No. 06-211

IN THE
Supreme Court of the United States

JOHN GILMORE,

Petitioner,

v.

ALBERTO GONZALES, ATTORNEY GENERAL, *et al*.,

Respondents.

ON PETITION FOR WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

AMICI CURIAE BRIEF OF THE ELECTRONIC FRONTIER FOUNDATION, AMERICAN ASSOCIATION OF LAW LIBRARIES, AMERICAN LIBRARY ASSOCIATION, ASSOCIATION OF RESEARCH LIBRARIES, CENTER FOR DEMOCRACY AND TECHNOLOGY, NATIONAL SECURITY ARCHIVE, PROJECT ON GOVERNMENT SECRECY OF THE FEDERATION OF AMERICAN SCIENTISTS, AND SPECIAL LIBRARIES ASSOCIATION IN SUPPORT OF THE PETITION FOR A WRIT OF CERTIORARI

DAVID L. SOBEL
Counsel of Record
MARCIA HOFMANN
ELECTRONIC FRONTIER FOUNDATION
1875 Connecticut Avenue, NW
Suite 650
Washington, DC 20009
(202) 797-9009

CINDY COHN
LEE TIEN
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333

Counsel for Amici Curiae

TABLE OF CONTENTS

INTEREST OF THE *AMICI CURIAE* 1

SUMMARY OF THE ARGUMENT 3

ARGUMENT 4

A. The Laws of the United States Do Not Permit the Executive Branch to Govern Public Conduct Through Secret Laws; Thus, This Court Must Carefully Review the Executive Branch's Attempts to Hide the Content of its Identification Requirement. 5

1. The FOIA's Legislative History Shows That Congress Did Not Intend for Agencies to Create and Govern the Public With Secret Laws. 6

2. FOIA's Affirmative Disclosure Requirements and Judicial Precedent Recognize Congress' Intention Not to Permit the Shielding of Secret Law From the Public..... 8

B. This Court Should Ensure that TSA Does Not Abuse Its Authority to Designate "Sensitive Security Information" to Impose Secret Laws Upon the Public.. . 12

1. TSA's Authority to Conceal Information as SSI is Overly Broad and Invites Capricious Application, Which Congress Has Recently Recognized..... 13

2. TSA Has Used the SSI Designation to Avoid Releasing Harmless or Already Public Information. 16

3. The SSI Designation May Conceal Security Flaws or Illegal Activity, Undermine the Justice System, and Create Confusion. 17

CONCLUSION 19

TABLE OF AUTHORITIES

Cases

U.S. Dep't of the Air Force v. Rose, 425 U.S. 352 (1976)..... 6, 9

Coastal States Gas Corp. v. U.S. Dep't of Energy, 617 F.2d 854 (D.C. Cir. 1980)..... 11

Cox v. U.S. Dep't of Justice, 601 F.2d 1 (D.C. Cir. 1976)..... 10

Crooker v. BATF, 670 F.2d 1051 (D.C. Cir. 1981)..... 9, 10

U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749 (1989)..... 6, 9

Electronic Privacy Information Center v. U.S. Dep't of Homeland Security, 384 F. Supp. 2d 100 (D.D.C. 2005)..... 16

EPA v. Mink, 410 U.S. 73 (1973)..... 5, 10

Gordon v. FBI, 390 F. Supp. 2d 897 (N.D. Cal. 2004)..... 16

Hardy v. BATF, 631 F.2d 653 (9th Cir. 1980)..... 10

Jordan v. U.S.Dep't of Justice, 591 F.2d 753 (D.C. Cir. 1978)..... 8

Nat'l Archives & Records Admin. v. Favish, 541 U.S. 157 (2004)..... 12

Nat'l Treasury Employees Union v. U.S. Customs Serv., 602 F. Supp. 469 D.D.C. 1984)..... 10

National Labor Relations Board v. Sears, Roebuck & Co., 421 U.S. 132 (1975)..... 9

Renegotiation Bd. v. Bannercraft Clothing Co. Inc., 415 U.S. 1 (1974)..... 6

Rose v. U.S. Dep't of the Air Force, 495 F.2d 261 (2d Cir. 1974)..... 6

Schwartz v. IRS, 511 F.2d 1303 (D.C. Cir. 1975) 11

Sterling Drug Inc. v. FTC, 450 F.2d 698 (D.C. Cir. 1971) 10

Tax Analysts v. IRS, 117 F.3d 607 (D.C. Cir. 1997)..... 10, 11

Wiesenfelder v. U.S. Dep't of Education, 959 F. Supp. 532 (D.D.C. 1997) 10

Wolfe v. U.S. Dep't of Health and Human Servs., 839 F.2d 768 (D.C. Cir. 1988)..... 10

Statutes and Regulations

14 C.F.R. § 191.1 (1997)..... 14

69 Fed. Reg. 28066, 28082-83 16

49 U.S.C. § 114 ..... 12, 15, 16

5 U.S.C. § 552 ..... passim

Pub. L. No. 107-296-116 Stat. 2312..... 15

Pub. L. No. 107-71 § 101(e)(3), 115 Stat. 597 (2002) 15

Pub. L. No. 93-366 § 316, 88 Stat. 409 (1974) 14

Other Authorities

Building on the Information Sharing Environment: Addressing Challenges of Implementation: *Hearing of House Comm. on Homeland Security Subcomm. on Intelligence, Information Sharing, and Terrorism Risk Assessment,* 109th Cong. (2006) 13

Congressional Research Service, RL31826, *Protecting Our Perimeter: "Border Searches" Under the Fourth Amendment* (Aug. 15, 2006)..... 9

Congressional Research Service, RL32664, Interstate Travel: Constitutional Challenges to the Identification Requirement and Other Transportation Security Regulations (2004)..... 14

Meredith Fuchs, *Judging Secrets: The Role Courts Should Play in Preventing Unnecessary Secrecy*, 58 ADMIN. L. REV. 131 (2006) 5, 19

H.R. Rep. No. 1497, 89th Cong., 2d Sess. (1966)..... 8

OpenTheGovernment.org, *Secrecy Report Card 2006* (2006).. 13

RS21727, *Sensitive Security Information (SSI) and Transportation Security: Background and Controversies* (2004) 16, 18, 19

S. Rep. No. 1219, 88th Cong., 2d Sess. (1964) 7

S. Rep. No. 813, 89th Cong., 1st Sess. (1965) 6, 7

The National Security Archive, *Pseudo-Secrets: A Freedom of Information Audit of the U.S. Government's Policies on Sensitive Unclassified Information* (March 2006)..... 14

INTEREST OF THE *AMICI CURIAE*[1]

Amici are a group of non-profit organizations that oppose the Executive branch's regulation of public conduct without appropriate checks or transparency. We believe that a thriving democratic society is inconsistent with governance of the public through secret law.

The Electronic Frontier Foundation ("EFF") is a non-profit, public interest organization dedicated to protecting civil liberties and free expression in the digital world. Founded in 1990 and based in San Francisco, California, EFF has more than 12,000 members and publishes a comprehensive archive of digital civil liberties information at one of the most linked-to websites in the world, http://www.eff.org.

The American Association of Law Libraries ("AALL") is a nonprofit educational organization with over 5000 members nationwide. AALL's mission is to promote and enhance the value of law libraries, to foster law librarianship and to provide leadership and advocacy in the field of legal information and information policy.

The American Library Association ("ALA") is a nonprofit educational organization of over 66,000 librarians, library educators, information specialists, library trustees, and friends of libraries representing public, school, academic, state, and specialized libraries. ALA is dedicated to the improvement of library and information services and the public's right to a free and open information society.

The Association of Research Libraries ("ARL") is a nonprofit association of 123 research libraries in North America. ARL's

---

[1] Neither party has participated in the preparation or financing of this brief. In the interest of fullest disclosure, *amicus* EFF notes that Petitioner Gilmore was a co-founder of the organization, serves on EFF's board of directors and, like many private individuals interested in this field, makes general financial contributions to the operations of EFF.

members include university libraries, public libraries, government and national libraries. Its mission is to shape and influence forces affecting the future of research libraries in the process of scholarly communication. ARL programs and services promote equitable access to and effective uses of recorded knowledge in support of teaching, research, scholarship and community service.

The Center for Democracy and Technology ("CDT") is a non-profit public interest and Internet policy organization. CDT represents the public's interest in an open, decentralized Internet reflecting constitutional and democratic values of free expression, privacy, and individual liberty. CDT's staff has conducted extensive policy research, published academic papers and analyses, and testified before Congress about the impact of national security concerns on civil liberties, as well as on the need for an open and transparent government.

The National Security Archive (the "Archive") is an independent, non-partisan, non-governmental, non-profit research institute located at the George Washington University, which collects and publishes declassified documents concerning U.S. foreign policy.

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 Special Libraries Association ("SLA") is a nonprofit global organization for innovative information professionals and their strategic partners. SLA serves more than 11,000 members in 75 countries in the information profession, including corporate, academic, and government information specialists. SLA promotes and strengthens its members through learning, advocacy, and networking initiatives. For more information, visit us on the Web at http://www.sla.org.

SUMMARY OF THE ARGUMENT

This case squarely presents one of the most critical civil liberties questions of the post-9/11 era: whether a federal agency may set standards for the conduct of members of the public through rules and requirements the public is not permitted to see. Specifically, this case concerns a mandate imposed by the Transportation Security Agency ("TSA") that apparently requires members of the public to present identification or submit to additional security screening to board a domestic airline flight ("the identification requirement").

A prohibition against secret law is reflected throughout the constitutional and statutory law of this nation. Congress created a mechanism to ensure that agencies would not be permitted to impose secret law when it passed the Freedom of Information Act ("FOIA"), a law that grants the public the right to obtain all government agency records with few exceptions. This Court and others have repeatedly affirmed that the FOIA protects the fundamental principle that the public is entitled to know the laws under which it is governed and the standards of conduct to which it will be held. While the FOIA does allow the government to withhold materials that are specifically exempted from disclosure under another statute, and Congress has given the TSA authority to withhold certain transportation security information under this provision, the identification requirement imposes a behavioral mandate upon the public, and is therefore not the type of information Congress intended for agencies to hide from public scrutiny.

TSA has refused to allow the public to see the actual provisions of the identification requirement, claiming that they constitute unclassified "sensitive security information" ("SSI"). The Court should grant *certiorari* and carefully review the government's SSI designation because TSA's actions are a serious encroachment upon constitutional and statutory protections against secret law. The dangers posed by this encroachment are foreshadowed by the overly broad manner

that SSI regulations promulgated by TSA have been applied in the past. If the Court does not review this case and stem the promulgation and enforcement of secret law by TSA, then all executive branch agencies with responsibility for security matters will feel emboldened to legislate in private. Furthermore, the overly broad application of SSI may hide security flaws and illegal activity, frustrate the justice system, create confusion among the public, and otherwise severely undermine government accountability.

Aviation security is an important governmental objective, but should not serve as an excuse not to hold the government accountable. This Court should grant *certiorari* and exercise its authority to review the propriety of TSA's withholding of the identification requirement from the public.

ARGUMENT

While Congress has passed laws giving the TSA and other agencies some latitude to withhold information from the public that might affect transportation security, Congress never intended to give agencies unfettered discretion to impose requirements upon the public's conduct without allowing the public to review those requirements.

Furthermore, there is significant evidence in the public record that TSA has used its SSI regulations to inappropriately withhold excessive amounts of information from the public. Such secrecy may permit TSA to conceal security weaknesses and illegal activity, undermine the administration of justice, and create confusion about what TSA's regulations require.

For these reasons, it is critical that the Court review TSA's application of the SSI regulations to the identification requirement. *Certiorari* should be granted, and the Ninth Circuit's judgment reversed.

A. The Laws of the United States Do Not Permit the Executive Branch to Govern Public Conduct Through Secret Laws; Thus, This Court Must Carefully Review the Executive Branch's Attempts to Hide the Content of its Identification Requirement.

Congress has granted TSA the ability to designate certain types of unclassified information "sensitive security information" for aviation security purposes. However, the legislative history and case law of the primary federal open government law, the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, make clear that Congress never intended to allow agencies unbridled discretion to keep laws or regulations that govern the people's conduct from public review. Although Congress has granted TSA the ability to designate certain types of unclassified information "sensitive security information" for aviation security purposes, Congress did not intend that authority to override constitutional and statutory prohibitions against secret law.

"At a fundamental level, secrecy claims must be measured against our historic and constitutional commitments to government openness." Meredith Fuchs, *Judging Secrets: The Role Courts Should Play in Preventing Unnecessary Secrecy*, 58 ADMIN. L. REV. 131, 139 (2006). The clearest embodiment of American transparency principles, the FOIA, is a benchmark against which the government's SSI claim in this case should be examined.

The FOIA creates a judicially enforceable right for individuals to obtain government agencies records with a few narrowly drawn exceptions. As explained by this Court, "the Act is broadly conceived. It seeks to permit access to official information long shielded unnecessarily from public view and attempts to create a judicially enforceable right to secure such information from possibly unwilling official hands." *EPA v. Mink*, 410 U.S. 73, 80 (1973). The law was intended to "pierce

the veil of administrative secrecy and open agency action to the light of public scrutiny." *Rose v. U.S. Dep't of the Air Force*, 495 F.2d 261, 263 (2d Cir. 1974). Since its initial passage forty years ago, the FOIA was amended by Congress to strengthen the public's right to access government information in 1974, 1976, 1986 and 1996.

1. The FOIA's Legislative History Shows That Congress Did Not Intend for Agencies to Create and Govern the Public With Secret Laws.

The FOIA's legislative history makes clear that Congress did not intend for requirements on the public's behavior to be shrouded in secrecy by agencies. When it passed the FOIA, this Court has noted, Congress was "principally interested in opening administrative processes to the scrutiny of the press and general public," *Renegotiation Bd. v. Bannercraft Clothing Co. Inc.*, 415 U.S. 1, 17 (1974) (citation omitted), and "enabl[ing] the public to have sufficient information in order to be able . . . to make intelligent, informed choices with respect to the nature, scope, and procedure of federal government activities." *Id*. As this Court has recognized, Congress sought to "eliminate [] secret law." *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 796 n.20 (1989) (quoting Frank H. Easterbrook, *Privacy and the Optimal Extent of Disclosure Under the Freedom of Information Act*, 9 J. LEGAL STUDIES 775, 777 (1980)).

Prior to the FOIA's enactment in 1966, the primary public disclosure statute was section 3 of the Administrative Procedure Act, which was "of little or no value to the public in gaining access to records of the Federal Government." S. Rep. No. 813, 89th Cong., 1st Sess. (1965). It had, in fact, "precisely the opposite effect: it is cited as statutory authority for the withholding of virtually any piece of information that an official or an agency does not wish to disclose." *Id*. According to the Senate Committee on the Judiciary:

> Under the present section 3, any Government official can under color of law withhold almost anything from any citizen under the vague standards—or, more precisely, lack of standards—in section 3. It would require almost no ingenuity for any official to think up a reason why a piece of information should not be withheld (1) as a matter of "public interest," (2) "for good cause found," or (3) that the person making the request is not "properly and directly concerned."

S. Rep. No. 1219, 88th Cong., 2d Sess. (1964).

The FOIA was passed specifically to replace this weak and ineffective disclosure law. In their conference reports, the judiciary committees of both the Senate and House of Representatives expressed a clear intent to ensure the law's narrow exceptions to disclosure would not create secret regulations on public conduct. The Senate committee explained that the law's purpose was to

> establish a general philosophy of full agency disclosure unless information is exempted under clearly delineated statutory language and to provide a court procedure by which citizens and the press may obtain information wrongly withheld. . . . It is essential that agency personnel, and the courts as well, be given definitive guidelines in setting information policies. Standards such as "for good cause" are certainly not sufficient.

S. Rep. No. 813, 89th Cong., 1st Sess. (1965). The House committee provided further context for the impetus to revise the federal disclosure law:

> As the Federal Government has extended its activities to solve the Nation's expanding problems—and particularly in the 20 years since the Administrative Procedure Act was established—the bureaucracy has developed its own form of case law. This law is embodied in thousands of orders, opinions, statements, and instructions issued by hundreds of agencies. This is the material which would be made available under subsection (b) of S. 1160 [the bill that eventually became the FOIA].

H.R. Rep. No. 1497, 89th Cong., 2d Sess. (1966).

Thus, the FOIA's legislative history clearly reflects the intent of Congress to prevent the creation of secret, unreviewable agency regulations on public conduct.

2. FOIA's Affirmative Disclosure Requirements and Judicial Precedent Recognize Congress' Intention Not to Permit the Shielding of Secret Law From the Public.

In the four decades since the FOIA's enactment, this Court and others have repeatedly recognized that a fundamental purpose of the statute is to prohibit agencies from maintaining secret requirements with which the public must comply. Put bluntly, "[o]ne of the principal purposes of the Freedom of Information Act is to eliminate 'secret law.'" *Jordan v. U.S. Dep't of Justice*, 591 F.2d 753, 781 (D.C. Cir. 1978) (en banc) (Bazelon, J., concurring).

As an initial matter, the judiciary has noted that the affirmative obligations the FOIA places on agencies weighs against secret law. The Act requires agencies to index "final opinions," "statements of policy and interpretations which have been adopted by the agency," and "instructions to staff that affect a member of the public." 5 U.S.C. § 552(a)(2). As this Court has found, these requirements demonstrate "a strong

congressional aversion to secret (agency) law," as well as "an affirmative congressional purpose to require disclosure of documents which has the force and effect of law." *NLRB v. Sears, Roebuck & Co.*, 421 U.S. 132, 153 (1975) (quoting Kenneth Culp Davis, *The Information Act: A Preliminary Analysis*, 34 U. CHI. L. REV. 761, 797 (1967) and H.R. Rep. No. 1497) (internal citations and quotation marks omitted). *See also Reporters Comm. For Freedom of the Press*, 489 U.S. at 772 n.20 (The FOIA's "indexing and reading-room rules indicate the primary objective is the elimination of 'secret law.'") (quoting Easterbrook, *Privacy, supra*, at 777.)

Furthermore, the courts have repeatedly noted Congress' aversion to secret law in analyses of two of the FOIA's exemptions to the law's broad disclosure requirement: Exemptions 2 and 5.

Exemption 2 of the FOIA exempts from disclosure agency records that are "related solely to the internal personnel rules and practices of an agency." 5 U.S.C. § 552a(b)(2). This Court has established that Exemption 2 may be used to withhold intra-agency records in which the public could not be expected to have any significant interest, *U.S. Dep't of the Air Force v. Rose*, 425 U.S. 352, 369-70 (1976), as well as parts of law enforcement manuals where disclosure could be expected to risk the circumvention of laws or agency regulations. *Crooker v. BATF*, 670 F.2d 1051, 1074 (D.C. Cir. 1981).[2]

---

[2] It is worth underscoring that TSA's identification requirement has not been imposed for criminal investigation purposes. Rather, "the suspicionless screening of passengers *boarding* airplanes is based on . . . the *administrative search* doctrine. Under this exception [to full Fourth Amendment requirements], searches are conducted as part of a regulatory scheme in furtherance of an administrative purpose, rather than as part of a criminal investigation to secure evidence, but must still be reasonable under the Fourth Amendment." Congressional Research Service, RL31826, *Protecting Our Perimeter: "Border Searches" Under the Fourth Amendment* 7 (Aug. 15, 2006) (citing *United States v. Davis*, 482 F.2d 893 (9th Cir. 1973) (emphases in original).

The courts have declared again and again, however, that Exemption 2 may not be used to withhold "secret law" from the public. "All administrative materials, even if included in staff manuals that otherwise concern law enforcement, must be disclosed unless they come under one of the other exemptions of the act. Such materials contain the 'secret law' which was the primary target of the act's broad disclosure provisions." *Hardy v. BATF*, 631 F.2d 653, 657 (9th Cir. 1980) (citing *Cox v. U.S. Dep't of Justice*, 601 F.2d 1, 5 (D.C. Cir. 1976)). Information cannot be properly withheld under Exemption 2 when it "purport[s] to regulate activities among members of the public [or] set[s] standards to be followed by agency personnel in deciding whether to proceed against or to take action affecting members of the public." *Cox*, 601 F.2d at 5; *see also Crooker,* 670 F.2d at 1075*; Wiesenfelder v. U.S. Dep't of Education*, 959 F. Supp. 532, 535 (D.D.C. 1997); *Nat'l Treasury Employees Union v. U.S. Customs Serv*., 602 F. Supp. 469, 474 (D.D.C. 1984).

Likewise, a strong preference against secret law has been read by courts into Exemption 5 of the FOIA, which protects "inter-agency or intra-agency memorandums or letters which would not be available to a party other than an agency in litigation with the agency." 5 U.S.C. § 552a(b)(5). This exemption includes a deliberative process privilege, which protects from public disclosure "materials which are both predecisional and deliberative." *Mink*, 410 U.S. at 88; *Tax Analysts v. IRS*, 117 F.3d 607, 616 (D.C. Cir. 1997); *Wolfe v. U.S. Dep't of Health and Human Servs.*, 839 F.2d 768, 774 (D.C. Cir. 1988) (en banc). Just a few years after the FOIA was first passed, the D.C. Circuit unequivocally declared that the deliberative process privilege could *not* be asserted to protect materials that directly govern the public's conduct: "These are not the ideas and theories which go into the making of the law, they are the law itself, and as such should be made available to the public." *Sterling Drug Inc. v. FTC*, 450 F.2d 698, 708 (D.C. Cir. 1971).

Courts have continued to apply this fundamental principle in subsequent cases. As the D.C. Circuit has stressed:

> [A] major limitation on the exemption for internal memoranda is that they are not protected, even though they are deliberative rather than factual, if they represent policies, statements or interpretations of law that the agency has actually adopted. The purpose of this limitation is to prevent bodies of "secret law" from being built up and applied by government agencies. The policy basis for this exemption is derived from a perceived need not to frustrate the explicit commands of the statute that "final opinions . . . and . . . orders," "statements of policy" and "instructions to staff" be accessible to the public.

Schwartz v. IRS, 511 F.2d 1303, 1305-06 (D.C. Cir. 1975) (citing *Sterling Drug*, 450 F.2d at 698, and 5 U.S.C. § 552a(a)(1) & (2)). Over the decades, the prohibition against "secret law" has become well established in FOIA case law.

> A strong theme of our [deliberative process] opinions has been that an agency will not be permitted to develop a body of 'secret law,' used by it in the discharge of its regulatory duties and in its dealings with the public, but hidden behind a veil of privilege because it is not designated as "formal," "binding" or "final."

Coastal States Gas Corp. v. U.S. Dep't of Energy, 617 F.2d 854 (D.C. Cir. 1980); *Tax Analysts*, 117 F.3d at 616.

The FOIA does contain an exemption for materials "specifically exempted from disclosure by statute," 5 U.S.C. § 552a(b)(3), and Congress has permitted TSA to shield certain "security activities" from disclosure under the FOIA, 49 U.S.C.

§ 114(s). However, agency regulations on public behavior are not the type of information Congress meant to preclude from public scrutiny, as the legislative history and judicial interpretation of the FOIA show. The Court must not permit this exemption to swallow a central purpose of the statute: to provide an oversight mechanism for the government's actions. As this Court recently observed, FOIA is "a means for citizens to know 'what the Government is up to.' This phrase should not be dismissed as a convenient formalism. *It defines a structural necessity in a real democracy*." *Nat'l Archives & Records Admin. v. Favish*, 541 U.S. 157, 171-172 (2004) (citations omitted) (emphasis added).

Thus, the Court should grant *certiorari* to review the propriety of the government's SSI designation in this case.

B. This Court Should Ensure that TSA Does Not Abuse Its Authority to Designate "Sensitive Security Information" to Impose Secret Laws Upon the Public.

This Court should examine whether the government's identification requirement is properly designated as SSI and thus rightfully shielded from public review. While Congress has given TSA discretion to designate SSI, the agency has promulgated regulations in recent years suggesting that it has unfettered discretion to keep virtually anything from the public merely by labeling it SSI. Courts have determined that this authority has been applied in an overly broad manner, and the Congressional Research Service ("CRS") has reported that TSA has used the SSI designation in controversial ways. This Court must not permit TSA to use the SSI label to impose secret laws upon the pubic. If the Court permits this sort of administrative lawmaking, other agencies will follow TSA's lead and create secret laws to govern the public's conduct. For this reason, it is critical that the Court exercise its authority here to review the propriety of the agency's SSI designation as applied to the identification requirement.

1. TSA's Authority to Conceal Information as SSI is Overly Broad and Invites Capricious Application, Which Congress Has Recently Recognized.

In recent years, the government has developed new policies to keep certain types of unclassified information from the public. "Government secrecy continues to expand across a broad array of agencies and actions, including military procurement, new private inventions, and the scientific and technical advice that the government receives." OpenTheGovernment.org, *Secrecy Report Card 2006* at 2 (2006). According to an official within the Office of the Director of National Intelligence, more than 60 unique designations are used throughout the government to label information sensitive but unclassified, thus keeping it from public review. *Building on the Information Sharing Environment: Addressing Challenges of Implementation*: *Hearing of House Comm. on Homeland Security Subcomm. on Intelligence, Information Sharing, and Terrorism Risk Assessment,* 109th Cong. (2006) (testimony of Thomas E. McNamara, Program Manager, Office of the Director of National Intelligence).

Troublingly, there is little institutional oversight of administrative use of these designations:

> The picture that emerges from the diverse [sensitive but unclassified] policies . . . shows little likelihood that Congress or the public will be able to assess whether these policies are being used effectively to safeguard the security of the American public, or abused for administrative convenience or for improper secrecy. Unlike classified records or ordinary agency records subject to FOIA, there is no monitoring on the use or impact of protective sensitive unclassified information markings.

The National Security Archive, *Pseudo-Secrets: A Freedom of Information Audit of the U.S. Government's Policies on Sensitive Unclassified Information* i (March 2006).

Because administrative agencies apply these secrecy labels with little or no accountability, it is critical that this Court ensure these designations are not used to undermine the fundamental principles of the FOIA and impose secret law upon the public.

The concept of SSI originated with the Air Transport Security Act of 1974, which authorized the Federal Aviation Administration ("FAA") to withhold certain information from the public. Pub. L. No. 93-366 § 316, 88 Stat. 409 (1974). The narrow language of this law permitted the FAA to:

> Prohibit disclosure of any information obtained or developed in the conduct of research and development activities . . . if in the opinion of the Administrator the disclosure of such information—(A) would constitute an unwarranted invasion of personal privacy . . . (B) would reveal trade secrets or privileged or confidential commercial or financial information obtained by any person; or (C) *would be detrimental to the safety of persons traveling in air transportation.*

Id. (emphasis added). The FAA implemented these requirements by promulgating regulations that, *inter alia*, established the SSI designation, which in 1997 was defined as "records and information . . . obtained or developed during security activities or research and development activities." 14 C.F.R. § 191.1 (1997); Congressional Research Service, RL32664, *Interstate Travel: Constitutional Challenges to the Identification Requirement and Other Transportation Security Regulations* 2 (2004). The SSI designation applied at that time

to air transportation entities and personnel. Congressional Research Service, *Interstate Travel* at 2.

In 2002, the Aviation and Transportation Security Act created TSA within the Department of Transportation ("DOT"), and transferred authority for designating SSI, among other responsibilities, to the TSA. Pub. L. No. 107-71 § 101(e)(3), 115 Stat. 597, 603 (2002). The law also broadened the definition of SSI to include information about other forms of transportation. *Id*. Later that year, the Homeland Security Act of 2002 transferred TSA from the DOT to the Department of Homeland Security ("DHS"). Pub. L. No. 107-296-116 Stat. 2312. This law delegated to TSA authority to:

> Prescribe regulations prohibiting the disclosure of information obtained or developed in carrying out security under authority of the Aviation and Transportation Security Act (Public Law 107-71) or under chapter 449 of this title if the Under Secretary decides that disclosing the information would—(A) be an unwarranted invasion of personal privacy; (B) reveal a trade secret or privileged or confidential commercial or financial information; or (C) *be detrimental to the security of transportation*.

Id. at § 1601(b) (codified as amended at 49 U.S.C. § 114(s) (2004)) (emphasis added).[3]

In May 2004, TSA and DHS published a Federal Register notice listing sixteen distinct types of information that may be labeled SSI under the Homeland Security Act, including such broad categories as material that might "be detrimental to transportation safety"; "Security Directives," along with "[a]ny

[3] A similar statutory provision applying to DHS's Secretary of Transportation authorizes nondisclosure of information that is "obtained or developed in ensuring [transportation] security." 49 U.S.C. § 40119(b)(1).

comments, instructions, and implementing guidance pertaining thereto"; and the catch-all "any information not otherwise described in this section that TSA determines is SSI under 49 U.S.C. 114(s) or that the Secretary of [the DOT] determines is SSI under 49 U.S.C. 40119." 69 Fed. Reg. 28066, 28082-83 (codified at 49 C.F.R. § 1520.5).

2. TSA Has Used the SSI Designation to Avoid Releasing Harmless or Already Public Information.

According to a report by CRS, the SSI regulations at issue here "are intended to reduce the risk of vital security information reaching the wrong hands and resulting in another terrorist attack." RS21727, *Sensitive Security Information (SSI) and Transportation Security: Background and Controversies* 3 (2004). Courts have found, however, that TSA applied these regulations in an overbroad manner to avoid releasing innocuous or already public information.

In 2004, Judge Charles R. Breyer of the Northern District of California performed an *in camera* review of material withheld by the government when a FOIA requester challenged, *inter alia*, TSA's designation of information about the agency's "no-fly" watch list as related to a security directive under its SSI regulations. *Gordon v. FBI*, 390 F. Supp. 2d 897, 899-900 (N.D. Cal. 2004). Judge Breyer determined that TSA did not meet its burden of showing that certain information was properly withheld "by simply reciting" that it was SSI. *Id*. In fact, the court found, TSA relied upon "frivolous claims of exemption" to withhold "innocuous information" that was "common sense and widely known." *Id*.

Since then, the district court for the District of Columbia has similarly found an unsupported SSI designation legally inadequate to support withholding of information under the FOIA. *See Electronic Privacy Information Center v. Dep't of Homeland Security*, 384 F. Supp. 2d 100, 110 (D.D.C. 2005)

(rejecting TSA's mere statement that a document constitutes SSI, and finding that the government must "provide a more adequate description in order to justify the application of [Exemption 3] to the withheld material.").

In addition to these judicial determinations, at least one FOIA request shows that TSA made arbitrary withholdings of information under the SSI regulations. In this instance, TSA refused to release information labeled SSI in a response to a FOIA request from the National Security Archive, despite the fact that the information had been disclosed to the public in the final report of the National Commission on Terrorist Attacks Upon the United States ("9/11 Commission"). Press Release, National Security Archive, Government Censors Aviation Warnings Leading Up to 9/11 (Nov. 14, 2004).[4] Specifically, TSA used the SSI designation to keep secret the titles and texts of five aviation warnings, also known as Information Circulars, that had been transmitted to airlines shortly before the attacks. *Id*. However, the titles and information in the warnings had already been published in the 9/11 Commission report, which was at one time the bestselling book in the United States. *Id*. When the National Security Archive appealed the withholdings, TSA finally released the information. National Press Release, Security Archive, 9/11 Commission Staff Report on FAA Failings Published on Web (Feb. 10, 2005).[5]

3. The SSI Designation May Conceal Security Flaws or Illegal Activity, Undermine the Justice System, and Create Confusion.

In addition to these documented uses of the SSI regulations to withhold information that should have rightfully been released to the public, the CRS has reported at length that the designation has "raised a number of concerns about the management of [SSI] information and the accountability of

[4] http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB137/index.htm.
[5] http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB148/index.htm.

governmental agencies." CRS, *Sensitive Security Information* at 3.

In one instance identified by the CRS, the SSI label was controversially applied to conceal information related to an incident in which a baggage screener permitted a passenger to clear security after a test indicated his luggage might contain an explosive. *Id*. The lack of public information about this incident made it impossible to understand how this security breach occurred or might be avoided in the future, and ultimately undermines public faith in the reliability of airport security measures.

The government has also applied the SSI designation in a manner that undermined the criminal justice system. The CRS reported that TSA's assertion of the SSI label may have negatively impacted the criminal prosecution of a baggage screener who allegedly stole items from passenger baggage. *Id*. at 3-4. The U.S. attorney prosecuting the case ultimately dropped the charges when a court ruled that the baggage screener's attorneys would be permitted to cross-examine the government's witnesses, which the government determined "could raise the possibility of disclosing SSI about TSA's security and training procedures." *Id*. at 4. This incident may have discouraged future prosecutions against TSA employees accused of criminal activity that could potentially concern SSI. The government's SSI claims have made it impossible for plaintiffs to pursue recourse in the civil context, as well, as this case demonstrates). In civil cases, as in the criminal prosecution discussed *supra*, concerns about disclosing SSI undermine the ability of the courts to render justice.

According to the CRS, another divisive use of SSI involved the execution of security agreements between TSA, airports, and local law enforcement that prohibited police from publicly commenting, without the approval of TSA officials, on incidents occurring on airport property that involved SSI. *Id*. at 5. A police chief in Iowa expressed concern that these

agreements might bar the police from reporting arrests for minor incidents at airports or even presenting testimony in court without the prior approval of TSA. *Id*. (citing Tom Alex, "Secrecy in Airport Security Contract Criticized," *Des Moines Register*, Sept. 27, 2003, at 1A). Upon the request of Iowa's senators, TSA explained that the agreements were not intended to impose a "gag order" on police, and also clarified that law enforcement officers did not require TSA approval to testify in court about matters not involving sensitive information. CRS, *Sensitive Security Information* at 5-6. TSA also ultimately agreed to make copies of the agreement publicly available, with redactions for SSI. *Id*. at 6. This incident illustrates, however, that the SSI designation can easily create confusion about the measures those with a "need to know" are expected to take to conceal SSI from the public. Such confusion may lead officials to exercise an abundance of caution, and keep more information secret than necessary.

This Court should not allow TSA to use the SSI designation to govern the public's conduct through secret laws. As one open government authority has noted, there are "real costs associated with keeping unnecessary secrets." Fuchs, *Judging Secrets,* 58 ADMIN. L. REV. at 136. These costs include "undermining the legitimacy of government actions, reducing accountability, hindering critical technological and scientific progress, interfering with the efficiency of the marketplace, and breeding paranoia." *Id*. at 136-137. It is clear that the SSI designation has raised many of these concerns in the context of the identification requirement. For this reason, it is critical that the Court carefully examine TSA's application of the SSI label here to ensure that it has not been used to impose secret law upon the public.

CONCLUSION

For the forgoing reasons, the petition for a writ of *certiorari* should be granted.

Respectfully submitted,

David L. Sobel
Counsel of Record
Marcia Hofmann
ELECTRONIC FRONTIER FOUNDATION
1875 Connecticut Ave. NW
Suite 650
Washington, DC 20009
(202) 797-9009

Cindy Cohn
Lee Tien
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell St.
San Francisco, CA 94110
(415) 436-9333

November 2006

Counsel for Amici