to allow for aggregate public reporting of FBI orders.

[6] Such as "interfere with a criminal, counterintelligence or counterterrorism investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person."

The Government has argued that the procedures it has adopted for issuing and enforcing NSLs nationwide comply with the rules adopted in *Doe*. (Gov't Br. at 11). Yet, the district court found that it had not been "presented with any *evidence*" that the Department of Justice "has implemented regulations" or a formal policy "to impose the construction and safeguards mandated by the Second Circuit in *Doe*." *In re Nat'l Security Letter*, 930 F. Supp. 2d 1064, 1073 (2013) (emphasis in original). Any special NSL procedures adopted by the Department of Justice on a voluntary basis are insufficient to cure the core transparency flaw in the NSL authorities because even the procedures for these discretionary determinations are kept secret. Without access to the procedures or any other information about the use of these NSL authorities, there is effectively no way for recipients or the public to ensure that the government is complying with the necessary restrictions.

As President Obama recently stated on this very topic:

> Given the unique power of the state, it is not enough for leaders to say: Trust us. We won't abuse the data we collect. For history has too many examples when that trust has been breached. Our system of government is built on the premise that our liberty cannot depend on the good intentions of those in power. It depends on the law to constrain those in power.

Remarks by the President on Review of Signals Intelligence, 2014 Daily Comp.

Pres. Doc. 30 (Jan. 17, 2014).[7] Yet, in this instance, the American public is being asked to trust the voluntary policy changes of the Department of Justice. President Obama himself has said trust is not enough and that the American public deserves instead to "depend upon the law to constrain those in power." *Id.*

II. Transparency is Necessary to Facilitate Public Oversight of Government Surveillance Methods

The electronic surveillance methods used by the FBI and other government agencies have been the subject of intense public debate,[8] internal audits and reports,[9] review by Congress,[10] yet little information has been made available to the public. Long ago Congress recognized that meaningful review of electronic

---

[7] *Available at* http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

[8] *See e.g.,* Barton Gellman, *The FBI's Secret Scrutiny*, Wash. Post (Nov. 6, 2005) *available at* http://www.washingtonpost.com/wp-dyn/content/article/2005/11/05/AR2005110501366.html; Alison Leigh Cowan, *Judges Question Patriot Act in Library and Internet Case*, N.Y. Times (Nov. 3, 2005), *available at* http://www.nytimes.com/2005/11/03/nyregion/03library.html?ex=1175918400&en=ecfd3350a291ea3c&ei=5070&_r=0; Anonymous, My National Security Letter Gag Order, Wash. Post, (Mar. 23, 2007), *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/03/22/AR2007032201882_pf.html.

[9] *See e.g.,* U.S. Dep't of Justice, Office of the Inspector Gen., *A Review of the Federal Bureau of Investigation's Use of National Security Letters* (2007), *available at* www.justice.gov/oig/special/s0703b/final.pdf.

[10] *Report by the Office of the Inspector General of the Department of Justice on the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Jud.* (Apr. 10, 2010), *available at* www.fas.org/irp/congress/2010_hr/exigent.pdf

surveillance requires the collection and publication of aggregate data that is available to the public and the press. In 1968 Congressed passed a federal wiretap Act,[11] with the dual purpose of "(1) protecting the privacy of wire and oral communications, and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized." S. Rep. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2153.

Congress recognized that the public reporting was necessary to facilitate oversight of this new authority. Congress established reporting requirements "intended to form the basis for a public evaluation" of the surveillance authorities to "ensure the community that the system of court-order electronic surveillance envisioned by the proposed chapter is properly administered and will provide a basis for evaluating its operation." *Id.* at 2196, codified at 18 U.S.C. § 2519. However, similar information is not available for the use of NSL authority.

A. Public Reporting of the Government's Activities is Essential in a Democratic Society

At the beginning of his tenure, President Obama made clear that his "Administration is committed to creating an unprecedented level of openness in government," and emphasized that "information maintained by the Federal Government is a national asset." Memorandum on Transparency and Open

[11] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, 82 Stat. 197. The wiretap provisions are codified at 18 U.S.C. §§ 2510-2520.

Government, 2009 Daily Comp. Pres. Doc. 10 (Jan. 21, 2009).[12]

The President reaffirmed this commitment to transparency in his recent speech on reform of the NSA surveillance programs:

> There is an inevitable bias, not only within the intelligence community but among all of us who are responsible for national security, to collect more information about the world, not less. So in the absence of institutional requirements for regular debate and oversight that is public as well as private or classified, the danger of government overreach becomes more acute . . . .

Remarks by the President on Review of Signals Intelligence, 2014 Daily Comp. Pres. Doc. 30 (Jan. 17, 2014).[13] Specifically, the President addressed the need for additional oversight of the use of National Security Letters:

> Now, these are cases in which it's important that the subject of the investigation, such as a possible terrorist or spy, isn't tipped off. But we can and should be more transparent in how government uses this authority. I've therefore directed the attorney general to amend how we use national security letters so that this secrecy will not be indefinite, so that it will terminate within a fixed time unless the government demonstrates a real need for further secrecy. We will also enable communications providers to make public more information than ever before about the orders they have received to provide more data to the government.

Id.

The President's conclusion reflects the recommendations of an expert panel selected to recommend changes to intelligence programs in light of changing

---

[12] *Available at* http://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment

[13] *Available at* http://www.gpo.gov/fdsys/pkg/DCPD-201400030/pdf/DCPD-201400030.pdf.

communications technologies. The Review Group stated "When it is possible to promote transparency without appreciably sacrificing important competing interests, we should err on the side of transparency." President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World* 128 (2013).[14] The Review Group specifically identified the reporting of aggregate statistics as a priority:

> the government should, to the greatest extent possible, report publically on the total number of requests made and the number of individuals whose records have been requested. These totals inform Congress and the public about the overall size and trends in a program, and are especially informative when there are major changes in the program.

Id. The Review Group's recommendations also follow from earlier recommendations made by EPIC and others to promote greater accountability in the use of electronic surveillance authority. *See, e.g., The FISA Amendments Act of 2008: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Jud.* (May 31, 2012) (Testimony of Marc Rotenberg, Executive Director, EPIC).[15]

This need for greater public reporting was also endorsed by a special committee of the American Bar Association that undertook an evaluation of the expanded use of the FISA, shortly after 9-11, to ensure that Government conduct

[14] *Available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.
[15] *Available at* http://epic.org/privacy/testimony/EPIC-FISA-Amd-Act-Testimony-HJC.pdf

complied with constitutional principles while effectively and efficiently safeguarding national interests. American Bar Association, *FISA Resolution* (February 10, 2013).[16] The ABA report stressed the importance of both the Government's legitimate intelligence gathering activity and the protection of individuals from unlawful government intrusion. The ABA recommended that the Congress conduct regular and timely oversight, that FISA orders be sought only when the government has a "significant" foreign intelligence purpose, and that the Government make available an "annual statistical report on FISA investigations, comparable to the reports prepared by the Administrative Office of the United States Courts pursuant to 18 U.S.C. § 2519." *Id.*

Yet the provisions under review before this Court provide for indefinite gag orders regarding national security letters, issued to the recipients without regard for the transparency interest at stake.

B. Statistical Reports Provide an Effective Mechanism for Public Oversight of Government Surveillance Without Compromising Individual Investigations

While the government has an important interest in maintaining the integrity of its investigations, it has done so in the law enforcement context for decades while still providing for aggregate reporting on the use of electronic surveillance techniques. The annual reports prepared by the Administrative Office of the U.S.

[16] *Available at* http://epic.org/privacy/terrorism/fisa/aba_res_021003.html.

Courts on the use of Title III Wiretap Authorities provide remarkably useful data for evaluating surveillance methods without compromising any particular investigations.[17] EPIC and many others, including press organizations, review these reports closely and use them to inform the public about important developments related to government surveillance.

The Administrative Office of the US Courts is required by statute to report to Congress annually "a full and complete report concerning the number of applications for orders authorizing or approving the interception of wire, oral, or electronic communications" made at the federal and state level. 18 U.S.C. § 2519 (3). This is commonly known as the Wiretap report and has been submitted annually since 1969. The report of the Administrative Office is a remarkable document, perhaps the most comprehensive report on wiretap authority produced by any government agency in the world.

These comprehensive reports highlight various types of information in statistical tables.[18] The annual Wiretap Reports contain information such as the

---

[17] *See*, *e.g.*, Admin. Office of the U.S. Courts, *Wiretap Reports*, http://www.uscourts.gov/Statistics/WiretapReports/wiretap-report-2012.aspx (last visited Mar. 24, 2014).

[18] There are nine tables:
Table 1—Jurisdictions with Statues Authorizing the Interception of Wire, Oral, or Electronic Communications
Table 2—Intercept Orders Issued by Judges
Table 3—Major Offenses for Which Court-Authorized Intercepts Were Granted
Table 4—Summary of Interceptions of Wire, Oral, or Electronic Communications

overall number of intercept orders issued by judges, the average cost per order, as well as the arrests and convictions resulting from intercepts installed, among other data. The data provided in these reports provide EPIC and others the data necessary to evaluate changes in government surveillance at the state and federal level, the efficacy of these wiretaps, and the costs of the intercepts. This information allows the public, the press, and policymakers to evaluate important trends in the use of this investigative technique.

EPIC has used the information provided by these reports to construct charts and graphs demonstrating the use of electronic surveillance authority. EPIC has tracked wiretap orders from 1968-2012,[19] noting the total number of authorized orders each year, and the number of federal and state orders. EPIC also tracks Foreign Intelligence Surveillance Act Court ("FISC") orders, including pen register orders, traditional FISA orders, and NSL and 215 orders. [20] EPIC analyzes the FISA Pen Register applications four ways: by noting the overall number of pen

---

Table 5—Average Cost Per Order
Table 6—Types of Surveillance Used, Arrests, and Convictions for Intercepts Installed
Table 7—Authorized Intercepts Granted
Table 8—Summary of Supplementary Reports for Intercepts Terminated
Table 9—Arrests and Convictions Resulting from Intercepts Installed
Available at http://www.uscourts.gov/Statistics/WiretapReports/wiretap-report-2012.aspx

[19] *Id.*

[20] *See* EPIC, *Foreign Intelligence Surveillance Act Court Orders—1979-2012*, *available at* http://epic.org/privacy/wiretap/stats/fisa_stats.html.

register applications, if the applications have been modified or rejected by the FISC, and how many U.S. persons have been targeted for pen registers. EPIC analyzes the traditional FISA Surveillance Orders by noting the number of applications presented each year and then the number approved or rejected. EPIC analyzes the 215 orders by noting the number of 215 applications, the number modified by the FISC, and the number of combined 215 and pen register applications (if any) that particular year.

This information is critical to evaluating both the effectiveness and the need for various types of Government surveillance activities. For example, in 2012 EPIC reviewed the wiretap report and found that wiretaps were "up 24%" and that encryption had affected law enforcement's ability to conduct surveillance for the first time since the Administrative Office began collecting encryption data. EPIC, *Federal and State Wiretaps Up 24%, Primary Target Mobile Devices According to 2012 Report* (June 28, 2013).[21] Similarly, EPIC reported that "wiretap orders dropped 14 percent in 2011," which "resulted primarily from a drop in applications for intercepts in narcotics offenses." EPIC, *2011 Report: Wiretap Authorization Decrease* (Jul. 3, 2012).[22] In 2010, EPIC reported that wiretaps had "reached an all time high" with an increase in the "average number of persons whose communications were intercepted" per wiretap order, even though "only 26% of

[21] *Available at* http://epic.org/2013/06/federal-and-state-wiretaps-up.html
[22] *Available at* http://epic.org/2012/07/2011-report-wiretap-authorizat.html.

intercepted communications in 2010 were incriminating." EPIC, *Court Approved Wiretaps Reach a New All-Time High* (Jul. 6, 2011).[23] Aggregate statistical reports have provided much needed public accountability of federal wiretap practice and that is the approach that should be followed now for NSLs.

By contrast, EPIC currently analyzes the NSL information in only two categories: the number of NSL applications concerning U.S. persons and the number of U.S. persons involved in NSL applications, as this is the only information available. Presently the DOJ releases the aggregate number of NSLs and the aggregate number of U.S. persons affected by NSLs but no other information.[24] Aggregate reporting of more detailed NSL information could provide valuable data on trends and differences amongst the various NSLs that are served across the country. It would be of great value to the public to have data on NSLs broken down by region, by FBI field-office, by whether the NSL had a certified non-disclosure provision or not, what type of data the NSL is seeking to uncover, the efficacy of the NSL in question, and the general industries which are receiving NSLs. All of this information could be delivered in aggregate form (as

[23] *Available at* http://epic.org/2011/07/court-approved-wiretaps-reach.html.
[24] USA PATRIOT Improvement and Reauthorization Act, Pub. L. 109-177 § 118 (2006). The numbers are reported to Congress in the FISA Annual report. *See e.g.,* Peter Kadzik, *FISA Annual Report to Congress, 2012* (April 30, 2013), *available at* http://www.fas.org/irp/agency/doj/fisa/2012rept.pdf.

has been done in the case of the Wiretap Act) without impairing the success of these investigations.

Currently, we lack data on the type of information being sought and the results of the investigations that take place through NSLs. The Wiretap report, by contrast, provides a granular examination of the various regions, costs of investigation, the efficacy of the various wiretaps, and numerous other factors, which provide the public insight into what is being done in their name.

Both the Privacy and Civil Liberties Oversight Board ("PCLOB") and the President's Review Group on Intelligence and Communications Technologies have called for a greater release of aggregate statistics about electronic surveillance activities. In the recent report on the government's collection of telephone records, the PCLOB stated that "One way to understand and assess any government program is numerically. . . .Periodic public reporting on surveillance programs is a valuable tool in promoting accountability and public understanding." Privacy & Civil Liberties Oversight Board, *Report on the Telephone Records Program Conducted Under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court* 201 (2014).[25] The report emphasized that "the publication of additional numerical information on the frequency with which various surveillance authorities are being used would be possible without

[25] *Available at* http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf.

allowing terrorists to improve their tradecraft." *Id.* The report also found that current rules limit the ability "of private sector entities to disclose to their customers the scope of government surveillance or data disclosure demands" and noted the value of permitting "reasonable disclosures of aggregate statistics that would be meaningful without revealing sensitive government capabilities or tactics." *Id.* at 202.

The President's Review Group report recommended several substantial reforms of the procedures for issuing NSLs.[26] Specifically, the Review Group recommended that non-disclosure orders only be issued after a judicial finding of necessity, should only be in effect for 180 days, and never prevent the recipient of an order from being able to challenge the order. *Liberty and Security in a Changing World* at 122-23. The Review Group also emphasized that recipients of NLS should be able to disclose general information and aggregate statistics on the NSL orders, as well as allow the government to disclose aggregate statistics. *Id*. at 123-24. The Review Group further cautioned that all government actions related to its surveillance programs should be undertaken "only with due consideration of and respect for the strong presumption of transparency that is central to democratic governance." *Id.* at 124.

[26] Of the Review Group's 46 recommendations, 6 involved changes to NSL procedures.

C. Without Proper Oversight, National Security Letters Could Be Used to Circumvent Restrictions on Access to Business Records

Transparency in the government's use of National Security Letters is especially important given the overlap between NSLs and the controversial 215 telephone record collection program. The President's Review Group recently noted that "there have been serious compliance issues in the use of NSLs," *id.* at 91, and that "it is essential that the standards and processes for issuance of NSLs match as closely as possible the standards and processes for issuance of section 215 orders. Otherwise, the FBI will naturally opt to use NSLs whenever possible in order to circumvent the more demanding—and perfectly appropriate—section 215 standards." *Id.* at 93 n. 83.

The Department of Justice's Inspector General found that the FBI had issued NSLs, "after the FISA court, citing First Amendment concerns, had twice declined to sign Section 215 orders in the same investigation." U.S. Dep't of Justice, Office of the Inspector Gen., *A Review of the FBI's Use of Section 215 Orders for Business Records in 2006* 5 (2008) [hereinafter *Section 215 IG Report*]. The FBI's justification "was that as a matter of separation of powers, the FISA Court could not order the FBI to close an investigation, and while the court's judgment on the First Amendment question necessarily prevailed under Section 215, the FBI's own contrary interpretation necessarily prevailed with respect to interpretation of the NSI Guidelines and (to the extent applicable) the First Amendment proviso in the

NSL statutes." 1 Kris & Wilson § 20:8, 749. But, as the Inspector General report emphasized, the NSL provisions "have the same First Amendment caveat as Section 215 requests and the FBI issued the NSLs based on the same factual predicate, without further reviewing the underlying investigation to ensure that it was not premised solely on protected First Amendment conduct." *Section 215 IG Report* at 5.

Thus in the past the Department of Justice has issued NSLs to obtain the same information that the Foreign Intelligence Surveillance Court had prohibited it from obtaining under Section 215. The public would have no knowledge this occurred at all, were it not for the Inspector General Report. Aggregate data on when and if NSLs are issued in cases where Section 215 orders have been denied will allow the public to be aware of these situations, without damaging the integrity of the ongoing investigations. It is precisely this type of "gradual and silent encroachment" that our the founders warned would lead to greater "abridgement of the freedom of the people" than by "violent and sudden usurpations." James Madison, Speech in the Virginia Ratifying Convention on the Control of the Military (June 16, 1788), *in The History of the Virginia Federal Convention of 1788, with Some Account by Eminent Virginians of That Era Who Were Members of That Body* (Vol. I) p. 130 (Hugh Blair Grigsby et al. eds., 1890).

Public vigilance regarding secret interpretation of the law is essential, and transparency is necessary to facilitate such oversight.

D. The Justice Department Inspector General Reports Show That Oversight is Necessary to Curb Misuse of NSL Authorities

The Inspector General's ("OIG") initial reports on the FBI's use of NSL authority found significant violations of law. The subsequent reports also reflected improved compliance by the FBI. These reports show that public reporting can improve compliance, without endangering the FBI's ability to conduct investigations relevant to national security. Yet even the IG's reports have failed to address the ongoing problem with the "gag" order or the absence of routine reporting on the use of NSL authority.

Under the Patriot Reauthorization Act of 2005, the Department of Justice Office of the Inspector General (OIG) is required to review "the effectiveness and use, including any improper or illegal use, of national security letters issued by the Department of Justice." Pub. L. No. 109-177 § 119. The OIG released its first report, covering calendar years 2003 through 2005, on March 9, 2007. U.S. Dep't of Justice, Office of the Inspector Gen., *A Review of the Federal Bureau of Investigation's Use of National Security Letters* (2007).[27] The OIG then issued two

[27] *Available at* http://www.justice.gov/oig/special/s0703b/final.pdf.

follow up reports over the next few years, covering FBI corrective actions and investigating abuses and illegalities discovered in the first report.[28]

The FBI is required to report to Congress on the number of NSLs issued; the OIG found in their first report that the FBI underreported this number. The OIG review looked at 77 case files containing 293 NSLs from four separate FBI field offices issued in the 2003-2005 period. This review found that there were 17% more NSLs in the sample of case files than in FBI reporting databases. *Id.* at 32. Delays in data entry also caused about 4,600 NSLs to not be reported to Congress. *Id.* at 33. The OIG concluded that the FBI database significantly understates the number of NSL requests issued, and that Congress has been misinformed about the scale of the usage of the NSL authority.

The report further stated that violations are supposed to be reported by the FBI to the Intelligence Oversight Board. During the 3-year period in question, the FBI self-reported 26 violations out of the 140,000 NSLs issued. The OIG, however, found 22 potential violations out of the sample of 293 NSLs it reviewed. *Id.* at 69. The OIG has stated that there is no indication that the 293 NSLs it reviewed are not representative of all of the NSLs issued, thus indicating that the FBI is failing to self-report a very significant number of violations. *Id.* at 84.

---

[28] *See 2008 IG Report*; U.S. Dep't of Justice, Office of the Inspector Gen., *A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records* (2010), *available at* http://www.justice.gov/oig/special/s1001r.pdf.

The OIG also found over 700 "exigent letters," which are not authorized by statute and some of which appear to have been issued when no exigency or emergency existed. *Id.* at 86. These letters requested records from telephone companies and promised that proper subpoenas had been submitted or would follow. However the OIG found no confirmation that subpoenas, NSLs, or other proper process did follow or had in fact been submitted.

The second Inspector General Report found similar errors in the use of NSLs by the FBI in 2006 and also found that the FBI's Field Review "did not capture all NSL-related possible intelligence violations in the files it reviewed and therefore did not provide a fully accurate baseline from which to measure future improvement." 2008 IG Report at 8.[29] The report also found "that 97% of the NSLs in the random sample imposed non-disclosure and confidentiality obligations on recipients." *Id*. at 10.

The third Inspector General Report evaluated the 739 exigent letters requested by the FBI, identified in the first report. This report detailed substantial illegality and lack of compliance with the proper NSL provisions. U.S. Dep't of Justice, Office of the Inspector Gen., *A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records* 257-59 (2010). Most disturbingly, the IG report found the FBI put forward

[29] *Available at* http://www.justice.gov/oig/special/s0803b/final.pdf.

a novel legal theory (which is redacted in the report) to support the collection of phone records, "only after the OIG found repeated misuses of its statutory authority to obtain telephone records through NSLs or the ECPA's emergency voluntary disclosure provisions." *Id.* at 268. These findings would not have been possible without examination by the Inspector General but are not sufficient to ensure that the FBI's use of NSLs are lawful and in compliance with all relevant procedures. The FBI should disclose comprehensive aggregate statistics to maintain credibility with the American public.

The Inspector General Reports helped shed light on the FBI's practices with NSLs and provide evidence that the FBI has improved compliance. However, this is an argument for more oversight, not less. The success of the Inspector General Reports argues for continued, institutionalized oversight. *See, e.g.,* Andy Greenberg, *As Reports Of Wiretaps Drop, The Government's Real Surveillance Goes Unaccounted*, *Forbes* (July 2, 2012) (arguing for enhanced reporting of electronic surveillance.)[30]

Aggregate statistics would complement the mandated reviews by the Inspector General and provide essential data necessary for the public to analyze and evaluate surveillance authorities used in national security investigations.

[30] *Available at* http://www.forbes.com/sites/andygreenberg/2012/07/02/as-reports-of-wiretaps-drop-the-governments-real-surveillance-goes-unaccounted/.

Without this information, the public cannot effectively evaluate the programs that its representatives vote to renew or to reject.

CONCLUSION

Amicus respectfully requests this Court affirm the lower court's decision.

Respectfully submitted,

/s/ Marc Rotenberg

Marc Rotenberg
Counsel of Record
Alan Butler
David Husband
Electronic Privacy Information Center
1718 Connecticut Ave. NW, Suite 200
Washington, DC 20009
(202) 483-1140

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of 7,000 words of Fed. R. App. P. 29(d) and Fed. R. App. P. 32(B)(i). This brief contains 5,743 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii). This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Office Word in 14 point Times New Roman style.

Dated: March 27, 2014

/s/ Marc Rotenberg
Marc Rotenberg
Counsel of Record
Alan Butler
David Husband
Electronic Privacy Information Center
1718 Connecticut Ave. NW, Suite 200
Washington, DC 20009
(202) 483-1140

CERTIFICATE OF SERVICE

I hereby certify that on this 27th Day of March, 2014, the foregoing Brief of *Amicus Curiae* Electronic Privacy Information Center in Support of Petitioners was served via U.S. Mail on:

Susan Soong, Chief Deputy Clerk – Operations

U.S. Court of Appeals for the Ninth Circuit

P.O. Box 193939

San Francisco, CA 94119-3939

Dated: March 27, 2014

/s/ Marc Rotenberg

Marc Rotenberg
Counsel of Record
Alan Butler
David Husband
Electronic Privacy Information Center
1718 Connecticut Ave. NW, Suite 200
Washington, DC 20009
(202) 483-1140