Privacilla.org

Your Source for Privacy Policy from a Free-market, Pro-technology Perspective

September 30, 2003

Privacy Office
U.S. Department of Homeland Security
Washington, D.C. 20528

Re: **DHS/TSA-2003-1**
Comments of Privacilla.org on "Notice of Status of System of Records; Interim Final Notice; Request for Further Comments"
68 Fed. Reg. 45,265 (August 1, 2003)

To Whom It May Concern:

Privacilla.org is pleased to offer comments on the revised Privacy Act notice for the CAPPS II system. The new notice exhibits substantial improvements over the previous one. Unfortunately, the CAPPS II program continues to have substantial flaws that needlessly degrade the privacy of American travelers. A variety of important non-privacy concerns persist as well.

Below, we will assess each of the major criticisms Privacilla raised in previous comments (attached), and the changes made in the new notice. Our analysis goes only to actual privacy concerns. We touch on, but do not thoroughly analyze, other important interests such as constitutional due process. We do not attempt to gauge whether the CAPPS II system appropriately balances the multiple competing interests, including privacy, civil rights, cost, convenience, and effectiveness.

The Database will Record the Movements of Every Traveler

In our previous comments, we objected to the fact that the system of records would cover all "[i]ndividuals traveling to, from, or within the United States (U.S.) by passenger air transportation." We focused especially on the collection of "associated data," a clause indicating no limit on what data might be collected.

The new Privacy Act notice continues to contemplate collection of information about all air travelers in the United States. To the Department's credit, the term "associated data" has been deleted.

The Department is still apparently considering the length of time that records will be kept. If at all, records should only be kept as long as they are absolutely necessary for security purposes. Given the likelihood of mission creep, "a set number of days" is not reassuring.

The addition of airline "Passenger Name Records" to the system of records also adds new uncertainty. Incorporating entire PNRs creates needless over-breadth to the categories of records in the system, depending on how airlines conduct business. When an airline includes a great deal of personal information in its PNRs, the privacy of American travelers will needlessly be reduced by incorporating them into the CAPPS II database. Consumers may appropriately press airlines to restructure their PNRs in the interest of privacy from government, creating needless distortions in the business practices of airlines.

If the system continues to collect information about every traveler — and, as discussed below, it should not — PNRs should not be included in their entirety. The system should be designed to collect only such data from PNRs as is essential to perform security functions.

Moving from the overbroad "associated data" to PNRs is an improvement, though further improvements can be made without sacrificing security.

Information Can be Disclosed to Nearly All Comers

As we noted in our previous comments, the Department previously promised essentially no confidentiality for information in the proposed system of records. A plethora of "routine uses" granted the Department nearly unlimited authority to disclose information. We are gratified to see that the routine uses have been curtailed

As we noted previously, commercial promises of confidentiality are enforceable, while government promises of confidentiality can be made and unmade at will — or at whim. To provide the American people the fullest disclosure, the Privacy Act notice should declare that its terms are revocable at any time by issuance of an additional *Federal Register* notice.

One contemplated disclosure is needlessly lax on privacy. The preamble to the notice describes how information will be transferred to commercial data providers who will return a score "indicating a confidence level in that passenger's identity." Though several safeguards have obviously been contemplated, privacy protection dictates that

such contractors should immediately destroy the data they receive once they have returned a confidence score. Contractors should be bound to this ultimate safeguard, suffering substantial penalties including disqualification from further contract eligibility if they do not.

While this rule would dispose of many *privacy* concerns with transfer of information to private sector contractors, substantial *due process* concerns would remain. Perhaps identifying this as a 'privacy' issue, other commenters may argue that private data can not be used in government decision-making without granting citizens due process rights such as access and correction. This is true. Delegation of government power to a private-sector entity does not and should not dispose of the constitutional and statutory rights against government that apply.

On the broadest level, this illustrates the folly of the federal policy creating a special government security function for the private transportation industry. Were the responsibility for security properly placed in the hands of the industry itself, airlines could use personal data as fully or as restrictively as consumers wished, restrained from extremes on either side by public demand for both privacy and security.

There are multiple complex problems involved if private data is to be used in government decision-making. Commercial data providers would be wise to avoid this market if they wish to avoid public-utility-style regulation of their functions, or public ownership of their data.

Anyone Can be Deemed a Suspect

The Department's previous Privacy Act notice suggested no limits on who could decide that an American traveler posed a "possible risk" to air safety. This was a warrant for unlimited data collection and retention, and a clear and direct threat to privacy. It is gratifying to see it removed.

A new and different threat exists in the currently envisioned program, however. The preamble discusses a "risk assessment function" to follow the passenger authentication process. Murkily, the notice says this will be conducted "internally within the U.S. government," making reference to "[n]ational security information."

This may be intended to describe only comparison between travelers and valid, well-scrubbed terrorism watch lists. But the broad language leaves room for comparison of traveler information to personal data held by the Internal Revenue Service, the Social

Security Administration, the Medicare system, the Department of Education, and dozens of other departments, agencies, and bureaus.

There are hundreds, if not thousands, of databases of personal information ensconced throughout the U.S. government. Using tax records, Social Security records, welfare records, education records, health records,[1] public service records, military records, and so on, the U.S. government has by far the greatest capacity of any entity to profile citizens and learn detailed information about all facets of their lives. If CAPPS II will use data from a variety of agencies, this "internal" risk assessment function may still be extremely intrusive — a new Total Information Awareness program.

This potential is not actually a new privacy problem because it requires no new collection of data. Rather, it illustrates the cost in privacy that Americans have already paid for living in a welfare state with an individual income tax that requires highly detailed personal information to administer.

Two other non-privacy issues present themselves, clustered around the question of who will be specially deemed suspects in the proposed system.

First, the plan to review travelers for outstanding arrest warrants is a blatant and regrettable example of mission creep. It converts this airline security program into an internal passport system harkening to the worst regimes of the past century. Only clearly identified threats to air safety should be identified by the system. In limited cases, outstanding warrants may indicate a threat to air safety. In the vast majority of cases, they do not.

Second, the maintenance of data on government officials, holders of security clearances, and people in positions of trust or confidence appears to be for the purpose of exempting certain people from screening. This is as elitist as it is foolish. Reports of espionage by military personnel at Guantanamo have been reported in just the last weeks, illustrating that officialdom is not immune from infiltration by enemies of freedom. Just as importantly, in our society government officials stand in line like everybody else. Government personnel should suffer every delay, needed or needless, that the general public suffers in the name of transportation security.

The concerns expressed here go to privacy already lost to big government and to non-privacy values like constitutional due process and equality. The previous notice

[1] The preamble disclaims use of health data but the notice itself does not.

allowed additional information collection about people "deemed" risks to air safety under standardless procedures. The elimination of these provisions is a significant advance for privacy.

This Database Treats All American Travelers as Suspects

Alas, the current notice still, in a crucial sense, treats all American travelers as crime and terrorism suspects. The Department continues to invoke 5 U.S.C. § 552a(k) to deny notice to individuals when they are part of the database and it denies individuals access to data about themselves (though part of the 'Privacy' Act, a due process right). This section allows such denials for purposes of national defense and foreign policy, and for investigatory material compiled for law enforcement purposes. This is still a "suspects" database.

It is no cure that the Department may grant people access to records about themselves as a matter of grace or largesse. A database of all air travelers in the United States may not be shielded by law from public view using national defense and law enforcement exceptions to the Privacy Act while the Department claims that it is not treating all travelers as suspects.

Conclusion: Department Efforts to Protect Privacy are Unavailing

Privacilla recognizes and applauds the effort and improvement that went into the current Privacy Act notice. The Department's Privacy Office has demonstrated its good faith through this notice and through affirmative outreach to privacy advocates and groups. But good faith does not protect privacy. The structure of programs and explicit legal protections do.

In terms of privacy alone, this Privacy Act notice shows substantial improvement over the prior one. Substantial flaws still exist, however, and decisions yet to be made will affect both due process and privacy.

There remains only one truly appropriate way to structure a government-controlled security or law enforcement database. That is to collect information only about individuals who meet a requisite legal level of suspicion.

For non-suspects, appropriate government security measures may include *checking* information about travelers, but they do not include *collecting* information

about travelers. The next CAPPS II Privacy Act notice should be no notice at all, because no new system of records is needed. A database-free system could provide all the air safety possible using the background-check theory of security on which CAPPS II is based.

Better security, and privacy on the terms Americans desire, would be available if the responsibility for transportation security were restored to its rightful place with the airlines themselves. At a minimum, the Department should further restructure the CAPPS II program so as to be more consistent with the privacy of law-abiding American travelers.

Sincerely,

James W. Harper
Editor
Privacilla.org

Attachment

Privacilla.org

Your Source for Privacy Policy from a Free-market, Pro-technology Perspective

February 21, 2003

Department of Transportation
Documentary Services Division
Attention: Docket Section, Room PL401
Docket Number: OST-1996-1437, SVC-124
Washington, DC 20590

Re: RIN: 2105-AD23
Comments of Privacilla.org on intended "Aviation Security Screening Records"
68 Fed. Reg. 2,101 (January 15, 2003)

To Whom It May Concern:

Privacilla.org wishes to register its strong objections to the creation of a new Privacy Act system of records that will store information about all persons traveling to, from, or within the United States. America requires transportation security; that security can be provided without tracking the movements of every single air traveler.

Privacilla.org is a Web-based think-tank devoted to privacy as a public policy issue. The Privacilla Web site (http://www.privacilla.org) provides hundreds of pages of information and links about privacy law and policy from a pro-technology, free-market perspective. Privacilla periodically reports on key elements of the privacy issue that may otherwise be overlooked by policy-makers, the press, and the public.

Important though it is, privacy has never been satisfactorily defined — not even in the Privacy Act of 1974. Unsurprisingly, the Privacy Act provides insufficient protection for the privacy interests of Americans. Nonetheless, the Act provides some protection for privacy and other important public and individual interests. Disclosure of new government databases is one.

Privacy is the subjective condition that people experience when two factors are in place: First, they must have power to control information about themselves and, second, they must exercise that power consistent with their interests and values. Governments have unique authority to deprive individuals of power over information about themselves — and to use that information contrary to their interests. The individual rights that

protect Americans' privacy from government are part of what make the United States the greatest country in the world.

Congress has recently acted to protect privacy — or at least slow its erosion — in the E-Government Act of 2002[1] and the Consolidated Appropriations Resolution, 2003.[2] The latter severely restricts the Department of Defense's Total Information Awareness program, which shares characteristics with the system of records planned by the Department of Transportation. The Department should consider these laws before going forward with any database of information on all travelers.

Privacy is in constant tension with other interests, such as security against terrorism. The database proposed by the Department puts that fact in high relief. Privacilla.org has no doubt of the good intentions underlying the planned "Aviation Security Screening Records." Nonetheless, privacy is needlessly sacrificed by elements of the plan, elements that do not significantly advance transportation security.

The *Federal Register* announcement does not state the program for which this intended Privacy Act system of records is being created, and a search of the Transportation Security Administration Web site does not reveal it. But, apparently the database is a part of the Computer Assisted Passenger Pre-Screening System (CAPPS II).

The Database will Record the Movements of Every Traveler

According to the Department's *Federal Register* notice, the system will cover "[i]ndividuals traveling to, from, or within the United States (U.S.) by passenger air transportation." For all travelers, the Department will collect passengers' names and "associated data," as well as reservation and manifest information held by passenger air carriers. In other words, the movements of every traveler will be recorded.

Anyone can be subject to additional data collection. Passengers "deemed to pose a possible risk" will have recorded about them financial and transactional data, public source information, "proprietary data," and information from law enforcement and intelligence sources. As discussed further below, every air passenger poses some "possible risk" to the safety of air travel, however negligible that may be. There is no indication of who will "deem" passengers worthy of expanded data collection, nor

[1] E-Government Act of 2002, Pub. L. No. 107-347, § 208 (requiring privacy impact assessments for information technologies and collections).
[2] § 111, H.J. Res. 2, 108th Cong., 1st Sess. (2003).

whether risk assessment of passengers will be subject to standards of any kind. Every traveler may be subject to additional data collection.

In short, this database is unlimited as to whom information may be collected about or what information the Department may maintain. This is a substantial incursion on the privacy of entirely law-abiding American travelers.

Information Can be Disclosed to Nearly All Comers

In the private sector, commercial promises of confidentiality are enforceable. In the public sector, promises of confidentiality can be made and unmade by governments at will — or at whim. In its *Federal Register* notice, the Department promises no confidentiality at all.

Eleven separate "routine uses" permit release of data to Federal, State, territorial, tribal, local, international, or foreign government agencies; to contractors, grantees, experts, consultants, agents, and other non-Federal employees; to foreign, international, and domestic regulatory agencies; to individuals and organizations; to the news media; to the Department of State, immigration authorities, and the intelligence community; to courts; to airports and aircraft operators; and to the National Archives and Records Administration.

Each of these disclosures may have some purpose related to the security of air travel, or enforcement of some law, but the connection may be exceedingly remote. Disclosure of information in this database appears as likely to be related to terrorism as to discredited domestic surveillance and "data mining" programs, to divorce proceedings, to tax investigations by foreign bureaucrats, and so on.

Anyone Can be Deemed a Suspect

No standards limit who may be "deemed to pose a possible risk" to transportation security. Thus, any American — traveler or non-traveler — can be the subject of a dossier in the Department's intended database.

The Department's announcement places no limits on who may decide that an American traveler poses a "possible risk." Using the passive voice ("individuals who *are deemed* to pose a possible risk"), the Department has hidden the responsible actor or actors. Who may identify individuals as presenting a "possible risk"? It may be unidentified bureaucrats, flight attendants, other passengers, the Internal Revenue Service, anonymous callers, elected officials, and so on. The absence of limitation on

who may authorize expanded data collection and data retention about American travelers is needlessly threatening to the privacy of law-abiding Americans.

Equally unsatisfactory is the absence of standards by which American travelers and others may be deemed a possible risk. Every passenger poses some risk to the security of air travel; for most, the risk is infinitesimal. Without standards higher than "possible risk" — which is no standard at all — any American traveler may be deemed a risk and made the subject of a Department of Transportation dossier. A hunch may turn a traveler into a "possible risk," or a traveler may be identified because he or she appears angry or disheveled, because he or she is traveling without bags, because he or she has unpopular opinions, because he or she appears to be from a particular group or nation, because he or she has annoyed the wrong official, and so on without limit.

The Department's intended database can be a repository for information about anyone for any reason. This over-breadth makes it a menace to the privacy of law-abiding Americans.

This Database Treats All American Travelers as *Suspects*

There should be no mistaking that this database will treat all American travelers as crime and terrorism suspects. The Department invokes Privacy Act sections 5 U.S.C. § 552a(k)(1) and (k)(2) to deny notice to individuals when they are part of the database and to deny individuals access to data about themselves in the database. These sections allow such denial for purposes of national defense and foreign policy, and for investigatory material compiled for law enforcement purposes.

The Department may not create a database of all air travelers in the United States, shield the database from public view using national defense and law enforcement exceptions to the Privacy Act, and simultaneously claim that it is not treating all travelers as suspects. This is a "suspects" database.

Department Efforts to Protect Privacy are Unavailing

Privacilla recognizes and applauds some sensitivity to privacy reflected in the Department's plan to dispose of records when an individual not deemed a possible security risk concludes his or her travel. Because the program places no limits on who may be deemed a risk, however, this protection is insufficient. The good faith of the Department and its officials is not in question, but good faith does not protect privacy. The structure of programs and explicit legal protections do.

There is only one appropriate way to structure a government-controlled security or law enforcement database. That is to collect information only about individuals who meet a requisite legal level of suspicion. For non-suspects, appropriate government security measures may include *checking* information about travelers, but they do not include *collecting* information about travelers. Happily, this structure is as consistent with the Fourth Amendment's privacy protections as it is cost-effective.

Database-Style Security and Law Enforcement Do Not Work

Experience shows that databasing information about innocent people in the name of national security or law enforcement is ineffective and wasteful.

Currency transaction reporting and mandated suspicious activity reporting under the Bank Secrecy Act have been in place since the early 1970s. They have increased the cost of financial services to American consumers by billions of dollars per year. Yet they have brought little in the way of crime or terrorism control. In 1998, the cost-per-conviction to the private sector — that is, not including the cost to taxpayers of investigation, prosecution, and adjudication — was more than $10 million dollars in cases that relied on Bank Secrecy Act data.

More importantly, databasing information about the movements of innocent people would be even *less* effective than databasing suspicious information. When Mohammed Atta, the ringleader of the September 11th hijackers, received wire transfers from the United Arab Emirates totaling as much as $100,000 in 2000, the bank receiving the transfers reported it, as required by law. But, as the Wall Street Journal reported, the first time the Financial Crimes Enforcement Network became aware of this document — in its own files — Mr. Atta had flown a plane into the side of the World Trade Center. Going beyond Bank Secrecy Act-style requirements and recording the non-suspicious movements of innocent people would deliver even worse results than Bank Secrecy Act reporting has.

Expansive government databases about the behavior of all Americans needlessly degrade the privacy of the law-abiding. They do not prevent terrorism or cost-effectively catch crime. They are a poor, but expensive substitute for good analysis of information about threats and suspects that is already available to law enforcement and national security agencies. They are not worth the incursion against Americans' privacy.

Data about ordinary air travelers lawfully going about their daily lives should remain where it is useful: in the hands of airlines. There, it serves the interests of the traveling public as airlines use it to tailor services, reward faithful customers, and reduce costs.

When data is in private hands, consumer choice, market incentives, and private and public law constrain its use. If airlines misuse personal information in any way, including by violating privacy, they are subject to suit and consumerist retaliation. Because they are not government actors, they are not in a position to violate civil liberties using information they collect for security purposes. Airlines also risk substantial loss and liability if they fail to find the right balance between privacy and security; they have every incentive to get that balance right.

In the event of a transportation-related emergency or incident, it may be necessary to transfer data to public authorities — and perhaps the Department should prepare with airlines for that unfortunate eventuality. But the Department should not collect information about every air traveler in the absence of suspicion or emergency. Doing so would needlessly destroy privacy for negligible security gains.

As structured, the Department's intended "Aviation Security Screening Records" system is anathema to both privacy and cost-effective security. The Department is proposing to maintain secret files about all American travelers. The files may contain all kinds of travel and transactional data. The files may be shared with nearly any type of government authority and many private organizations and individuals. The files will not be available for review or inspection by the data subjects. Indeed, Americans will not be entitled to know whether files about them are being maintained.

The Department should withdraw this system of records and restructure the CAPPS II program consistent with the privacy of law-abiding American travelers.

Sincerely,

James W. Harper
Editor
Privacilla.org