DEPARTMENT OF HOMELAND SECURITY
Privacy Office

Docket No. DHS-2005-0029
Notice of proposed rulemaking:
Privacy Act of 1974: Implementation of Exemptions:
The Homeland Security Operations Center Database

COMMENTS OF:

AMERICAN-ARAB ANTI-DISCRIMINATION COMMITTEE
AMERICAN ASSOCIATION OF LAW LIBRARIES
AMERICAN CIVIL LIBERTIES UNION
AMERICAN LIBRARY ASSOCIATION
ASIAN AMERICAN LEGAL DEFENSE AND EDUCATION FUND
ASSOCIATION OF AMERICAN PHYSICIANS AND SURGEONS
ASSOCIATION OF CORPORATE TRAVEL EXECUTIVES
ASSOCIATION OF RESEARCH LIBRARIES
CENTER FOR DEMOCRACY AND TECHNOLOGY
BILL OF RIGHTS DEFENSE COMMITTEE
CENTER FOR FINANCIAL PRIVACY AND HUMAN RIGHTS
CENTER FOR NATIONAL SECURITY STUDIES
COMPUTER PROFESSIONALS FOR SOCIAL RESPONSIBILITY
CONSUMER ACTION
COUNCIL ON AMERICAN-ISLAMIC RELATIONS
CYBER PRIVACY PROJECT
ELECTRONIC FRONTIER FOUNDATION
ELECTRONIC PRIVACY INFORMATION CENTER
FAIRFAX COUNTY PRIVACY COUNCIL
FRIENDS COMMITTEE ON NATIONAL LEGISLATION
GOVERNMENT ACCOUNTABILITY PROJECT
JAPANESE AMERICAN CITIZENS LEAGUE
JUNKBUSTERS
THE MULTIRACIAL ACTIVIST
NATIONAL ASIAN PACIFIC AMERICAN LEGAL CONSORTIUM
NATIONAL ASSOCIATION FOR THE ADVANCEMENT OF COLORED
PEOPLE WASHINGTON BUREAU
NATIONAL CONSUMERS LEAGUE
NATIONAL COUNCIL OF LA RAZA
NATIONAL IMMIGRATION LAW CENTER
PEOPLE FOR THE AMERICAN WAY
PRIVACYACTIVISM
PRIVACY JOURNAL
PRIVACY RIGHTS CLEARINGHOUSE
PRIVACY RIGHTS NOW
PRIVACY TIMES
THE RUTHERFORD INSTITUTE
SPECIAL LIBRARY ASSOCIATION
U.S. BILL OF RIGHTS FOUNDATION
U.S. BILL OF RIGHTS INSTITUTE
WORLD ORGANIZATION FOR HUMAN RIGHTS USA
WORLD PRIVACY FORUM

By notice published on April 18, 2005, the Department of Homeland Security ("DHS") proposes to add a system of records, the Homeland Security Operations Center Database ("HSOCD"), to its inventory of record systems,[1] DHS also seeks to exempt portions of this new system from one or more provisions of the Privacy Act of 1974.[2]

According to DHS, the HSOCD will be maintained in the Information and Analysis Infrastructure Protection Directorate.[3] The HSOCD "is being established to serve as the primary national-level hub for operational communications and information pertaining to domestic incident management … [and] will support a single, centralized repository for gathered information."[4] The vast new system of records will include domestic and foreign intelligence data, as well as information about the providers of the data.[5]

Pursuant to the DHS Privacy Act notices proposing a new system of records and exempting the new system from certain Privacy Act provisions, [the organizations below] submits these comments to address the substantial privacy issues raised by the database and to request that DHS substantially narrow the Privacy Act exemptions in the notice prior to the creation of this new system of records.

---

[1] Notice of proposed rulemaking, 70 Fed. Reg. 20061 (proposed Apr. 18, 2005), available at http://a257.g.akamaitech.net/7/257/2422/01jan20051800/edocket.access.gpo.gov/2005/05-7705.htm.

[2] Notice of Privacy Act systems of records, 70 Fed. Reg. 20156 (proposed Apr. 18, 2005), available at http://a257.g.akamaitech.net/7/257/2422/01jan20051800/edocket.access.gpo.gov/2005/05-7704.htm.

[3] 70 Fed. Reg. at 20062.

[4] *Id*. at 200061.

[5] *Id*. at 20157, 20062.

Introduction

When it enacted the Privacy Act, 5 U.S.C. § 552a, in 1974, Congress sought to restrict the amount of personal information that federal agencies could collect and required agencies to be transparent in their information practices.[6] The Supreme Court just last year underscored the importance of the Privacy Act's restrictions upon agency use of personal information to protect privacy interests, noting that:

> "[I]n order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary . . . to regulate the collection, maintenance, use, and dissemination of information by such agencies." Privacy Act of 1974, §2(a)(5), 88 Stat. 1896. The Act gives agencies detailed instructions for managing their records and provides for various sorts of civil relief to individuals aggrieved by failures on the Government's part to comply with the requirements.[7]

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[.]"[8] It is also intended to guard the privacy interests of citizens and lawful permanent residents 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."[9] 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.[10]

Adherence to these requirements is critical for a system like the HSOCD, a massive

---

[6] S. Rep. No. 93-1183 at 1 (1974).
[7] *Doe v. Chao*, 540 U.S. 614, 618 (2004).
[8] S. Rep. No. 93-1183 at 1.
[9] Pub. L. No. 93-579 (1974).
[10] *Id.*

centralized repository of information that would include:

> intelligence information and other information received from agencies and components of the federal government, foreign governments, organizations or entities, international organizations, state and local government agencies (including law enforcement agencies), and private sector entities, as well as information provided by individuals, regardless of the medium used to submit the information or the agency to which it was submitted. This system also contains: information regarding persons on watch lists with possible links to terrorism; the results of intelligence analysis and reporting; ongoing law enforcement investigative information, information systems security analysis and reporting; historical law enforcement information, operational and administrative records; financial information; and public-source data such as that contained in media reports and commercial databases as appropriate to identify and assess the nature and scope of terrorist threats to the homeland, detect and identify threats of terrorism against the United States, and understand such threats in light of actual and potential vulnerabilities of the homeland. Data about the providers of information, including the means of transmission of the data is also retained.[11]

Significantly, DHS states that individuals whose information will be contained in the system include American citizens who assist in homeland security investigations, and former or current employees of DHS administrative or homeland security operations.[12] As DHS notes in its Privacy Act Notice, the law "embodies fair information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses and disseminates personally identifiable information."[13] Unfortunately, DHS has exempted the HSOCD from key fair information principles such as the requirements that an individual be permitted access to personal information, that an individual be permitted to correct and amend personal information, and that an agency

[11] 70 Fed. Reg. at 20062.
[12] *Id*. at 20157.
[13] *Id*. at 20061.

assure the reliability of personal information for its intended use.[14] It is clear that this sweeping new system of records is precisely the type of database that requires application of these principles as embodied in the Privacy Act.

I. The Homeland Security Operations Center Database's Broad Exemptions Contravene the Intent of the Privacy Act

As an initial matter, we note that DHS has invoked 5 U.S.C. §§ 552a(j)(2), (k)(1) and (k)(2) as authority for its exemption of specific Privacy Act requirements. These broad exemptions would allow DHS to track and profile individuals, including those who seek to aid investigations, with little accountability.

The Department of Homeland Security claims subsection (j)(2) exemptions from 5 U.S.C. §§ 552a(e)(8) and (g). Subsection (e)(8) mandates that the agency "make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record."[15] If the process is a "matter of public record," it is unknown what value would be gained by exempting the agency from its Privacy Act obligation to make reasonable efforts to serve notice on an affected individual. This broad exception only serves to increase the secrecy of the new database.

Subsection (g) specifies the civil remedies that an individual has against an agency for failure to comply with its obligations under the Privacy Act. Exempting the new database from subsection (g) of the Privacy Act means that individuals will have no judicially enforceable rights of access to their records or correction of erroneous information in such records. However, providing individuals with the right to judicial review is crucial because the new database will have information not only about suspected

---

[14] *See* U.S. Dep't of Health, Education and Welfare, *Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and Rights of Citizens* viii (1973).

[15] 5 U.S.C. § 552(a)(e)(8).

criminals, but also about people who offer information about terrorism, as well as current and former DHS employees and contractors. [16] Though section (j) requires an agency to provide the "reasons why the system of records is to be exempted from a provision of this section," DHS does not explain why it has exempted HSOCD from these Privacy Act requirements.

A clear, timely, judicially enforceable redress procedure is vital here because there will be mistakes or confusion about the data in the HSOCD that will affect innocent Americans. DHS's redress procedures largely have been inadequate. For example, TSA maintains that it has an adequate redress process to clear individuals improperly flagged by watch lists; however, it is well known that individuals encounter difficulty in resolving such problems. Senators Ted Kennedy (D-MA) and Don Young (R-AK) are among the individuals who have been improperly flagged by watch lists.[17] Sen. Kennedy was able to resolve the situation only by enlisting the help of then-Homeland Security Secretary Tom Ridge; unfortunately, most people do not have that option.

In March, Rep. Loretta Sanchez (D-CA) expressed dismay to TSA officials that current TSA safeguards had failed her constituents. At a House subcommittee hearing on March 2, 2005, Rep. Sanchez reported that many of her constituents continue to face lengthy delays, questioning, and at times are prohibited from boarding flights because they are misidentified as people sought on no-fly lists. Her constituents continue to face these roadblocks even after they apply for, receive and then display to screener personnel

---

[16] 70 Fed. Reg. at 20157.

[17] *See, e.g.,* Sara Kehaulani Goo, *Committee Chairman Runs Into Watch-List Problem*, Washington Post, Sept. 30, 3004; Leslie Miller, *House Transportation Panel Chairman Latest to be Stuck on No-Fly List*, Associated Press, Sept. 29, 2004; Shaun Waterman, *Senator Gets a Taste of No-Fly List Problems*, United Press International, Aug. 20, 2004.

the official federal government letters that establish their innocence. Rep. Sanchez questioned why current redress procedures have failed these American citizens.[18] These problems provide further reasons for individuals to refrain from providing data on crimes to DHS, as they would then be targeted by the proposed database, but then be unable to access or correct personal information gathered in the HSOCD.

DHS also cites subsections (k)(1) and (k)(2) in support of these exemptions. However, subsection (k)(1) is applicable only where the system of records is "subject to the provisions of section 552(b)(1) of this section," *i.e.*, if the system contains classified information. While DHS has designated the "Security Classification" of the system of records as "[c]lassified, sensitive," it is obvious that not *all* information in the system of records warrants (or is entitled to) such classification.[19] For instance, "public source data such as that contained in media reports and commercial databases"[20] clearly is not subject to government classification. It is, in fact, improper to conceal unclassified data by mixing it with classified data. Therefore, it is not clear that DHS has properly invoked subsection (k)(1) to exempt the information in this system from crucial Privacy Act protections.

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 DHS seeks to exempt the HSOCD system of records from the Privacy Act's access provisions, as we discuss below, it is unclear whether subsection (k)(2) authorizes DHS's action. As such, we urge DHS to explain how (k)(1) and (k)(2) give the agency authority to

---

[18] Shaun Waterman, *No Redress Mechanism in New DHS Terrorist Screening Office,* United Press International, Mar. 2, 2005.
[19] 70 Fed. Reg. at 20157.
[20] *Id.*

exempt the system of records from the various Privacy Act provisions it cites.

II. The Homeland Security Operations Center Database Fails to Provide Meaningful Citizen Access to Personal Information

In its notice, DHS has exempted the HSOCD from all 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;[21]
- an individual may seek judicial review to enforce the statutory right of access provided by the Act,[22] and
- the agency must publish a notice of the existence of records in the Federal Register, along with the procedures to be followed to obtain access.[23]

In lieu of the statutory, judicially enforceable right of access provided by the Act, DHS provides no redress process whatsoever for individuals who wish to access the information maintained about them in the HSOCD. This complete lack of due process directly conflicts with the purposes of the Privacy Act, which intended to provide citizens with an enforceable right of access to personal information maintained by government agencies. As DHS Privacy Officer Nuala O'Connor Kelly testified before Congress in February 2004, "Issues of privacy and civil liberties are most successfully navigated when the necessary legal, policy, and technological protections are built in to the systems or programs from the very beginning."[24] The HSOCD lacks any such protective framework.

---

[21] 5 U.S.C. § 552a(d)(1).
[22] 5 U.S.C. § 552a(g)(1).
[23] 5 U.S.C. §§ 552a(e)(4)(G), (e)(4)(H), (f).
[24] Statement of Chief Privacy Officer Nuala O'Connor Kelly Before the House of Representatives Judiciary Subcommittee on Commercial and Administrative Law (Feb. 10, 2004) *at* http://www.dhs.gov/dhspublic/interapp/testimony/testimony_0024.xml (last accessed May 17, 2005).

III. The Homeland Security Operations Center Database Fails to Provide Opportunities to Correct Inaccurate, Irrelevant, Untimely and Incomplete Information

Companion and complementary to the right to access information is the right to correct it. DHS's notice establishes a system that provides neither adequate access nor the ability to amend or correct inaccurate, irrelevant, untimely and incomplete records. The agency has exempted[25] the HSOCD 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 must correct identified inaccuracies promptly;[26]
- an agency must make notes of requested amendments within the records;[27] and
- an agency must establish procedures to handle disputes between the agency and individual as to the accuracy of the records.[28]

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.[29]

Instead of the judicially enforceable right to correction set forth in the Privacy Act,[30] DHS has provided no method for an individual to ensure that information about him maintained by the agency is correct, timely, and complete. Furthermore, there would be no right to judicial review of DHS's determinations. The agency presents no explanation why

---

[25] 70 Fed. Reg. at 20062.
[26] 5 U.S.C. § 552a(d)(2)(B), (d)(3).
[27] 5 U.S.C. § 552a(d)(4).
[28] 5 U.S.C. § 552a(f)(4).
[29] H.R. Rep. No. 93-1416, at 15 (1974).
[30] 5 U.S.C. § 552a(g)(1).

judicially enforceable Privacy Act correction procedures would be inappropriate in the context of HSOCD. Denying citizens the right to ensure that the system contains only accurate, relevant, timely and complete records will increase the probability that the HSOCD will be an error-prone, ineffective means of ensuring homeland security. DHS's failure to provide the public a Privacy Act-compliant correction and redress procedure is unjustified and unacceptable. The agency should not collect any information about individuals until it can articulate an appeals process to the public that complies with the requirements of the Privacy Act.

IV. The Homeland Security Operations Center Database Fails to Assure Collection of Information Only for "Relevant and Necessary" Use

DHS has also exempted the HSOCD from the fundamental Privacy Act requirement 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.[31] DHS states that "[i]n the interests of Homeland Security, it is appropriate to include a broad range of information that may aid in identifying and assessing the nature and scope of terrorist or other threats to the Homeland."[32] However, the threat of terrorism is not a blank check to gather any and all information on individuals who are not suspected of criminal activity, but merely either provide information to DHS concerning possible crimes, or who are current or former employees of DHS's administrative or homeland security operations. The agency's argument that what is "relevant and necessary" is unknown until the investigation is complete could be used in any investigative context. This broad, unsustainable rationale swallows the entire "relevant and necessary" requirement.

In adopting the Privacy Act, Congress was clear in its belief that the government should not collect and store data without a specific, limited purpose. The "relevant and necessary" provision

[31] 5 U.S.C. § 552a(e)(1).
[32] 70 Fed. Reg. at 20062.

> 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[.][33]

As OMB noted 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."[34] 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.

Such open-ended, haphazard data collection plainly contradicts the objectives of the Privacy Act and raises serious questions concerning the likely impact of the HSOCD on innocent Americans. By claiming these exemptions for the new database, the agency gains virtually unlimited discretion to track and profile American citizens, including those who assist in homeland security investigations, without any accountability.

V. The Homeland Security Operations Center Database Presents a High Risk of Misuse or Abuse of Database Information

The Government Accountability Office has stated in congressional testimony that "[t]o the extent that personal information is aggregated in public and private sector databases, it becomes vulnerable to misuse."[35] A recent scandal in Florida highlights the need for strong privacy protections and clear regulations governing databases such as the

---

[33] S. Rep. No. 93-3418 at 47 (1974).
[34] Office of Management and Budget, Privacy Act Implementation: Guidelines and Responsibilities, 40 Fed. Reg. 28948, 28960 (July 9, 1975).
[35] General Accounting Office, *Social Security Numbers: Ensuring the Integrity of the SSN, Statement of Barbara D. Bovbjerg, Director, Education, Workforce, and Income Security Issues*, GAO-03-941T at 12 (July 10, 2003).

HSOCD. In March, a woman who wrote to a newspaper criticizing a Florida sheriff as being too fat for police work and his agency's use of stun guns.[36] Orange County Sheriff Kevin Beary ordered staffers to use state driver's license records to find the home address of his critic.[37] Though state driver's license records have been restricted from personal use since 2000 by the federal Driver Privacy Protection Act,[38] a Florida Department of Law Enforcement investigation found there was "no clear violation of the statutes and rules governing" the incident.[39] However, this conclusion was reached partly because Florida state law does not define what types of use of restricted databases would not have a law-enforcement purpose, so "such use is generally left to the discretion of law enforcement officials."[40]

This Florida incident demonstrates that individuals can misuse the information maintained in restricted databases. The Privacy Act exemptions claimed by DHS increase the risk of questionable use of the information maintained in the HSOCD. Therefore, it is imperative for DHS to create and operate the new database in compliance with the requirements of the Privacy Act to ensure adequate security, privacy and redress.

VI. DHS Should Observe Constitutional Rights and International Standards for the Collection and Use of Personal Information for All Individuals

While the Privacy Act does not require DHS to apply the statute's provision to those who are not US citizens or lawful residents, we urge DHS to consider the application of fundamental constitutional privacy standards as recognized in the U.S.

---

[36] Staff writer, *Called fat, sheriff tracks down reader*, Associated Press, Apr. 6, 2005.
[37] *Id*.
[38] 18 U.S.C. §§ 2721 - 2725 (1994).
[39] Letter from Guy M. Tunnell, Commissioner, Florida Department of Law Enforcement, to Kevin Beary, Sheriff, Orange County (Apr. 28, 2005).
[40] *Id*.

Constitution as well as international privacy standards agreed to by the United States.

The United States is a signatory of the Universal Declaration of Human Rights,[41] the Organization for Economic Cooperation and Development ("OECD") Privacy Guidelines of 1980,[42] and the United Nations Guidelines for the Regulation of Computerized Personal Files of 1990.[43] Recently, the Government Accountability Office used the OCED Privacy Guidelines in its review of the Secure Flight travel program.[44] The GAO used the eight Fair Information Practices set out in the OCED guidelines: collection limitation, purpose specification, use limitation, data quality, security

---

[41] The Universal Declaration of Human Rights provides that no individual "shall be subjected to arbitrary interference with his privacy," and that "[e]veryone has the right to protection of the law against such interference or attacks." United Nations, Universal Declaration of Human Rights, G.A. Res. 217A(III), U.N. GAOR, 3d Sess., U.N. Doc. A/810 (1948), art. 12, reprinted in M. ROTENBERG ED., THE PRIVACY LAW SOURCEBOOK 2003 318 (EPIC 2003) (hereinafter "PRIVACY LAW SOURCEBOOK"). Furthermore, "no distinction shall be made on the basis of the political, jurisdictional, or *international* status of the country or territory to which a person belongs." *Id.* (emphasis added).

[42] The OECD Privacy Guidelines of 1980 apply to "personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties." Organization for Economic Cooperation and Development, Guidelines Governing the Protection of Privacy and Trans-Border Flow of Personal Data, OECD Doc. 58 final (Sept. 23, 1980), art. 3(a), reprinted in PRIVACY LAW SOURCEBOOK at 330. The OECD Privacy Guidelines require, among other things, that there should be limitations on the collection of information; collection should be relevant to the purpose for which it is collected; there should be a policy of openness about the information's existence, nature, collection, maintenance and use; and individuals should have rights to access, amend, complete, or erase information as appropriate. *Id.*

[43] The United Nations Guidelines for the Regulation of Computerized Personal Files of 1990 recognize many of the same rights in information as the OECD Privacy Guidelines provide, providing in addition that "data likely to give rise to unlawful or arbitrary discrimination, including information on racial or ethnic origin, colour, sex life, political opinions, philosophical and other beliefs . . . should not be compiled." United Nations, G.A. Res. 45/95, Guidelines for the Regulation of Computerized Personal Files (Dec. 14, 1999) prin. 5, reprinted in PRIVACY LAW SOURCEBOOK at 368.

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

safeguards, openness, individual participation, and accountability," and stated that these Fair Information Practices are "a set of internationally recognized privacy principles that underlie the Privacy Act."[45] The United States' collection and use of personal information of individuals in the HSOCD violates these guidelines, as well as the EU Data Protection Directive,[46] and suggests a disregard for international privacy laws and human rights standards.

Conclusion

For the foregoing reasons, the undersigned organizations believe that DHS must revise its Privacy Act notice for the Homeland Security Operations Center Database system to 1) provide individuals judicially enforceable rights of access and correction; 2) limit the collection of information to only that which is necessary and relevant; and 3) respect individuals' rights to their information that is collected and maintained by the agency.

Respectfully submitted,

American-Arab Anti-Discrimination Committee
American Association of Law Libraries
American Civil Liberties Union
American Library Association
Asian American Legal Defense and Education Fund
Association of American Physicians and Surgeons
Association of Corporate Travel Executives
Association of Research Libraries
Center for Democracy and Technology
Bill of Rights Defense Committee
Center for Financial Privacy and Human Rights

[45] GAO Report at 55.

[46] The European Union Data Protection Directive recognizes a right to privacy in personal information and establishes protections for information collected from all individuals, regardless of nationality.[46] Like both sets of Guidelines, the EU Directive recognizes an individual's right to access information and requires that information be kept accurate and timely. Parliament and Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, reprinted in PRIVACY LAW SOURCEBOOK at 384.

Center for National Security Studies
Computer Professionals for Social Responsibility
Consumer Action
Council on American-Islamic Relations
Cyber Privacy Project
Electronic Frontier Foundation
Electronic Privacy Information Center
Fairfax County Privacy Council
Friends Committee on National Legislation
Government Accountability Project
Japanese American Citizens League
Junkbusters
The Multiracial Activist
National Asian Pacific American Legal Consortium
National Association for the Advancement of
Colored People Washington Bureau
National Consumers League
National Council of La Raza
National Immigration Law Center
People For the American Way
PrivacyActivism
Privacy Journal
Privacy Rights Clearinghouse
Privacy Rights Now
Privacy Times
The Rutherford Institute
Special Library Association
U.S. Bill of Rights Foundation
U.S. Bill of Rights Institute
World Organization for Human Rights USA
World Privacy Forum