07-4943-cv

IN THE UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

JOHN DOE INC., JOHN DOE, AMERICAN CIVIL LIBERTIES UNION, and AMERICAN CIVIL LIBERTIES UNION FOUNDATION,
Plaintiffs-Appellees,
v.
MICHAEL B. MUKASEY, in his official capacity as Attorney General of the United States, ROBERT S. MUELLER III, in his official capacity as Director of the Federal Bureau of Investigation, and VALERIE E. CAPRONI, in her official capacity as General Counsel to the Federal Bureau of Investigation,
Defendants-Appellants.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

BRIEF OF *AMICUS CURIAE,* NATIONAL SECURITY ARCHIVE AND ELECTRONIC FRONTIER FOUNDATION
IN SUPPORT OF PLAINTIFFS-APPELLEES

Meredith Fuchs
National Security Archive
George Washington University
2130 H St. NW, Suite 701
Washington, D.C. 20037
202-994-7000

Marcia Hofmann
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
415-436-9333

CORPORATE DISCLOSURE STATEMENT

In accordance with Fed. R. App. P. 26.1, *amicus curiae* the National Security Archive discloses that it is a project of the National Security Archive Fund, Inc. The National Security Archive Fund, Inc. is a not-for-profit corporation established under the laws of the District of Columbia. The National Security Archive Fund, Inc. has no parent corporation and no stock, thus no publicly held corporation owns ten percent or more of its stock. The Archive identifies that its general nature and purpose is to promote research and public education on U.S. governmental and national security decisionmaking and to promote and encourage openness in government and government accountability. The Archive has no members, thus no member has issued shares or debt securities to the public.

In accordance with Fed. R. App. P. 26.1, *amicus curiae* Electronic Frontier Foundation ("EFF") discloses that it is a not-for-profit corporation established under the laws of the state of California. EFF identifies that its general nature and purpose is to promote and defend rights in the digital world. EFF has no parent corporation and no stock, and thus no publicly held corporation or other publicly held entity owns ten percent or more of its stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

LEGISLATIVE MATERIALS

OTHER AUTHORITIES

COMMITTEE, COMMISSION AND AGENCY REPORTS

INTEREST OF THE *AMICI CURIAE*

Amici curiae submit this brief in support of Plaintiffs/Appellees. Appellees brought this case to challenge the issuance and enforcement of national security letters ("NSLs") by the Federal Bureau of Investigation ("FBI") pursuant to 18 U.S.C. § 2709. The present appeal comes after Congress amended the statutory provisions at issue in the Patriot Act Reauthorization Act of 2005, which modified § 2709 and enacted new judicial review provisions for NSLs under 18 U.S.C. § 3511. The revised § 2709 grants the FBI broad discretion to issue NSLs and to bar the recipient from disclosing anything regarding the NSL when an FBI official certifies that disclosure "may result" in danger to national security or other harms, including interference with ongoing investigations. The judicial review provisions of § 3511 permit NSL recipients to petition a federal court to set aside an NSL request or the nondisclosure requirement, but requires courts to treat the FBI's certification of harm "as conclusive unless the court finds that the certification was made in bad faith." 18 U.S.C. § 3511(b)(2). The District Court ruled that the revised provisions in §§ 2709(c) and 3511(b) are facially unconstitutional because they violate the First Amendment and separation of powers principles. *Doe v. Gonzales*, 500 F. Supp. 2d 379, 386 (S.D.N.Y. 2007).

Amici are secrecy experts who have long monitored government secrecy policy. *Amici* each frequently seek information on important matters of significant

public interest under open government laws and have seen how openness has proven to be a check against government abuses and has advanced the security of the nation.

The National Security Archive is a non-governmental research institute and library located at the George Washington University. The Archive collects and publishes declassified documents concerning United States foreign policy and national security matters.

The Electronic Frontier Foundation ("EFF") is a not-for-profit membership organization with offices in San Francisco, California and Washington, DC. EFF works to inform policymakers and the general public about civil liberties issues related to technology, and to act as a defender of those liberties. In support of its mission, EFF uses the Freedom of Information Act to obtain and disseminate information concerning the activities of federal agencies.

This brief is filed with the consent of counsel for all parties in the case.

SUMMARY OF ARGUMENT

The United States was founded on democratic principles that recognize the importance of informed public debate about government activities. The need for such debate is at its apex in the area of defense and national security. Yet the Government's reflexive response to security threats is to increase secrecy. That

reaction does not necessarily serve the national interest. As the numerous investigations into the September 11 attacks on the United States concluded, excessive secrecy was part of the problem, interfering with detection and prevention of the attacks instead of aiding the nation's security.

In the six years since the September 11 attacks, a number of new laws restricting the dissemination of information to the public—including the national security letter provisions at issue in this case—have been enacted. There also has been a dramatic rise in classification of information and broad use of novel "mosaic" theories to prevent release of information. Experience shows, however, that the Government does not always have an incentive to limit secrecy to instances in which national security demands such protection. Thus, meaningful judicial review is necessary to distinguish between legitimate and illegitimate claims for secrecy.

The NSL power grants the FBI broad authority to compel customer information from communications and Internet providers under a shroud of secrecy. As the District Court found and the plaintiffs argue, this authority violates the First Amendment. In addition to the unconstitutional nature of the power, *amici* contend that the statute severely undermines accountability. Without a meaningful judicial check, the new judicial review provision creates a façade of legitimacy for NSLs without any protection for the public interest in an accountable government.

Congress has struggled to obtain timely, accurate information about the FBI's issuance of NSLs, but it has proven nearly impossible to oversee the agency's use of § 2709 authority. The secrecy surrounding this investigative technique raises significant concerns because the little evidence made publicly available over the past few years reveals widespread, systematic misuse of NSL authority by the FBI.

ARGUMENT

I. MEANINGFUL JUDICIAL REVIEW OF THE GOVERNMENT'S DEMANDS FOR SECRECY IS NECESSARY IN ORDER TO PROTECT THE SECURITY OF THE NATION AND THE QUALITY OF DEMOCRATIC DECISIONMAKING.

a. Excessive Secrecy Imposes Significant Social Costs on Society

An informed citizenry is one of our nation's highest ideals. In times of war or national crisis, the public's role in governance is especially critical. As the Supreme Court has noted:

> In the absence of the governmental checks and balances present in other areas of our national life, the only effective restraint upon executive policy and power in the areas of national defense and international affairs may lie in an enlightened citizenry—in an informed and critical public opinion which alone can here protect the values of democratic government.

New York Times Co. v. United States, 403 U.S. 713, 728 (1971) (Stewart, J., concurring). Yet the Government often demands complete deference to claims that secrecy is necessary to protect security.

The unthinking association of information disclosure with harm often drawn by the Executive in national security matters is a false dichotomy. While there is no doubt about the social cost of sharing highly sensitive information that might be used by a terrorist to cause harm, there also are real costs associated with keeping unnecessary secrets. As the former director of the Information Security Oversight Office ("ISOO"), the agency responsible for policy oversight of the government-wide security classification system and the National Industrial Security Program,[1] has explained:

> Classification, of course, can be a double edged sword. Limitations on dissemination of information that are designed to deny information to the enemy on the battlefield can increase the risk of a lack of awareness on the part of our own forces, contributing to the potential for friendly fire incidents or other failures. Similarly, imposing strict compartmentalization of information obtained from human agents increases the risk that a Government official with access to other information that could cast doubt on the reliability of the agent would not know of the use of that agent's information elsewhere in the Government. Simply put, secrecy comes at a price.[2]

[1] *See* The Information Security Oversight Office (ISOO), http://www.archives.gov/isoo/index.html (last visited March 18, 2008) (describing ISOO's mission).

[2] *Emerging Threats: Overclassification and Pseudo-classification, Hearing Before the Subcomm. on Nat'l Sec., Emerging Threats, and Int'l Relations of the H. Comm. on Gov't Reform*, 109th Cong. 45 (2005) (statement of J. William Leonard, Info. Sec. Oversight Office).

That price includes undermining the legitimacy of government actions,[3] reducing accountability,[4] hindering critical technological and scientific progress,[5] interfering with the efficiency of the marketplace,[6] and breeding paranoia.[7]

Indeed, this is one of the lessons of the September 11 attacks. It was directly addressed by Eleanor Hill, Staff Director, Joint House-Senate Intelligence Committee Investigation into the September 11 Attacks, who explained in a Staff Statement summarizing the testimony and evidence,

> the record suggests that, prior to September 11th, the U.S. intelligence and law enforcement communities were fighting a war against terrorism largely without the benefit of what some would call their most potent weapon in that effort: an alert and committed American public. One needs look no further for proof of the latter point than the

---

[3] *See, e.g.*, *Report of the Comm'n on Reducing and Protecting Gov't Secrecy*, S. Doc. No. 105-2, at 8 (1997) ("[T]he failure to ensure timely access to government information, subject to carefully delineated exceptions, risks leaving the public uninformed of decisions of great consequence. As a result, there may be a heightened degree of cynicism and distrust of government, including in contexts far removed from the area in which the secrecy was maintained.").

[4] *See, e.g., ACLU v. Dep't of Defense*, 339 F. Supp. 2d 501, 504-05 (S.D.N.Y. 2004) (ordering government to release records requested under FOIA concerning treatment of detainees held abroad, because "[i]f the documents are more of an embarrassment than a secret, the public should know of our government's treatment of individuals captured and held abroad").

[5] *See, e.g.*, Nat'l Acad. of Sciences, *Seeking Security: Pathogens, Open Access, and Genome Databases* 54-57 (2004), http://www.nap.edu/books/0309093058/html/R1.html ("[A]ny policy stringent enough to reduce the chance that a malefactor would access data would probably also impede legitimate scientists in using the data and would therefore slow discovery.").

[6] *See, e.g.*, Aaron Edlin & Joseph E. Stiglitz, *Discouraging Rivals: Managerial Rent-Seeking and Economic Inefficiencies*, 85 Am. Econ. Rev. 1301 (1995).

[7] *See* Kennedy Assassination Records Review Bd., *Final Report* 1 (1998), http://www.archives.gov/research/jfk/review-board/report/ ("30 years of government secrecy relating to the assassination of President John F. Kennedy led the American public to believe that the government had something to hide.").

> heroics of the passengers on Flight 93 or the quick action of the flight attendant who identified shoe bomber Richard Reid.[8]

This conclusion is echoed in the 9/11 Commission Report, which includes only one finding that the attacks on the World Trade Center and the Pentagon might have been prevented. According to the interrogation of the hijackers' paymaster, Ramzi Binalshibh, if Khalid Sheikh Mohammed and the other organizers had known that the so-called 20th hijacker, Zacarias Moussaoui, had been arrested at his Minnesota flight school on immigration charges, then Bin Ladin and Mohammed would have called off the September 11 attacks.[9] News of that arrest might also have alerted the FBI agent in Phoenix who warned of Islamic militants in flight schools in a July 2001 memo. Instead that memo vanished into the FBI's vaults in Washington and was not connected to Moussaoui in time to prevent the attacks.[10] The Commission's wording on this issue is important: only "publicity . . . might have derailed the plot."[11] Indeed, the Commission's former Executive Director, Phillip Zelikow, recently reiterated: "Imagine what might have happened if the Moussaoui arrest had gotten the kind of publicity and extended coverage that accompanied the Ressam arrest. [Ahmed Ressam was convicted of plotting to bomb Los Angeles International Airport on New Year's Eve 1999.] We had

---

[8] *Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001: Hearing Before the S. Select Comm. on Intelligence and the H. Permanent Select Comm. on Intelligence,* 107th Cong. (2002) (Joint Inquiry Staff Statement, Eleanor Hill, Staff Dir.), *available at* http://intelligence.senate.gov/021017/hill.pdf, at 5.
[9] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, 247, 276 & 541 n. 107 (2004), *available at* http://govinfo.library.unt.edu/911/report/911Report.pdf [hereinafter *9/11 Commission Report*].
[10] *See Joint Inquiry Into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*, S. Rep. No. 107-351, at 325 (2002).
[11] *9/11 Commission Report*, *supra* note 9, at 276.

evidence from [Khalid Sheikh Mohammed] that, had he known of the Moussaoui arrest, he might have cancelled the operation."[12] Simply put, disclosure of security-related information may reduce risk by alerting the public to threats and enabling better-informed responses from both local and federal agencies.

The rationale behind the nation's central openness law, the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, reflects the notion that sharing information with the public will help, not harm, society. The FOIA mandates complete openness, except where several carefully delineated exemptions apply. *Dep't of Air Force v. Rose*, 425 U.S. 352, 360-61 (1976) (holding that FOIA creates "a general philosophy of full agency disclosure unless information is exempted under the clearly delineated statutory language") (internal citation omitted). In enacting the law, Congress sought to "enable the public to have sufficient information in order to be able, through the electoral process, to make intelligent, informed choices with respect to the nature, scope, and procedure of federal governmental activities," *Renegotiation Board v. Bannercraft Clothing Co., Inc.*, 415 U.S. 1, 17 (1974) (internal citations omitted), and to prevent the damage that pervasive secrecy in government agencies did to public confidence in the Government. *See* S. Rep. No. 89-813 (1965), *as reprinted in* Senate Comm. on the Judiciary, *Freedom of Information Act Source Book: Legislative Materials, Cases,*

[12] E-mail correspondence between Phillip Zelikow and Phil Shenon about the 9/11 Commission (2007), http://www.fas.org/irp/news/2008/02/zelikow.pdf.

Articles, S. Doc. No. 93-82, at 45 (1974) [hereinafter *FOIA Source Book*] ("A government by secrecy benefits no one. It injures the people it seeks to serve; it injures its own integrity and operation. It breeds mistrust, dampens the fervor of its citizens, and mocks their loyalty.").

The benefit recognized by courts ruling in favor of open government and by Congress trying to pry open the drawers of government filing cabinets is that informed democratic participation ensures elected officials make the best decisions, including those in our national security interest. As Luther Gulick, a high-level Roosevelt administration official during World War II, observed, despite the apparent efficiencies of totalitarian political organizations, democracy and expressive freedom gave the United States and its democratic allies an important competitive advantage because public debate encouraged wise policy choices.[13]

The necessary corollary to this point—that secrecy can interfere with informed decisionmaking in areas of foreign and national security policy—is true as well. For example, as Senator Daniel Patrick Moynihan concluded in his book *Secrecy: The American Experience*, the Cold War and related arms race were greatly exacerbated by the secrecy imposed by the military establishment.[14]

---

[13] Cass R. Sunstein, *Why Societies Need Dissent* 8 (2003) (citing Luther Gulick, *Administrative Reflections from World War II* 121-29 (1948)).
[14] Daniel Patrick Moynihan, *Secrecy: The American Experience* 154-77 (1998).

Overclassification and unnecessary secrecy also undermine efforts to keep truly sensitive information secret, "[f]or when everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or careless, and to be manipulated by those intent on self-protection or self-promotion." *New York Times Co.*, 403 U.S. at 729 (Stewart, J., concurring). Indeed, this is the same conclusion reached by ISOO in its 2002 Report to the President:

> Much the same way the indiscriminate use of antibiotics reduces their effectiveness in combating infections, classifying either too much information or for too long can reduce the effectiveness of the classification system, which, more than anything else, is dependent upon the confidence of the people touched by it. While there is always a temptation to err on the side of caution, especially in times of war, the challenge for agencies is to similarly avoid damaging the nation's security by hoarding information.[15]

b. Secrecy Has Grown Exponentially Over the Last Six Years and Government Officials Admit That Much of it is Unnecessary.

Over the past six years there has been a dramatic surge in government secrecy. Classification has multiplied, reaching an all-time high of 20.6 million

[15] ISOO, *2002 Report to the President* 7 (2003), http://www.archives.gov/isoo/reports/2002-annual-report.pdf; *see also* Office of Scientific and Technical Info., Dep't of Energy, *Openness in the Department of Energy* (1997), https://www.osti.gov/opennet/forms.jsp?formurl=document/prcfacts.html ("Maximizing openness not only benefits the public, but also enhances national security. Limiting classification to sensitive information that protects our national security allows for such information to be better protected.").

classification actions in 2006, more than double the number in 2001.[16] Moreover, the cost of the security classification program has skyrocketed from an estimated $4.7 billion in 2002[17] to $8.2 billion in 2006.[18]

Officials throughout the military and intelligence sectors have admitted that much of this classification activity is unnecessary. Former Secretary of Defense Donald Rumsfeld acknowledged the problem in an op-ed: "I have long believed that too much material is classified across the federal government as a general rule[.]"[19] The extent of over-classification is significant. Under repeated questioning from members of Congress at a hearing concerning over-classification, Deputy Secretary of Defense for Counterintelligence and Security Carol A. Haave eventually conceded that approximately 50 percent of classification decisions are over-classifications.[20] These opinions echoed that of former CIA Director and then-chair of the House Intelligence Committee Porter Goss, who told the 9/11

---

[16] ISOO, *2006 Report to the President* 3 (2007), http://www.archives.gov/isoo/reports/2006-annual-report.pdf.
[17] ISOO, *2001 Report to the President* 9 (2002), http://www.archives.gov/isoo/reports/2001-annual-report.pdf.
[18] *2006 Report to the President*, *supra* at note 16.
[19] Donald Rumsfeld, *War of the Worlds*, Wall St. J., July 18, 2005, at A12.
[20] *Too Many Secrets: Overclassification as a Barrier to Critical Information Sharing: Hearing Before the Subcomm. on National Security, Emerging Threats and International Relations of the H. Comm. on Gov't Reform*, 108th Cong. 82 (2004) (testimony of Carol A. Haave); *see also id.* at 23 (testimony of J. William Leonard) ("It is no secret that the government classifies too much information.").

Commission, "we overclassify very badly. There's a lot of gratuitous classification going on, and there are a variety of reasons for them."[21]

Former Solicitor General of the United States Erwin Griswold, who led the government's fight for secrecy in the Pentagon Papers case, acknowledged some of the reasons for rampant overclassification:

> It quickly becomes apparent to any person who has considerable experience with classified material that there is massive overclassification and that the principal concern of the classifiers is not with national security, but with governmental embarrassment of one sort or another. There may be some basis for short-term classification while plans are being made, or negotiations are going on, but apart from details of weapons systems, there is very rarely any real risk to current national security from the publication of facts relating to transactions in the past, even the fairly recent past.[22]

The broadened NSL authority and its bar against recipients speaking about receipt of an NSL was one of a number of new laws enacted in the wake of September 11 that creates new categories of secret information. These also include the critical infrastructure information provisions of the Homeland Security Act of 2002, 6 U.S.C.S §133 (2005); the so-called gag order provisions of Section 215 of the Patriot Act, 50 U.S.C.S. § 1861(2005); and the revisions to the sensitive security information provisions of the Air Transportation Security Act. 49 U.S.C.S. §§ 114(s), 40119 (2005).

---

[21] *Public Hearing of the 9/11 Commission* (2003), http://www.9-11commission.gov/archive/hearing2/9-11Commission_Hearing_2003-05-22.htm (testimony of Rep. Porter Goss).

[22] Erwin N. Griswold, *Secrets Not Worth Keeping: The courts and classified information*, Wash. Post, Feb. 15, 1989, at A25.

It is not merely in the areas of classification, information policy, and freedom of speech that secrecy has expanded. The government has also extended its use of the "mosaic" theory of intelligence gathering to a level never before seen, perhaps finally falling down the "slippery slope . . . lurking in the background of the [mosaic] theory" that the Third Circuit recognized in *American Friends Service Committee v. Department of Defense*, 831 F.2d 441, 445 (3d Cir. 1987) (internal citation omitted). Several other courts properly have highlighted the risks attendant in the mosaic theory. For example, in *Detroit Free Press v. Ashcroft*, 303 F.3d 681, 709 (6th Cir. 2002), the court struck down the blanket closure of immigration hearings and cautioned:

> The Government could use its 'mosaic intelligence' argument as a justification to close any public hearing completely and categorically, including criminal proceedings. The Government could operate in virtual secrecy in all matters dealing, even remotely with 'national security,' resulting in a wholesale suspension of First Amendment rights.

Likewise, in a FOIA case, the government argued that it could not disclose the total number of applications (for "production of any tangible things") sought by FBI field offices under Section 215 of the Patriot Act because disclosure would permit adversaries to create a mosaic of FBI investigations. *ACLU v. Dep't of Justice*, 321 F. Supp. 2d 24, 38 n.16 (D.D.C. 2004). Nonetheless, DOJ saw fit to declassify a memorandum from Attorney General John Ashcroft to FBI Director Robert S. Mueller indicating that the power had never been used. *Id.* at 27. Thus,

except for the possibility of parsing the controlled, selective, and conflicting release of information by DOJ about its use of a highly controversial new power, enacted into law at a time of extreme national crisis, the public was completely denied the information necessary to assess the impact of Section 215 of the Patriot Act. The government's willingness to employ such an expansive and unconstrained mosaic theory is particularly troubling in the context of this case, where it is being used not only to suppress information, but also to prevent individuals from exercising their constitutional rights to speak about the receipt of an NSL.

The government's position on these issues and the FBI's extraordinary discretion to quell discussion or debate by NSL recipients ensures that there is no effective check on overreaching. The government has an interest in preserving such secrecy; it permits the government to control knowledge and pursue unimpeded its aims. And while Congress attempted to check the FBI's power by revising the NSL provisions to permit judicial review, it has not done so in a meaningful way.

c. Meaningful Judicial Review of Government Secrecy is Necessary to Prevent Overreaching.

When internal and external checks against government misconduct are lacking, as with Section 2709's broad discretion for FBI officials to ban speech by NSL recipients, the judiciary is critically necessary to protect against overreaching. Our nation's experience when extreme secrecy has been invoked in the past is that

secrecy can stem from many motives—some legitimate and some possibly illegitimate. The government has no motivation to separate out the illegitimate incentives. This certainly is the lesson of cases such as *Korematsu v. United States*, 323 U.S. 214 (1944), and *New York Times Co.,* 403 U.S. 713, which demonstrate the danger of a doctrine of deference that precludes dispositive counterarguments and prompts judges to decline substantive review of agencies' positions.

Korematsu concerned an order that directed the exclusion from the West Coast of all persons of Japanese ancestry which the Supreme Court held constitutional. In that case, the Court's finding of "military necessity" was based on the representation of government lawyers that Japanese Americans *were committing espionage and sabotage* by signaling enemy ships from shore. Documents later released under FOIA revealed that government attorneys suppressed key evidence and authoritative reports from several federal agencies that flatly contradicted the government claim that Japanese Americans were a threat to security. *Korematsu v. United States*, 584 F. Supp. 1406, 1416-19 (N.D. Cal. 1984). The complete deference granted to the government in *Korematsu* – without any effort to ensure the veracity of the government's claims – undermined accountability and in turn prevented the public from fulfilling its intended role as a check against abuse.

New York Times Co. involved an effort to enjoin the *New York Times* from publishing a classified study entitled "History of U.S. Decision-Making Process on Viet Nam Policy" (also known as the Pentagon Papers). As with *Korematsu*, the motivation behind the secrecy was not protection of national security. The Pentagon Papers, which were improperly leaked, described a series of misrepresentations and poor policy decisions concerning the Vietnam War. As former Solicitor General Erwin Griswold eventually admitted: "I have never seen any trace of a threat to the national security from publication. Indeed, I have never seen it suggested that there was such an actual threat."[23] The Supreme Court denied the government's efforts to enjoin publication by newspapers. Had the Pentagon Papers not been leaked, there would have been no First Amendment clash to resolve—secrecy for the purpose of covering up government misrepresentations and missteps likely would have triumphed.

These cases illustrate the importance role the courts can plan in sorting out appropriate secrecy from inappropriate secrecy. The constitutional system of checks and balances does not permit the executive branch to act beyond the accountability of the judiciary. As the Supreme Court asserted when it mandated due process for enemy combatants, "a state of war is not a blank check for the President when it comes to the rights of the Nation's citizens." *Hamdi v. Rumsfeld*,

[23] Griswold, *supra* note 22.

542 U.S. 507, 603 (2004) (O'Connor, J., plurality opinion). Congress also has acknowledged the judiciary's constitutional role in policing executive claims of secrecy. In a definitive pronouncement on the issue, Congress overturned *EPA v. Mink*, 410 U.S. 73 (1973) (holding that FOIA does not permit courts to conduct *in camera* review of classified records), by passing the 1974 amendments to the Freedom of Information Act ensuring that the FOIA explicitly provides for judges to conduct *in camera* review of records despite the Government's assertion of national security. This authority was given to judges to safeguard against arbitrary, capricious, and myopic use of the awesome power of the classification stamp by the Government bureaucracy. S. Rep. No. 93-854 (1974), *as reprinted in FOIA Source Book,* at 183.

The courts are certainly competent to understand when an informed citizenry instinctively would want judicial review of secret intelligence activities or matters. Properly exercised, deference to the government in national security matters includes a presumption of good faith and a recognition that the Executive Branch has the special competence to make some judgments. It should not mean, however, acceptance of government demands for new unchecked powers that are veiled in a cloak of secrecy or a denial of fundamental rights without a meaningful inquiry into the basis for such actions.

The new judicial review provisions of § 3511 permit NSL recipients to petition a federal court to set aside an NSL request or nondisclosure order, but prohibits courts from setting aside the gag orders unless "there is no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person" and requires courts to treat the FBI's certification of harm "as conclusive unless the court finds that the certification was made in bad faith." 18 U.S.C. § 3511(b)(2). In practice, this standard nullifies the judicial review provision by preventing courts from acting as a check against abuse.

II. 18 U.S.C. § 2709 UNDERMINES NATIONAL SECURITY BY UNDERMINING ACCOUNTABILITY

Since the September 11 attacks, the gap between governmental power and public accountability has widened as the Government has increasingly withheld information about its counterterrorism efforts from Congress and the public. The lack of meaningful, reliable reporting has frustrated Congress' ability to oversee the Government's use of NSLs, and thwarted public understanding of how the FBI uses this investigative power.

While the Government may be able to show on a case-by-case basis that limited nondisclosure requirements are appropriate to protect the integrity of particular investigations, § 2709(c)'s nondisclosure provision allows the FBI

extraordinary discretion to keep secret virtually any NSL request, a power not sufficiently checked by the limited judicial review contemplated in § 3511. As the lower court noted, "[i]n light of the seriousness of the potential intrusion into the individual's personal affairs and the significant possibility of a chilling effect on speech and association—particularly of expression that is critical of the government or its policies—a compelling need exists to ensure that the use of NSLs is subject to the safeguards of public accountability, check and balances, and separation of powers that our Constitution prescribes." *Doe v. Gonzales*, 500 F. Supp. 2d at 394. The FBI's minimal disclosure about its use of § 2709 NSLs since the passage of the USA PATRIOT Act, coupled with the little information that has been publicly released about the FBI's misuse of such authority, underscores the need to ensure that the Bureau is subject to meaningful accountability as it exercises its discretion to silence recipients of § 2709 NSLs.

a. Congressional Oversight of § 2709 NSLs Has Been Misinformed and Ineffective.

The lack of accountability surrounding § 2709 NSLs has resulted from an absence of public information about the FBI's use of its authority and a lack of meaningful congressional oversight to serve as a check on the controversial power. This problem was caused in part by the FBI's failure to fully comply with the Electronic Communications Privacy Act's requirement that the FBI report to Congress on its use of NSL authority. 18 U.S.C. § 2709(e). Twice a year, the

director of the FBI is required by statute to "fully inform" the House of Representatives Permanent Select Committee on Intelligence, the Senate Select Committee on Intelligence, and the Judiciary Committees of the House of Representatives and Senate "concerning all requests" for information made via NSLs issued pursuant to §2709. *Id*. The congressional committees, however, have experienced significant difficulty obtaining this information. For example, after the House Judiciary Committee approved the USA PATRIOT Act reauthorization bill in 2005, nearly four years after the PATRIOT Act expanded the FBI's authority to issue NSLs, minority members noted in a dissenting statement, "[t]he Justice Department has never accounted for [NSL] use."[24] Furthermore, Senator Russ Feingold pointed out in 2006 that the FBI had provided incomplete NSL figures to Congress and the public.[25] That same year, the FBI conceded that it may have reported inaccurate information to Congress in its semiannual reports. Dep't of Justice, Inspector Gen., *A Review of the Federal Bureau of Investigation's Use of National Security Letters* 33 (2007), *available at* http://www.usdoj.gov/oig/special/s0703b/final.pdf [hereinafter *2007 OIG Report*]. The Department of Justice Office of the Inspector General ("OIG") determined the following year that the FBI failed to report nearly 4,600 NSL requests to Congress

[24] *USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005*, H.R. Rep. No. 109-174, at 465 (2005).
[25] *FBI Oversight: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. 22 (2006) (exchange between Sen. Russ Feingold and Robert S. Mueller III, FBI Director).

between 2003 and 2005, most of which were issued under § 2709. *Id*.

This incomplete and inaccurate reporting has been exacerbated by the failure of high-level Justice Department officials to report information about NSLs that is or should be within their knowledge. For example, former Attorney General Alberto Gonzales told a congressional committee during an April 27, 2005, hearing that "[t]here has not been one verified case of civil liberties abuse" attributable to the USA PATRIOT Act.[26] However, documents released to *amicus* EFF in response to a Freedom of Information Act lawsuit revealed that the attorney general was aware of numerous intelligence missteps disclosed by the FBI to the Intelligence Oversight Board ("IOB") at the time he delivered this testimony, including one report sent on April 21, 2005—just six days before Gonzales' statement.[27] The FBI reports such incidents to the IOB only when it determines that they were "conducted contrary to the attorney general's guidelines for FBI National Security Investigations and Foreign Intelligence Collection and/or laws, executive orders and presidential directives."[28] Likewise, during another congressional hearing the same year, FBI Director Robert S. Mueller III cited a university's failure to comply with an NSL as an example of why the FBI should

[26] *USA PATRIOT Act: Hearing Before the S. Select Comm. on Intelligence*, 109th Cong. 99 (2005) (statement of Attorney General Alberto Gonzales).
[27] Letter to James Langdon, Intelligence Oversight Board, from Julie F. Thomas, Deputy General Counsel, FBI, and Report of Intelligence Oversight Board Matter (Apr. 21, 2005), http://www.eff.org/files/filenode/07656JDB/042105_iob.pdf (last visited March 19, 2008); *see also* John Solomon, *Gonzales Was Told of FBI Violations*, Wash. Post, July 10, 2007, at A1.
[28] Letter to James Langdon, *supra* note 27.

be given even greater investigative power (a request which Congress did not ultimately grant).[29] Documents released in response to EFF's FOIA lawsuit showed that in fact this NSL had been issued under § 2709, but had demanded educational records, which are not subject to § 2709 or any other NSL authority.[30]

In 2005, Congress attempted to improve the FBI's accountability for NSL use by requiring the OIG to review "the effectiveness and use, including any improper or illegal use, of national security letters issued by the Department of Justice" in the USA PATRIOT Improvement and Reauthorization Act of 2005. Pub. L. No. 109-177, § 119, 120 stat. 192, 219 (2006). The President attempted to undermine this much needed effort to create transparency, however, when he signed the bill into law and qualified:

> The executive branch shall construe the provisions of H.R. 3199 that call for furnishing information to entities outside the executive branch, such as sections 106A [requiring the Inspector to audit the FBI's access to business records under the Foreign Intelligence Surveillance Act] and 119 [requiring the Inspector General to audit the FBI's use of NSLs], *in a manner consistent with the President's constitutional authority to supervise the unitary executive branch and to withhold information the disclosure of which could impair foreign relations, national security, the deliberative processes of the Executive, or the performance of the Executive's constitutional duties.*

---

[29] *Oversight of the Federal Bureau of Investigation: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. (2005) (statement of Robert S. Mueller III, FBI Director).

[30] FOIA Documents Discussing Improper Issuance of NSL to a North Carolina University, July 21, 2005-March 13, 2007, http://www.eff.org/files/filenode/07656JDB/charlotte.pdf (last visited March 19, 2008); *see also 2007 OIG Report*, at 82-83.

Remarks on Signing the USA PATRIOT Improvement and Reauthorization Act of 2005, 42 Weekly Comp. Pres. Doc. 423 (Mar. 9, 2006) (emphasis added),. Despite this caveat, the OIG's reporting has revealed more about the FBI's use of NSLs than any other source to date. These reports are discussed in detail below.

b. The Little Public Reporting Available Reveals That the FBI Has Systematically Misused Its NSL Authority.

The PATRIOT Act Reauthorization required the OIG to audit the "effectiveness and use, including any improper or illegal use, of national security letters issued by the Department of Justice." Public Law No. 109-177, § 119. The OIG subsequently issued two reports analyzing the FBI's issuance of NSLs from 2003 through 2006. *See 2007 OIG Report*; Dep't of Justice, Inspector Gen., *A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006* (2008), *available at* http://www.usdoj.gov/oig/special/s0803b/final.pdf [hereinafter *2008 OIG Report*]. These reports documented extensive and systematic misuse of NSLs throughout the FBI, finding that "the FBI used NSLs in violation of applicable NSL statutes, Attorney General Guidelines, and internal FBI policies." *2007 OIG Report*, at 124.

Among other findings, the OIG reports concluded:

- FBI NSL requests have surged from about 8,500 NSL requests in 2000, the year before the PATRIOT Act was passed, to more than 48,106 NSL

requests in 2006.[31] *2007 OIG Report*, at 120; *2008 OIG Report*, at 107.[32]

- The number of NSL requests issued by the FBI under each of the five separate NSL provisions remains secret. However, "the overwhelming majority" of the FBI's NSL requests have been made pursuant to § 2709. *2007 OIG Report*, at 36-37; *2008 OIG Report*, at 107.

- The FBI identified 26 possible violations of the attorney general's intelligence guidelines, laws, executive orders, and/or presidential directives between 2003 and 2005, and 84 possible IOB violations in 2006. *2007 OIG Report*, at 69; *2008 OIG Report*.[33]

- A review of 2003-2005 investigative files at four field offices revealed that 22 percent contained one or more possible violations that had never been reported, representing an overall possible violation rate of 7.5 percent. *2007 OIG Report*, at 78; *2008 OIG Report*, at 76. According to the OIG, these findings suggested "that a significant number of NSL-related possible [IOB] violations throughout the FBI have not been identified or reported by FBI personnel." *2007 OIG Report*, at 84. Indeed, an FBI field review of a larger sample of files found a 9.43 percent rate of possible violations, though the OIG concludes that the actual rate is likely even higher. *2008 OIG Report*, at 76.

- The possible violations reported between 2003 and 2006 generally involved improperly authorized NSLs, improper requests under NSL statutes, and unauthorized collections of information through NSLs. *2007*

[31] The report distinguishes NSL requests from NSL letters, because a single NSL letter may contain multiple requests for information. *2007 OIG Report*, at 120. For example, the FBI issued nine NSL letters in one investigation requesting subscriber information on 11,100 different phone numbers. *Id.* at 36.

[32] Many of these figures are, unfortunately, only the OIG's best estimate, as the FBI's NSL recordkeeping system was poor during the time period covered by the reports, and the available data significantly underestimated the number of NSL requests that had been made. *Id.* at 34. In fact, the OIG estimated that "approximately 8,850 NSL requests, or 6 percent of NSL requests issued by the FBI during [2003-2005], were missing from the [FBI Office of the General Counsel's] database." *Id*.

[33] The increase in 2006 appears to be due to more frequent reporting of third-party errors, as well as greater internal scrutiny of NSLs during the OIG's auditing activities in 2006. *See 2008 OIG Report*, at 153.

OIG Report, at 66-67; *2008 OIG Report*, at 138-143.[34]

- Between 2003 and 2005, the FBI Headquarters Counterterrorism Division issued more than 700 "exigent letters" to three telephone companies seeking information related to more than 3,000 separate telephone numbers. *2007 OIG Report*, at 89. Section 2709 does not permit the FBI to collect such information through so-called "exigent letters," nor does any other legal authority. *Id*. at 93-98. After the exigent letters were discovered, the FBI issued 11 "blanket" NSLs in an attempt to retroactively legitimize the acquisition of information it had obtained through the exigent letters. *2008 OIG Report*, at 123-124. These NSLs were also improperly issued. *Id*. The OIG determined that eight of the "blanket" NSLs contained language categorically barring recipients from disclosing that the FBI had sought or obtained access to requested information under § 2709, and therefore did not comply with the nondisclosure and confidentiality provisions of the USA PATRIOT Improvement and Reauthorization Act of 2005. *Id*. at 127.

- Approximately 300 NSLs were issued under § 2709 between 2003 and 2005 that were apparently not connected to any specific pending FBI investigation. 2007 OIG Report 98-103.[35]

While the FBI is taking steps to mitigate the problems discovered by the OIG,[36] these findings show that the FBI has systematically misused its broad discretion to issue § 2709 NSLs. This discretion, in turn, undermines the central

[34] According to the OIG, "it is important to recognize that in most cases the FBI was seeking to obtain information that it could have obtained properly if it had followed applicable statutes, guidelines, and internal policies." *2007 OIG Report*, at 67.

[35] Congress still struggles to conduct oversight in the wake of the OIG's findings of NSL misuse. During a FBI oversight hearing earlier this month, Senator Chuck Grassley complained, "I'm frustrated by the FBI's refusal to provide us with documents on the exigent letters." *Oversight of the Federal Bureau of Investigation: Hearing Before the S. Comm. on the Judiciary*, 110th Cong. (2008) (statement of Sen. Chuck Grassley).

[36] The OIG has stated, "[w]e believe it is too soon to conclude 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.

goal of law enforcement accountability necessary in a constitutional democracy. *Amici* urge the Court to consider the FBI's documented misuse of § 2709 in determining whether § 2709(c)'s nondisclosure provision can survive constitutional scrutiny.

CONCLUSION

For the foregoing reasons and the reasons set forth in Plaintiffs /Appellees Brief, the Court should uphold the ruling of the District Court.

DATED: March 19, 2008

Respectfully submitted,

/S/

Meredith Fuchs
National Security Archive
George Washington University
Gelman Suite 701
2130 H Street, NW
Washington, D.C. 20016
(202) 994-7000

Marcia Hofmann
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because it contains 6,570 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).
2. 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 it has been prepared in a proportionally spaced typeface using Microsoft Word in 14-point Times New Roman.

/S/
Meredith Fuchs
Counsel for Amicus Curiae
March 19, 2008

CERTIFICATE OF SERVICE

I hereby certify that on March 19, 2008, I filed and served the foregoing BRIEF FOR AMICI CURIAE IN SUPPORT OF PLAINTIFFS-APPELLEES by (1) causing ten copies to be sent to the Clerk of the Court by Fedex overnight mail delivery; (2) sending a PDF copy of the brief to the clerk of the court at briefs@ca2.uscourts.gov; (3) by causing two copies to be sent by First Class U.S. Mail to the below listed counsel; and (4) by causing a PDF copy of the brief to be sent to the below listed counsel:

Jameel Jaffer
Melissa Goodman
L. Danielle Tully
National Legal Department
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
212-549-2500
Counsel for Plaintiffs/Appellees

Jeffrey S. Oestericher
Benjamin H. Torrence
Assistant United States Attorneys
Southern District of New York
86 Chambers Street
New York, NY 10007
Counsel for Defendants/Appellants

/S/
Meredith Fuchs