DEPARTMENT OF JUSTICE
Federal Bureau of Investigation

AAG/A Order No. 005-2005
Privacy Act of 1974; Notice to Establish System of Records

AAG/A Order No. 006-2005
Proposed Rule

Terrorist Screening Records System

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

By notice published on July 28, 2005, the Federal Bureau of Investigation ("FBI") established a system of records, the Terrorist Screening Records System ("TSRS"), to encompass the government's consolidated terrorist watch list information, operational support records, and records related to complaints or inquiries.[1] The same day, the FBI published a notice that exempts the TSRS from numerous Privacy Act requirements.[2]

Pursuant to these notices, the Electronic Privacy Information Center ("EPIC") submits these comments to address the substantial privacy issues raised by government watch lists and other information contained in this new system of records; to request that the Bureau extend this public comment period until the government is willing to make more information about the TSRS available to the public; to request that the FBI substantially revise its Privacy Act notice prior to implementation of the new system of records; and to urge the agency to delay the implementation of this system until crucial due process and privacy issues have been addressed.

---

[1] Notice to Establish System of Records, 70 Fed. Reg. 43715 (July 28, 2005).

[2] Proposed Rule, 70 Fed. Reg. 43661 (July 28, 2005).

According to the Bureau, the TSRS will contain classified and unclassified information about known or suspected terrorists, individuals who are screened by the Terrorist Screening Center ("TSC") as possible watch list matches, individuals who are misidentified as watch list matches, individuals who submit redress inquiries, and information about encounters with all of these individuals.[3] As envisioned, the system will be used to make important determinations about individuals, such as whether they may fly on airplanes, enter the United States, obtain United States citizenship, or be arrested.[4] Despite its potential impact on the lives of millions of citizens, the system is likely to contain inaccurate, incomplete, untimely, irrelevant and unnecessary information. In addition, citizens may not be able to access or correct this information, and they will have no judicially enforceable right of redress for negative determinations made on the basis of the information in this system. Furthermore, neither the FBI nor agencies that use TSRS information have yet identified effective redress procedures to ensure that innocent citizens are not improperly flagged again and again. In short, the TSRS is exactly the sort of records system Congress intended to prohibit when it enacted the Privacy Act of 1974.[5]

Introduction

The Terrorist Screening Center ("TSC") is a multi-agency effort spearheaded by the FBI that has been tasked with consolidating several watch lists into a single database.[6]

---

[3] 70 Fed. Reg. 43716.

[4] *Id.*

[5] 5 U.S.C. § 552a.

[6] Congressional Research Service, RL32366, *Terrorist Identification, Screening, and Tracking Under Homeland Security Presidential Directive 6* 2 (Apr. 21, 2004).

The purpose of the TSC is to enhance the government's ability to "protect the people, property, and territory of the United States against acts of terrorism."[7] As of April 2005, the TSC's Terrorist Screening Database included information from twelve government watch lists maintained by the Department of State, Department of Homeland Security ("DHS"), Department of Justice, FBI, Marshals Service, Department of Defense, and the Air Force.[8]

Two watch lists that have become part of the Terrorist Screening Database are the Department of Homeland Security's "no-fly" and "selectee" lists,[9] which have been long known to pose misidentification problems that passengers find difficult, if not impossible, to resolve.[10] Although the public does not know—based upon the FBI's TSRS notices—all the ways in which the consolidated watch list may be used, it is expected to be a central feature of Secure Flight, the Transportation Security Administration's proposed air passenger prescreening program that will "screen" tens of millions of citizens.[11]

---

[7] The White House, *Homeland Security Presidential Directive/HSPD-6, Integration and Use of Screening Information* (Sept. 16, 2003), http://www.whitehouse.gov/news/releases/2003/09/20030916-5.html.

[8] Department of Justice, Inspector General, Audit Division, Audit Report No. 05-27, *Review of the Terrorist Screening Center* iii (June 2005) (hereinafter "Inspector General Report").

[9] *Id*. at 8.

[10] In 2002, EPIC obtained through the Freedom of Information Act dozens of complaint letters sent to TSA by irate passengers who felt they had been incorrectly identified for additional security or were denied boarding because of the "selectee" and "no fly" watch lists. The complaints describe the bureaucratic maze passengers encounter if they happen to be mistaken for individuals on the list, as well as the difficulty they encounter trying to exonerate themselves. Documents recently obtained from TSA show that passengers still experience these problems. *See* EPIC, *Documents Show Errors in TSA's "No-Fly" Watchlist*, http://www.epic.org/privacy/airtravel/foia/watchlist_foia_analysis.html (last accessed Sept. 5, 2005).

[11] Privacy Act of 1974; System of Records: Secure Flight Test Records; Privacy Impact Assessment; Secure Flight Test Phase, 70 Fed. Reg. 36320 (June 22, 2005).

The U.S. Supreme Court has long recognized that citizens enjoy a constitutional right to travel. Thus, in *Saenz v. Roe*, the Court noted that the "'constitutional right to travel from one State to another' is firmly embedded in our jurisprudence."[12] For that reason, any governmental initiative that conditions the ability to travel upon the surrender of privacy rights requires particular scrutiny. This concern is particularly relevant to the use of watch list information in the context of aviation security. When the Department of Justice Inspector General issued a report on the Terrorist Screening Center in June 2005, he concluded that the system presented major concerns about, among other things, data accuracy and completeness.[13]

When it enacted the Privacy Act in 1974, Congress sought to restrict the amount of personal information that federal agencies could collect and, significantly, required agencies to be transparent in their information practices.[14] The Privacy Act is intended "to promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems and data banks of the Federal Government[.]"[15] Adherence to these requirements is critical for a system like the TSRS.

Unfortunately, the FBI's exemption-heavy Privacy Act notice, along with a complete lack of responsiveness to requests for information under Freedom of Information Act ("FOIA"), shows that the FBI and other agencies involved in providing

---

[12] 526 U.S. 489 (1999), quoting *United States v. Guest*, 383 U.S. 745 (1966).

[13] Inspector General Report, *supra* note 8, at 66-67.

[14] S. Rep. No. 93-1183, at 1 (1974).

[15] *Id*.

information to the TSC continue to fall short of such accountability and transparency in the creation and maintenance of anti-terrorism watch lists.

I. The FBI Has Thwarted Public Scrutiny of Watch Lists and the Terrorist Screening Center Under the Freedom of Information Act

As an initial matter, we note the lack of public disclosure concerning the system of records at issue in this proceeding. Last year, EPIC submitted a FOIA request to the FBI for information about the use of the Terrorist Screening Database within the proposed Secure Flight program. Almost a year and two lawsuits later, EPIC continues to experience tremendous difficulty gathering meaningful information from the FBI through the FOIA about the government's most recent passenger prescreening initiative and the use of watch lists in that program.

On September 30, 2004, EPIC submitted a FOIA request to the FBI asking for information about the maintenance and administration of the Terrorist Screening Database in the context of Secure Flight.[16] EPIC noted the substantial public interest in the issue, and noted the urgency for the public to learn as much as possible about Secure Flight prior to the expiration of a comment period during which the public could provide feedback on the Secure Flight proposal. The Bureau denied EPIC's request, claiming that EPIC failed to adequately justify the need for the information's quick release.[17] In response to the FBI's denial, EPIC filed suit and sought an order requiring the Bureau to

[16] Letter from Marcia Hofmann, Staff Counsel, EPIC, to David M. Hardy, Chief, Record/Information Dissemination Section, Records Management Division, FBI, Sept. 30, 2004 (on file with EPIC).

[17] Letter from David M. Hardy, Chief, Record/Information Dissemination Section, Records Management Division, FBI, to Marcia Hofmann, Staff Counsel, EPIC, Oct. 1, 2004 (on file with EPIC).

process and release the documents immediately.[18] The very next day, the FBI voluntarily granted expedited processing of EPIC's request, which rendered EPIC's lawsuit moot.[19]

When the FBI failed to respond to EPIC's request by December, EPIC filed a second lawsuit and motion for a preliminary injunction to force the agency to release the documents EPIC had requested.[20] EPIC agreed to withdraw the motion in exchange for the FBI's promise to release the requested documents by March 1, 2005. The FBI then identified 887 pages of material responsive to EPIC's request, releasing only 132 heavily redacted pages. Four months later, the FBI informed EPIC that it had failed to conduct a full search for the records, and that it had improperly withheld material on national security and proprietary grounds. To date, the Bureau continues to resist disclosure of relevant material.

The Bureau's refusal to release responsive information about the use of watch list information in the Secure Flight program prior to the close of this comment period frustrates the ability of the public to submit meaningful, well-informed comments in response to these notices. In order for this notice and comment period to be anything other than a perfunctory exercise, the time for comment should be extended until the Bureau and other agencies are willing to release more substantial information about the consolidated watch list and its use in programs such as Secure Flight.

---

[18] Motion for a Temporary Restraining Order and Preliminary Injunction, *Electronic Privacy Information Center v. Dep't of Justice*, C.A. 04-1736 (D.D.C. 2004 HHK).

[19] Letter from David M. Hardy, Chief, Record/Information Dissemination Section, Records Management Division, FBI, to Marcia Hofmann, Staff Counsel, EPIC, Oct. 13, 2004 (on file with EPIC); Order, *Electronic Privacy Information Center v. Dep't of Justice*, C.A. 04-1736 (D.D.C. 2004 HHK).

[20] Motion for a Preliminary Injunction, *Electronic Privacy Information Center v. Dep't of Justice*, C.A. 04-2164 (D.D.C. 2004 HHK).

II. The FBI's TSRS Proposal Contravenes the Intent of the Privacy Act

The Privacy Act was intended to guard citizens' privacy interests against government intrusion. Congress found that "the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies," and recognized that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States."[21] It thus sought to "provide certain protections for an individual against an invasion of personal privacy" by establishing a set of procedural and substantive rights.[22] As we detail below, the exemptions claimed by the FBI for the TSRS are thoroughly inconsistent with the purpose and intent of the Privacy Act.

As an initial matter, we note that the FBI has invoked 5 U.S.C. §§ 552a(j)(2), (k)(1), and (k)(2) as authority for its exemption of specific Privacy Act requirements. Subsection (k)(2) is applicable only where the system of records is "investigatory material compiled for law enforcement purposes." The subsection provides, however, that "if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual[.]" Given that the Bureau seeks to exempt the TSRS system of records from the Privacy Act's access provisions, as we discuss in detail below, it is unclear whether subsection (k)(2) authorizes the FBI's action. As such, we urge the Bureau to explain more fully how subsection (k)(2) provides the authority to exempt the system of records from the

[21] Pub. L. No. 93-579 (1974).

[22] *Id*.

various Privacy Act provisions the agency cites.

We also question whether the FBI's invocation of exemptions is procedurally and substantively sound. The legislative history of the Privacy Act suggests it is not:

> Once the agency head determines that he has information legitimately in one of his information systems which falls within these definitions [of exemptable categories] then he must, via the rulemaking process, determine that application of the challenge, access and disclosure provisions would "seriously damage or impede the purpose for which the information is maintained." The Committee intends that this public rulemaking process would involve candid discussion of the general type of information that the agency maintains which it feels falls within these definitions and the reasons why access, challenge or disclosure would "seriously damage" the purpose of the maintenance of the information. The Committee hastens to point out that even if the agency head can legitimately make such a finding he can only exempt the information itself or classes of such information . . . and not a whole filing system simply because intelligence or investigative information is commingled with information and files which should be legitimately subject to the access, challenge and disclosure provisions.[23]

The FBI's notice does not appear to be the kind of "rulemaking" that Congress envisioned. Though the FBI has cited reasons for claiming Privacy Act exemptions, it has not explained why it has determined that the application of standard Privacy Act procedures would "seriously damage" the purpose of the system of records. In addition, the application of the claimed exemptions to the *entire* system of records is clearly inappropriate, as it will obviously contain information "which should be legitimately subject to the access, challenge and disclosure provisions."[24] The Bureau must cure these defects before implementing the TSRS system of records.

---

[23] S. Rep. No. 93-3418, at 75 (1974).

[24] *See also* Privacy Act Implementation: Guidelines and Responsibilities, 40 Fed. Reg. 28948, 28972 (Office of Management and Budget July 9, 1975) (hereinafter "OMB Guidelines") ("agencies should, wherever practicable, segregate those portions of systems for which an exemption is considered necessary so as to hold to the minimum the amount of material which is exempted").

A. The FBI's TSRS Proposal Permits the Collection and Maintenance of Inaccurate, Untimely, Incomplete, Irrelevant, and Unnecessary Information

The TSC is required to "develop and maintain, to the extent permitted by law, the most thorough, accurate, and current information possible about individuals" related to terrorism.[25] It is thus incredible that the FBI has exempted the TSRS from the fundamental Privacy Act requirement that it "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination."[26] To make matters worse, the FBI has also exempted the system from the obligation that an agency "maintain in its records only such information about an individual as is relevant and necessary" to achieve a stated purpose required by Congress or the President.[27] Such open-ended, haphazard data collection plainly contradicts the objectives of the Privacy Act and raises serious questions concerning the potential impact of the TSC screening process on millions of law-abiding citizens.

The TSC's refusal to ensure the accuracy of the data in the TSRS is particularly troubling in light of evidence that the consolidated watch list has been found to be rife with inaccuracies. The Department of Justice Inspector General reported in June 2005 that

> our review of the consolidated watch list identified a variety of issues that contribute to weaknesses in the completeness and accuracy of the data, including variances in the record counts between [two versions of the Terrorist Screening Database], duplicate records, missing or inappropriate

[25] *Memorandum of Understanding on the Integration and Use of Screening Information to Protect Against Terrorism* 1 (Sept. 16, 2003).

[26] 5 U.S.C. § 552(a)(e)(5).

[27] 5 U.S.C. § 552a(e)(1); 70 Fed. Reg. 43661.

handling instructions or categories, missing records, and inconsistencies in identifying information between TSDB and source records."[28]

Furthermore, a TSC official informed the Government Accountability Office that approximately 4,800 individuals' records had been purged from the consolidated watch list as of December 2004, presumably because they did not belong there.[29] Though the Inspector General's report indicated that the TSC has taken steps to improve data accuracy,[30] it is unclear that the Terrorist Screening Database's problems have been fully resolved.

As OMB noted in its guidelines for Privacy Act implementation, "[t]he objective of [requiring agencies to maintain reasonable data quality] is to minimize, if not eliminate, the risk that an agency will make an adverse determination about an individual on the basis of inaccurate, incomplete, irrelevant, or out-of-date records that it maintains."[31] Maintaining the most accurate possible data is unquestionably a critical goal for the TSRS, since a false negative match to the consolidated watch list could fail to detect a known a terrorist, while a false positive match could erroneously label an innocent citizen a terrorist. The Bureau should therefore observe the Privacy Act's accuracy requirements as carefully as possible, rather than exempt itself from the responsibility to maintain accurate records.

Furthermore, in adopting the Privacy Act, Congress was clear in its belief that the

---

[28] Inspector General Report, *supra* note 8, at 66.

[29] Government Accountability Office, GAO-05-356, *Aviation Security: Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed* 31 (March 2005) (hereinafter "GAO Report").

[30] Inspector General Report, *supra* note 8, at 115-128.

[31] OMB Guidelines at 28964.

government should not collect and store data without a specific, limited purpose. The "relevant and necessary" provision

> reaffirms the basic principles of good management and public administration by assuring that the kinds of information about people which an agency seeks to gather or solicit and the criteria in programs for investigating people are judged by an official at the highest level to be relevant to the needs of the agency as dictated by statutes . . . . This section is designed to assure observance of basic principles of privacy and due process by requiring that where an agency delves into an area of personal privacy in the course of meeting government's needs, its actions may not be arbitrary[.][32]

As OMB declared in its Privacy Act guidelines, "[t]he authority to maintain a system of records does not give the agency the authority to maintain any information which it deems useful."[33] The Privacy Act's "relevant and necessary" provision thus seeks to protect individuals from overzealous, arbitrary and unnecessary data collection. It embodies the common sense principle that government data collection is likely to spiral out of control unless it is limited to only that information which is likely to advance the government's stated (and legally authorized) objective. Like the FBI's other deviations from customary Privacy Act requirements, the "relevant and necessary" exemption will serve only to increase the likelihood that the TSRS will become an error-filled, invasive repository of all sorts of information bearing no relationship to terrorist screening. The Bureau should be particularly sensitive to this issue because the maintenance of information that is neither relevant nor necessary to achieve the TSC's stated goals encourages "mission creep" — the tendency of government agencies to expand the use of personal information beyond the purpose for which it was initially collected. It is crucial

[32] S. Rep. No. 93-3418, at 47 (1974).

[33] OMB Guidelines at 28960.

that the FBI strictly limit the use of collected information to the Terrorist Screening Center's core mission.

B. The TSRS Fails to Provide Meaningful Citizen Access to Personal Information and Correction of Inaccurate Data

In its notice, the FBI has exempted the TSRS from important Privacy Act provisions guaranteeing citizens the right to access records containing information about them. The Privacy Act provides, among other things, that an individual may request access to records an agency maintains about him or her.[34] In lieu of the statutory, judicially enforceable right of access provided by the Act, the Bureau instead states that requests for access to non-exempt records may be mailed to the Record Information Dissemination Office.[35] No timelines are specified for the procedure, and the process is left entirely to the agency's discretion. The FBI's weak access provisions are in direct conflict with the purposes of the Privacy Act, which sought to provide citizens with an enforceable right of access to personal information maintained by government agencies.

Companion and complementary to the right to access information is the right to correct it. Unfortunately, the FBI's notice establishes a system that also fails to provide the ability to amend or correct inaccurate, irrelevant, untimely and incomplete records. The agency has exempted the TSRS from the Privacy Act requirements that define the government's obligation to allow citizens to challenge the accuracy of information contained in their records, such as an agency's obligation to correct identified

[34] 5 U.S.C. § 552a(d)(1). Individuals generally have the right to seek judicial review to enforce the statutory right of access provided by the Act under 5 U.S.C. § 552a(g), but the FBI has exempted the TSRS from this provision, as well.

[35] 70 Fed. Reg. 43717.

inaccuracies promptly, and the requirement that an agency make notes of requested amendments within the records.[36]

The rights of access and correction were central to what Congress sought to achieve through the Privacy Act:

> The committee believes that this provision is essential to achieve an important objective of the legislation: Ensuring that individuals know what Federal records are maintained about them and have the opportunity to correct those records. The provision should also encourage fulfillment of another important objective: maintaining government records about individuals with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to individuals in making determinations about them.[37]

Instead of the judicially enforceable right to correction set forth in the Privacy Act,[38] the FBI has established its own discretionary procedure for individuals to contest the accuracy of their records.[39] The FBI's Federal Register notices explain the agency has the discretion to correct erroneous information upon an individual's request, but the agency has no obligation to do so. This correction process offers a token nod to the principles embodied in the Privacy Act, but does not provide a meaningful avenue to pursue correction and is subject to change at the FBI's whim.

Disturbingly, the Bureau's notice goes on to disclaim responsibility for handling complaints from individuals who have screening difficulty believed to be due to inaccurate information maintained by the TSC:

---

[36] 5 U.S.C. § 552a(d)(4).

[37] H.R. Rep. No. 93-1416, at 15 (1974).

[38] 5 U.S.C. § 552a(g)(1).

[39] 70 Fed. Reg. 43717.

> If individuals . . . are experiencing repeated delays or difficulties during a government screening process and believe that this might be related to terrorist watch list information, they may contact the Federal agency that is conducting the screening process in question. . . . The TSC assists the screening agency in resolving any screening complaints that may relate to terrorist watch list information, but does not receive or respond to individual complaints directly.[40]

In addition, the TSC previously made clear that it has no intention of establishing an ombudsman's office to address redress issues, explaining "[t]he ombudsman function will be at the nominating agency level."[41]

There will, therefore, be no recourse available to individuals misidentified as watch list matches, given that agencies using the database (such as the Transportation Security Administration) have also failed to establish effective redress processes for citizens adversely affected by watch list screening procedures. According to a report from the GAO, "TSA has not yet clearly defined how it plans to implement its redress process for Secure Flight, such as how errors, if identified, will be corrected[.]"[42] Furthermore, according to the GAO,

> TSA does not control the content of the terrorist screening database that it intends to use as the primary input in making screening decisions, and will have to reach a detailed agreement with the TSC outlining a process for correcting erroneous information in the terrorist screening database. Until TSA and TSC reach an agreement, it will remain difficult to determine whether redress under Secure Flight will be an improvement over the process currently used or if it will provide passengers with a reasonable opportunity to challenge and correct erroneous information contained in the system.[43]

---

[40] 70 Fed. Reg. 43718.

[41] Inspector General Report, *supra* note 8, app. IV at 97.

[42] GAO Report, *supra* note 29, at 7.

[43] *Id*. at 58.

It is not clear whether the problems identified by the GAO have been solved. The TSRS should not be used to make determinations about individuals until redress concerns are thoroughly addressed and resolved, both by the TSC and by agencies that use TSRS information for screening purposes.

Finally, the Bureau exempts the TSRS from the Privacy Act provision allowing individuals to bring civil actions against the agency if it fails to observe Privacy Act requirements,[44] underscoring the fact that there is no right to judicial review of the FBI's determinations. The agency presents no explanation why judicially enforceable Privacy Act correction procedures would be inappropriate in the context of the TSRS. Denying citizens the right to ensure that the system contains accurate, relevant, timely and complete records will increase the probability that the consolidated watch list will be an error-prone, ineffective means of singling out individuals as they seek to exercise a variety of rights and privileges.

C. The Broad "Routine Uses" of the Terrorist Screening Records System Will Exacerbate the System's Privacy Problems

The Bureau's notice identifies eleven categories of "routine uses" of personal information that will be collected and maintained in the TSRS, and allows for an additional ten "blanket routine uses" that apply to this and a number of other FBI systems of records.[45] While some of these categories are clearly related to law enforcement and intelligence efforts to combat terrorism, others are so broad as to permit the FBI to disclose TSRS information to virtually anyone at the agency's sole discretion. In

[44] 5 U.S.C. § 552a(g).

[45] 70 Fed. Reg. 43716-43717; Privacy Act of 1974; System of Records Notice, 66 Fed. Reg. 33558, 33559-33560 (June 22, 2001).

addition to law enforcement entities, the FBI anticipates that, under certain circumstances, it may disclose TSRS information to, among others:

- "owners/operators of critical infrastructure and their agents, contractors or representatives";[46]
- professional licensure authorities;[47]
- "the news media or members of the general public in furtherance of a legitimate law enforcement or public safety function as determined by the FBI;"[48]
- former DOJ employees;[49] and
- "any person or entity in either the public or private sector, domestic or foreign, where reasonably necessary to elicit information or cooperation from the recipient for use by the TSC[.]"[50]

Taken together, the 21 categories of "routine uses" are so broadly drawn as to be almost meaningless, allowing for potential disclosure to virtually any individual, company, or government agency worldwide for a vast array of purposes.

These "routine" disclosures are particularly alarming because, as we have shown, the information to be disclosed may well include material that is inaccurate, irrelevant and unnecessary to any legitimate counterterrorism purpose, and the information will not be subject to a meaningful redress process even if it forms the basis for negative determinations about affected individuals. The broad dissemination of TSRS information

[46] 70 Fed. Reg. 43716.

[47] 70 Fed. Reg. 43717.

[48] 66 Fed. Reg. 33559.

[49] 66 Fed. Reg. 33560.

[50] 70 Fed. Reg. 43717.

that the Bureau anticipates underscores the need for full transparency (and resulting public oversight), as well as judicially enforceable rights of access and correction.

Conclusion

For the foregoing reasons, EPIC believes that the FBI must revise its Privacy Act notice for the TSRS system to 1) provide individuals enforceable rights of access and correction; 2) ensure the accuracy, timeliness, and completeness of information, as well as limit the collection of information to only that which is necessary and relevant; and 3) substantially limit the routine uses of collected information. Further, development of the system should be suspended until the Bureau is willing to fully disclose relevant information about the program to the public, and the agency subsequently solicits informed public comment on the privacy implications of this database.

Respectfully submitted,

David L. Sobel
General Counsel

Marcia Hofmann
Staff Counsel

ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, DC 20009
(202) 483-1140