05-0570-cv

-

IN THE UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

JOHN ASHCROFT, 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 MARION E. BOWMAN, in his official capacity as Senior Counsel to the Federal Bureau of Investigation.

Defendants-Appellants,

v.

JOHN DOE, AMERICAN CIVIL LIBERTIES UNION, and AMERICAN CIVIL LIBERTIES UNION FOUNDATION,

Plaintiffs-Appellees.

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

BRIEF OF *AMICUS CURIAE, NATIONAL SECURITY ARCHIVE, et al.*
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

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* the Project on Government Secrecy discloses that it is a project of the Federation of American Scientists, a not-for-profit corporation established under the laws of the District of Columbia. The Federation of American Scientists has no parent corporation and no stock, thus no publicly held corporation owns ten percent or more of its stock. The Federation's purpose is to conduct policy research and advocacy on science and national security policy.

In accordance with Fed. R. App. P. 26.1, *amicus curiae* the Electronic Privacy Information Center ("EPIC") discloses that it is a not-for-profit corporation established under the laws of the District of Columbia. EPIC has no parent corporation and no stock, thus no publicly held corporation owns ten percent or more of its stock. EPIC's purpose is to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC 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* the National Whistleblower Center ("NWC") discloses that it is a not-for-profit corporation established under the laws of the District of Columbia. The NWC has no parent corporation and no stock, thus no publicly held corporation owns ten percent or more of its stock. The NWC's purpose is to conduct policy research, public education and advocacy for the protection of employees who report misconduct in the workplace or who testify in the proceedings to enforce federal law, and to promote and encourage openness in government and government accountability. The NWC supports employees who have suffered illegal retaliation due to the disclosure of matters in the public interest, including government employees who have reported wrongdoing, gross mismanagement and abuse by federal agencies

resulting in both the infringement of civil liberties and placing our national security at risk. Persons assisted by the NWC have a direct interest in the outcome of this case.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

LEGISLATIVE MATERIALS

INTEREST OF THE *AMICUS CURIAE*

Amicus curiae submit this brief in support of Plaintiffs/Appellees. Appellees brought this case to challenge the issuance and enforcement of national security letters (NSLs) pursuant to 18 U.S.C. § 2709 by the Federal Bureau of Investigation (FBI). Section 2709 permits the FBI to issue NSLs upon a self-certification that the NSL meets the statutory standards and bars the NSL recipient from talking with anyone about the NSL. Appellees argued that the issuance of NSLs without judicial oversight and the secrecy attendant to the process are unconstitutional. The District Court ruled that the statute violated the Constitution's First and Fourth Amendments. *Doe v. Ashcroft*, 334 F. Supp. 2d 471, 511 (S.D.N.Y. 2004). The court further struck down the categorical and permanent prohibitions on disclosing the receipt of such a letter as an impermissible, content-based prior restraint on speech. *Id.* at 525.

Amici are secrecy experts who have long monitored government secrecy policy. Since the September 11 attacks, *amici* have seen a dramatic increase in barriers to information. *Amici*'s interest in this case is to bring to the Court's attention the grave consequences such secrecy can have for the security of the nation and the health of American democracy. *Amici* each frequently seek information on important matters of significant public

interest under open government laws in order to inform the public debate, ensure government accountability, and protect the rights of U.S. citizens. In their work, *amici* 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 Project on Government Secrecy of the Federation of American Scientists promotes public access to government information through research, advocacy, investigative reporting, and publication of government records.

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C. that was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values.

The National Whistleblower Center promotes public access to information and government accountability through research, public education and advocacy. For example, the NWC has provided support and

advocacy on behalf of employee-whistleblowers who have exposed abuse of civil liberties and civil rights by the Federal Bureau of Investigation.

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 concerning government activities. The need for such debate is at its apex in the area of national defense and military relations. Yet, the Government's reflexive response to national 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 each concluded, excessive secrecy was part of the problem that interfered with detection and prevention of the attacks.

In the four years since the September 11 attacks on the United States, a number of new laws restricting the dissemination of information to the public – including the broadening of the national security letter provisions that are at issue in this case – have been enacted. There has also been a dramatic rise in classification of information, a dramatic reduction in

declassification of historical 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 when national security demands such protection. Thus, meaningful judicial review is necessary to separate out the legitimate and illegitimate claims for secrecy.

The FBI's NSL power permits 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 and Fourth Amendments. In addition to the unconstitutional nature of the power, *Amici* contend that the bar against recipients communicating about receipt of a NSL severely undermines accountability.

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 government information disclosure with harm that often is demanded by the Executive in national security matters is a false dichotomy. While there is no doubt that there is a social cost to sharing highly sensitive information that can be used by a terrorist, there also are real costs associated with keeping unnecessary secrets. As the Director of the Information Security Oversight Office (ISOO), the governmental agency responsible to the President for policy oversight of the government-wide security classification system and the National Industrial Security Program,[1] explains:

---

[1] *See* About ISOO, http://www.archives.gov/isoo/about_isoo/about_isoo.html (listing ISOO's

> 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]

That price includes, among others, undermining the legitimacy of government actions,[3] reducing accountability,[4] hindering critical

---

source of authority in executive orders and describing ISOO's mission) (last visited July 27, 2005).

[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. (2005) (statement of J. William Leonard, Director, Information Security Oversight Office (ISOO), Nat'l Archives and Records Admin.), http://reform.house.gov/UploadedFiles/ISOO Leonard testimony final 3-2-05 hearing.pdf.

[3] *See, e.g.*, 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."), http://www.access.gpo.gov/congress/commissions/secrecy/.

[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 process and release records requested under FOIA concerning treatment of detainees held abroad: "The information plaintiffs have requested are matters of significant public

technological and scientific progress,[5] interfering with the efficiency of the marketplace,[6] and breeding paranoia.[7]

Indeed, this is the lesson of the inquiries concerning the September 11 attacks on the United States. It was directly addressed by Eleanor Hill, Staff

---

interest. Yet, the glacial pace at which defendant agencies have been responding to plaintiffs' requests shows an indifference to the commands of FOIA, and fails to afford accountability of government that the act requires. If 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. . . . It is possible that the harm done during a process of negotiating such an agreement—through building walls of mistrust between peoples—would be greater than the benefit gained through the sense of security that such a regime might provide. Finally, such a restrictive regime, the committee believes, could seriously damage the vitality of the life sciences… There is some concern that restricting access to this information might lead to a situation in which the mainstream scientific community is unaware of dangers that may threaten us.").

[6] *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) ("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."), http://www.archives.gov/research/jfk/review-board/report/.

Director, Joint House-Senate Intelligence Committee Investigation into 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 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 Report of the National Commission on Terrorist Attacks on the United States (9/11 Commission), 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 the organizers, particularly Khalid Sheikh Mohammed, 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

---

[8] *Hearing on Intelligence Community's Response to Past Terrorist Attacks Against the United States from February 1993 to September 2001 Before the Joint House/Senate Intelligence Committee*, 107th Cong. (2002) (Joint Inquiry Staff Statement, Eleanor Hill, Staff Dir.), http://intelligence.senate.gov/0210hrg/021008/hill.pdf.

the 9/11 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] 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, 5 U.S.C. § 552, reflects the notion that sharing information with the public will help, not harm, society. The FOIA mandates complete openness, with only carefully delineated exemptions from that general rule. *Dep't of Air Force v. Rose*, 425 U.S. 352, 360-61 (1976) (FOIA creates "a general philosophy of full agency disclosure unless

---

[9] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, 247, 276 & 541 n. 107 (2004), http://www.9-1commission.gov/.

[10] *See Joint Investigation Into September 11th: Joint House/Senate Intelligence Committee Hearing*, 107th Cong. (2002), http://intelligence.senate.gov/0209hrg/020924/hill.pdf (Joint Inquiry Staff Statement, Eleanor Hill, Staff Dir., on "The FBI's Handling of the Phoenix Electronic Communication and Investigation of Zacarias Moussaoui Prior to September 11, 2001.")

[11] *The 9/11 Commission Report* at 276.

information is exempted under the clearly delineated statutory language") (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 Bd. v. Bannercraft Clothing Co., Inc.*, 415 U.S. 1, 17 (1974) (internal quotes omitted), and to prevent the damage that pervasive secrecy in government agencies did to public confidence in their Government. *See* S. Rep. No. 813 (1965), as reprinted in *Senate Comm. on the Judiciary, Freedom of Information Act Source Book: Legislative Materials, Cases, Articles*, S. Doc. No. 93-82, at 45 (1974) (hereinafter *FOIA Sourcebook*) ("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 that 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.[12]

And, 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 *Secrecy: The American Experience*, the Cold War and related arms race were greatly exacerbated by the secrecy imposed by the military establishment. *Id.* at 154-77 (1998). A similar conclusion was reached in a different context by the Senate Select Committee on Intelligence in its investigation of pre-war intelligence concerning weapons of mass destruction in Iraq. The Committee concluded that the CIA's assessment of the situation was hampered by "examining few alternatives, selective gathering of information, pressure to conform within the group or withhold criticism, and collective rationalization."[13]

---

[12] Cass R. Sunstein, *Why Societies Need Dissent* 8 (2003) (citing Luther Gulick, *Administrative Reflections from World War II* 121-29 (1948).

[13] Senate Select Committee on Intelligence, *Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq*, 108th Cong., Chap. 1 at 18 (2004), http://intelligence.senate.gov/iraqreport2.pdf.

Overclassification and unneeded secrecy also undermine the effort 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 the 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.[14]

Moreover, government transparency is a central principle of democracy, and thus not to be lightly tossed aside. As Secretary of Defense Donald Rumsfeld recognized in his recent op-ed in the *Wall Street Journal*,

---

[14] ISOO, *Report to the President* 7 (2002), 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), http://www.osti.gov/opennet/forms.jsp?formurl=document/prcfacts.html#I4 ("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.") (last visited on July 27, 2005).

"[a]s more citizens gain access to new forms of information, to new ways of learning of the outside world, it will be that much more difficult for governments to cement their [anti-democratic] rule by holding monopolies on news and commentary." Donald Rumsfeld, *War of the Worlds*, Wall St. J., July 18, 2005, at A12. This is consistent with the international consensus that the right to know about the activities of government is a fundamental right.[15] The United States has adopted this position by signing the Universal Declaration of Human Rights and the American Convention on Human Rights.

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

Over the past four years there has been a dramatic upsurge in government secrecy. Classification has multiplied, reaching an all-time high of 15.6 million classification actions in 2004, nearly double the number in

[15] *See* Universal Declaration of Human Rights, art. 19, Dec. 10, 1948, UN Resolution 217A(III); African Charter on Human and Peoples' Rights, art. 9, June 26, 1981; European Convention for the Protection of Human Rights and Fundamental Freedoms, art. 10, Nov. 4, 1950; American Convention on Human Rights, art. 13, Nov. 22, 1969; Inter-American Comm'n on Human Rights, Declaration of Principles on Freedom of Expression, para. 4, Oct. 19, 2000.

2001.[16] Moreover, the cost of the program has skyrocketed from an estimated $4.7 billion in 2002 to $7.2 billion in 2004.[17]

Officials from throughout the military and intelligence sectors have admitted that much of this classification activity is unnecessary. Secretary of Defense Donald Rumsfeld acknowledged the problem in an op-ed this past month: "I have long believed that too much material is classified across the federal government as a general rule …."[18] 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% of classification decisions are over-classifications.[19] These opinions echoed that of now-CIA Director Porter

---

[16] ISOO, *2004 Report to the President* at 3 (2005), http://www.archives.gov/isoo/reports/2004-annual-report.pdf.

[17] ISOO, *2004 Report on Cost Estimates for Security Classification Activities for 2004* at 3 (2005), http://www.archives.gov/isoo/reports/2004-cost-report.pdf; ISOO, *2001 Report to the President* at 9 (2002), http://www.archives.gov/isoo/reports/2001-annual-report.pdf.

[18] Donald Rumsfeld, *War of the Worlds*, Wall St. J., July 18, 2005, at A12.

[19] *Subcommittee on National Security, Emerging Threats and International Relations of the House Committee on Gov't Reform Hearing*, 108th Cong. (2004) (testimony of Carol A. Haave), http://www.fas.org/sgp/congress/2004/082404transcript.pdf; *See id*.,

Goss, who told the 9/11 Commission, "we overclassify very badly. There's a lot of gratuitous classification going on, and there are a variety of reasons for them."[20]

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:

> 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.[21]

At the same time that unnecessary classification has surged, the declassification process, which resulted in the declassification of millions of

---

(Testimony of J. William Leonard, Director of ISOO) ("It is my view that the government classifies too much information.").

[20] *9/11 Commission Hearing*, (Testimony of then Chair of the House Permanent Select Committee on Intelligence, now Director of Central Intelligence, Porter Goss) (2003), http://www.9-11commission.gov/archive/hearing2/9-11Commission_Hearing_2003-05-22.htm#panel_two.

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

records annually starting in the mid 1990s, has slowed considerably, falling from a high of 204 million pages in 1997 to 28 million pages in 2004.[22]

The broadened NSL authority and its bar against recipients speaking about receipt of an NSL is one of a number of new laws enacted in the wake of September 11 creating new categories of information that must be kept secret. 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).

It is not merely in the areas of classification, information policy and freedom of speech that secrecy has expanded. The government has expanded 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 *Am. Friends Serv. Comm. v. Dep't of Defense*, 831 F.2d 441,

---

[22] ISOO, *1997 Report to the President* (1998), http://www.archives.gov/isoo/reports/1998-annual-report.html; ISOO, *2004 Report to the President* at 17 (2005), http://www.archives.gov/isoo/reports/2004-annual-report.pdf.

445 (3d Cir. 1987). Several courts properly have highlighted the risks attendant to the 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.

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 it 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, the 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 the 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 categorically and permanently prevent a person from exercising the constitutional right to speak about the receipt of an NSL.

The same expansive use of mosaic theory can be seen in *Ctr. for Nat'l Sec. Studies v. Dep't of Justice*, 331 F. 3d 918 (D.C. Cir. 2003) [hereinafter "*CNSS*"]. There, public interest groups sought the names of more than 1000 individuals who had been rounded up in the aftermath of the September 11 attacks. The information was sought to serve the highest purposes of the open government laws—to investigate allegations that there had been "deprivations of fundamental due process, including imprisonment without probable cause, interference with the right to counsel, and threats of serious bodily injury." *Id.* at 922. Yet, the government argued that that the release of the names could assist terrorists in piecing together the course, direction, and focus of the investigation. *Id.* at 928. This was accepted by the court, over the dissent of Judge Tatel, who exclaimed, "the court's uncritical deference to the government's vague, poorly explained arguments for withholding broad categories of information about the detainees, as well as its willingness to fill in the factual and logical gaps in the government's case,

eviscerates both FOIA itself and the principles of openness in government that FOIA embodies." *Id.* at 937.

The practical implications of the denial of the information sought in *CNSS*) are detailed in a Report of the DOJ Inspector General, who concluded the roundup, detention, and deportation of many of the immigrants was abusive. Detainees, many of whom were held for weeks before they were formally charged, housed in restricted confinement conditions where they were unable to contact their attorneys and families for long periods of time, forced to live in cells illuminated 24-hours a day, and subjected to "pattern of physical and verbal abuse."[23] The vast majority of the detainees were held on immigration charges and ultimately released or deported. Of the 134 held on federal criminal charges, only one was found guilty of a terrorism-related offense.

Certainly the possibility that the government might overreact in the wake of a terrible attack and search for any available tools to establish a sense of control and authority is not itself surprising, but there is no reason

---

[23] Office of the Inspector General, Dep't of Justice, *The September 11 Detainees: A review of the Treatment of Aliens Held on Immigration Charges in Connection with the Investigation of the September 11 Attacks*, at 142-149 (June 2003), http://www.usdoj.gov/oig/special/0312/final.pdf.

for the government to interfere with subsequent discussion of the situation to prevent the perpetuation of abusive government practices.

The government's position on these issues, as with the bar on talking about receipt of a NSL, ensures that there is no check on overreaching. The Government has an interest in preserving such secrecy; it permits the Government to control knowledge and pursue unimpeded its aims.[24]

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

When there is an absence of internal and external checks against government misconduct, as in the case of Section 2709's automatic ban on 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 independent incentive to separate out the illegitimate incentives. This

---

[24] See, e.g., Joseph E. Stiglitz, *Information and the Change in the Paradigm in Economics*, Nobel Prize Lecture, at 523 (2001), http://nobelprize.org/economics/laureates/2001/stiglitz-lecture.pdf (discussion of how governmental control of information gives rise to "rents, "which in some countries are appropriated through outright corruption (selling information), but in others are part of a gift exchange' in which reporters not only provide puff pieces praising the government official who has given the reporter privileged access to information, particularly in ways which are designed to enhance the officials influence and power, but distort news coverage.").

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. It was 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 discovered under FOIA revealed that government attorneys suppressed key evidence and authoritative reports from the Office of Naval Intelligence, the FBI, the Federal Communications Commission, and Army intelligence 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. CA 1984). Had the court required an explanation of the evidence to support the central rationale for interning thousands of Japanese Americans, it would have learned that there was no evidence and would have been able to discern what likely was the true rationale for the policy. The complete deference granted to the government

in *Korematsu*, without any effort to ensure the veracity of the government's claims, undermined accountability, which in turn prevented the public from being the check against abuse that it is supposed to be.

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" (Pentagon Papers). As with *Korematsu*, review of the materials shielded by government secrecy demonstrates that the motivation behind the secrecy was not protection of national security. The Pentagon Papers described a series of misrepresentations and poor policy decisions concerning the Vietnam War. They were improperly leaked. 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."[25] 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.

---

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

In cases such as these, the courts are the only branch that can act as a check against government overreaching. Acquiescence by the judiciary in secrecy is not mandated by our constitutional system. The U.S. Constitution itself contains only one specific mention of secrecy, in Article I, Section 5, which states:

> Each House shall keep a Journal of its Proceedings, and from time to time publish the same, excepting such Parts as may in their Judgment require Secrecy; and the Yeas and Nays of the Members of either House on any question shall, at the Desire of one fifth of those Present, be entered on the Journal.

U.S. Const. art. I, § 5. This constitutional mention does not posit any tension between openness and secrecy. Instead, the Constitution compels publicity for the Congress's proceedings and accountability for its actions, with secrecy as the exception that proves the rule. The Executive's power to keep information secret is not mentioned in the Constitution, but is derived from the Article II powers vested in the President as commander-in-chief and as maker of treaties (with the advice and consent of the Senate).[26]

---

[26] U.S. Const. art. II, § 2. These significant presidential powers are balanced by congressional authority to "provide for the common Defence," *id.* art. I, § 8, cl. 1; "declare War . . . and make Rules concerning Captures on Land and Water," *id*. cl. 11; "make Rules for the Government and Regulation of the land and naval Forces," *id*. cl. 14; advise in and consent to the making of treaties, *id.* art. II, § 2, cl. 2 ; "make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers and all other Powers vested by th[e] Constitution in the Government of the United States," *id*. art. I, § 8, cl. 18; and insist that "[n]o money shall be

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 reminded the executive branch 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*, 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), with the 1974 amendments to the Freedom of Information Act (FOIA), 5 U.S.C. §552. President Ford vetoed the amendments based on his view that it would be unconstitutional for a judge to decide whether a record was properly classified.[27] Congress overrode that veto, 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

---

drawn from the Treasury, but in consequence of Appropriations made by Law." *Id.* § 9, cl. 7.

[27] Veto Message from President Ford to the House of Representatives (Oct. 17, 1974), http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB142/101774%20Veto%20Message.pdf

awesome power of the classification stamp by the Government bureaucracy. S. Rep. No. 93-854 (1974), as reprinted in *FOIA SourceBook,* 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 unique 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. It certainly should not mean deference to *categorical rules* that impose secrecy without reference to any particularized need.

II. 18 U.S.C. § 2709 FACILITATES GOVERNMENT SECRECY BY UNDERMINING ACCOUNTABILITY

Since September 11, 2001, the gap between governmental power and public accountability has widened as the government increasingly withholds from public view information about the agency's counterterrorism efforts. Such secrecy makes it impossible the public to know precisely how the FBI uses its NSL authority under Section 2709. Furthermore, the lack of meaningful reporting frustrates Congress' ability to oversee the government's investigative activity.

As the lower court stated, the "all-inclusive sweep" of Section 2709(c) forbids the recipient of an NSL from "revealing the existence of an NSL inquiry . . . in every case, to any person, in perpetuity, with no vehicle for the ban to ever be lifted from the recipient or other persons affected, under any circumstances, either by the FBI itself, or pursuant to judicial process." *Doe v. Ashcroft*, 334 F. Supp. 2d at 476. 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 specific investigations, Section 2709(c)'s mandatory, permanent "gag" provision shields from scrutiny *every* instance of the FBI's use of NSL authority. The FBI's minimal reporting about its use of Section 2709, along with the heavily redacted nature of the information that has been released, keeps the public and Congress in the dark about the use of this search authority.

a. While Statistics Show the Use of Other Counterterrorism Authority Has Increased Significantly Since 2001, There is Virtually No Public Information About How the FBI Has Exercised Section 2709 NSL Authority.

The FBI's broadened authority to use counterterrorism investigative authority has, since September 11, ignited a trend toward increased exercise of this power and heightened secrecy. At the same time, the continued issuance of NSLs with minimal congressional oversight and no public

disclosure makes this authority exceptional among the FBI's counterterrorism powers.

Due to the minimal public reporting required under the Foreign Intelligence Surveillance Act ("FISA"), we know that in every year since 2001, the FBI has applied for a greater number of orders under FISA.[28] Over the past four years, the number of FISA orders issued yearly has risen more than 75 percent — from 932 in 2001 to 1,228 in 2002, 1,727 in 2003, and 1,758 in 2004. *Id*.[29]

While the heightened use of FISA authorities underscores the need for expanded judicial oversight, even the Foreign Intelligence Surveillance Court ("FISC") has had difficulty obtaining accurate and complete information from the FBI about its counterterrorism investigations. In its

---

[28] *See* Dep't of Justice, Office of Intelligence Policy Review, FOIA Reading Room Records, Frequently Requested Records, http://www.usdoj.gov/oipr/readingroom/oipr_records.htm (last visited July 30, 2005), *also available at* Federation of American Scientists, FISA Annual Reports to Congress, http://www.fas.org/irp/agency/doj /fisa/#rept (last visited July 30, 2005).

[29] An examination of surveillance orders issued under domestic surveillance laws also reveals an increase since 2001, particularly by federal agencies. *See* Administrative Office of the United States Courts, Wiretap Reports, http://www.uscourts.gov/library/wiretap.html (last visited July 30, 2005). In 2004, federal courts in the United States authorized 730 orders at the federal level, compared with only 486 in 2001. During that four-year period, only one court denied a request for a wiretap order. *Id.*

only published decision, the FISC disclosed that prior to the September 11, 2001 attacks, the government had misstated and omitted material facts in more than 75 FISA applications to the court related to terrorism investigations. *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611, 620 (FISA Ct. 2002). No court would know if such misstatements or omissions formed the predication for an NSL, since judicial approval is not required for an NSL's issuance. The mandatory gag provision of Section 2709 only exacerbates this lack of review, as the plain language of the statute permanently prohibits disclosure of the NSL's existence to "any person." 18 U.S.C. § 2709(c).

The FBI is not required to publicly disclose any details of its use of NSLs under Section 2709. The Department of Justice has released no information regarding either the number of NSLs issued under that authority or the circumstances of the NSLs' issuances. In response to the 2003 FOIA request by EPIC and the ACLU, the FBI produced a six-page, fully redacted list, originally marked "secret," of NSLs issued for transactional records during the first fifteen months after the USA PATRIOT Act's enactment.[30] The agency withheld from public scrutiny the details and dates of issuance,

[30] FBI, Transactional Records NSLs Since 10/26/01 (Jan 29, 2003). *available at* http://www.epic.org/privacy/terrorism/usapatriot/foia/nsl-list.pdf.

as well as the "Grand Total" number of NSLs issued during the period. *Id*. Significantly, this redacted list remains the most illuminating public record of the FBI's use of NSLs.

The dramatic increase in FISA applications shows that the FBI's use of its counterterrorism investigative authority has risen drastically since 2001. It is likely that there has been a concomitant increase in the FBI's use of its NSL authority under Section 2709. A November 21, 2001 memorandum from the FBI National Security Law Unit ("NSLU") Office of General Counsel to FBI field offices, obtained by EPIC and the ACLU in 2003 under the FOIA demonstrated the likelihood that NSLs would be issued with greater frequency than in past years. Despite warnings not to overuse NSL authority, the memorandum instructed field offices that "exceed their capacity to issue NSLs" to "seek assistance [from the NSLU] in handling the overflow."[31] This statement indicates the NSLU's anticipation that future use of NSLs, if not widespread when the memorandum was issued in November 2001, was expected to increase substantially. However, the virtually unreviewable nature of this authority makes it impossible to know how extensively § 2709 has been exercised.

---

[31] FBI, Memorandum from Office of the General Counsel, National Security Law Unit, to All Field Offices 9 (Nov. 28, 2001) (hereinafter "FBI Memorandum"), *available at* http://www.epic.org/privacy/terroism.usapatriot/foia/fbi_nls_memo/pdf.

b. The FBI Reports Minimal Information to Congress About Its Issuance of Section 2709 NSLs.

The secrecy created by the lack of information about Section 2709 NSLs is exacerbated by an absence of meaningful congressional oversight. The Electronic Communications Privacy Act requires the FBI to report on the use of NSL authority. 18 U.S.C. § 2709(e). Twice a year, the agency director is expected 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 18 U.S.C. §2709. *Id*. However, Section 2709(e) does not specify what entails "fully inform[ing]" these subcommittees. The November 2001 FBI Memorandum obtained under the FOIA, reveals that the report is prepared on the basis of very little data:

> [E]very model EC [Electronic Communication, identified herein as a "document[] . . . approving the NSL and documenting the predication"] requests NSLU to "record the appropriate information needed to fulfill the Congressional reporting requirements for NSLs." NSLU will be able to compile the reporting data provided that the cover EC includes [1] the case file number, [2] the subject's U.S. person status, [3] the type of NSL issued, and [4] the number of phone numbers, e-mail addresses, account numbers, or individual records being requested in the NSL.[32]

[32] FBI Memorandum at 8.

Moreover, congressional subcommittees have experienced difficulty obtaining these minimal reports the FBI is required to submit on its use of NSLs. For example, after the House Judiciary Committee recently approved a USA PATRIOT reauthorization bill, minority members said in a dissenting statement, "[t]he Justice Department has never accounted for [NSL] use."[33] Further, during a oversight hearing on the USA PATRIOT Act held by the Senate Select Committee on Intelligence, Senator Ron Wyden declared, "[t]he Department of Justice is required to report to this committee on the use of national security letters by the FBI. We haven't gotten the report for 2004. We haven't gotten it. So that makes it hard for us to do oversight[.]"[34] The government's failure to report even the most basic information about issuance of NSLs frustrates Congress' ability to oversee the FBI's use of Section 2709 authority.

---

[33] *USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005, Report of the Committee on the Judiciary, House of Representatives, to Accompany H.R. 3199 Together with Dissenting Views*, H.R. Rep. No. 109-174, at 465 (July 18, 2005), http://judiciary.house.gov/media/pdfs/109-174p1.pdf.

[34] *U.S. Senate Select Committee on Intelligence Holds a Hearing on the USA PATRIOT Act: Hearing Before the Senate Select Comm. on Intelligence*, 109th Cong. (Lexis Apr. 27, 2005) (comment of Sen. Wyden).

Such secrecy allows the FBI tremendous discretion to issue Section 2709 NSLs. This discretion, in turn, undermines the central goal of law enforcement accountability necessary in a constitutional democracy. Amici thus urge the Court to consider the unreviewable nature of the FBI's use of Section 2709 in determining whether Section 2709(c)'s unconditional and permanent bar on disclosure can survive First Amendment 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: August 2, 2005

Respectfully submitted,

_____

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

Marc Rotenberg
Marcia Hofmann
Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 428-1140

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because it contains 6,983 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.

_____
Meredith Fuchs
Counsel for Amicus Curiae
August 2, 2005

CERTIFICATE OF SERVICE

I hereby certify that on August 2, 2005, I filed and served the foregoing BRIEF FOR AMICUS CURIAE IN SUPPORT OF PLAINTIFFS-APPELLEES by causing ten copies to be sent to the Clerk of the Court by Fedex overnight mail delivery and by causing two copies to be sent by First Class U.S. Mail to:

Jameel Jaffer
Ann Beeson
Sharon McGowan
National Legal Department
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
212-549-2500
Counsel for Plaintiffs/Appellants

Douglas N. Letter
Scott R. McIntosh
Attorneys, Appellate Staff
Civil Division Room 7259
Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001
202-514-4052
Counsel for Defendants/Appellees

_____
Meredith Fuchs