epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

Statement for the Record of

Cédric Laurant, Policy Counsel
Electronic Privacy Information Center

EUROPEAN PARLIAMENT

COMMITTEE ON CITIZENS' FREEDOMS AND RIGHTS, JUSTICE AND HOME AFFAIRS

Tuesday, 25 March 2003, 9 am - 12.30 pm

PUBLIC SEMINAR

Data Protection since 11 September 2001: What Strategy for Europe?

CHAMBER OF THE EUROPEAN PARLIAMENT

Paul-Henri Spaak Building, 3rd floor
Rue Wiertz 60
Brussels, Belgium

Introduction

EPIC is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values.

EPIC intends to make conference participants fully aware of the consequences of transferring European passengers' personal data to the United States.

Several US government projects are currently being implemented that would involve the data mining and profiling of airline passengers whether they are traveling to, from or within the United States. We have analyzed some of the risks that some of those profiling and data-mining programs have raised with respect to individuals' privacy and have asked a few questions that we invite the European Union competent authorities to examine.

Our aim is to make European officials and the public in the European Union aware of the way their personal data as passengers may be processed once they have been transferred to US authorities and the extent to which their privacy rights may be threatened.

1. New passenger profiling systems developed in the United States threaten American and European travelers' privacy

1.1. American civil liberties groups' critiques of the new passenger profiling systems

- *Reversal of the presumption of innocence*: the CAPPS-II[1] proposal violates the constitutional guarantee of protection from unwarranted government searches and the right to travel freely. The new monitoring system, by allegedly enabling the US transportation agency to collect information and conduct background investigations of *all*—American or foreign—commercial airline passengers in a manner that would otherwise require a court order on a case-by-case basis, qualifies *all* airline passengers as suspects of terrorism and a threat to national security, unless proven otherwise. The system makes everyone guilty unless proven innocent by carrying out a thorough search through extensive data mining of passengers' personal information.
- *Widespread spying*: the Transportation Security Agency ("TSA") would gain access to financial and transactional data, such as credit reports and

[1] Computer Assisted Passenger Prescreening System II ("CAPPS-II"): CAPPS-II is the second version of "CAPPS", a passenger monitoring system established in the late nineties and revamped after the 2001 terrorist attacks by the Federal Aviation Administration, that allowed airlines to demand photo identification and was based on travel data airlines routinely collected. CAPPS-II, the new generation of travelers' profiling systems, proposes to use extensive data mining of credit history, criminal records, and travel patterns and expand the range of databases searched for suspicious activity to profile all airline passengers. The new system would use an algorithm to determine indicators of characteristics or behavior patterns that are related to the occurrence of certain behavior.

records of purchases, confidential business records, proprietary data, information from law enforcement and intelligence sources[2], which could reveal a lot about an individual's personal lifestyle. The TSA does not say which information it considers off-limits.

- *Long-term retention of passengers' records*: the passenger data would be kept only until passengers complete their travel, TSA says. But for individuals "deemed to pose a possible risk to transportation," the data would be kept for up to 50 years. This 50-year retention policy system could have the unintended consequence of creating a permanent blacklist of travelers who, once only, would have been considered as a threat for airline travel and would not be able to travel freely later on.
- *Data sharing*: information on fliers rated as high risks could be given to private entities and government authorities. A yellow code in a passenger's file could be shared with other government agencies at the federal, state and local level, with intelligence agencies such as the CIA and with foreign governments and international agencies. These third parties could, in turn, use this yellow flag for other purposes, including hiring and other employment decisions, or the granting of government benefits.[3]
- *No access to the data – no judicial remedies are available*: the TSA system would be exempt from federal privacy protections that grant individuals access to government records to enable them to correct potential errors. Travelers would therefore not be informed when the database is used to deny them of any benefit or right. This would prevent passengers from learning what is compiled on them, how their threat level was determined, how information has been used against them, or even, whether they have been labeled a threat.
- *No oversight and no reporting requirements*: Without transparency requirement on the US government's shoulders, the system could easily be abused and lead to capricious, unfair, or politically biased decisions on who to stamp as suspect.
- *Function creep*: passengers' data used by the CAPPS-II system could later be used for different purposes not originally considered. The example of no-fly lists that the FBI circulated after September 11 shows the tendency that the government has to apply existing schemes to new purposes. In FBI's "Project Lookout" the US law enforcement agency gave private companies a list of hundreds of names of persons the agency wanted to talk to. The list was widely circulated and quickly became riddled with inaccurate information as it was transferred from company to company. The list, once established for a legitimate purpose—the combat against terrorism—was used later for denying jobs to, or arbitrarily discriminating against, innocent people.

[2] 68 Fed. Reg. 2101 (January 15, 2003), also available at http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/03-827.htm.
[3] *Ibid.*

1.2. New INS and DOT's Privacy Act notices[4] violate the Privacy Act of 1974[5]

1.2.1. The new INS proposed rule on passenger manifest information violates the Privacy Act and the US Constitution

A new Immigration and Naturalization Service ("INS") regulation[6] proposes to require that commercial carriers transporting passengers to or from the United States deliver arrival and departure manifest information electronically to the INS. This information has been collected in the past from non-US citizens only. Under the proposed rule, manifest information would, for the first time, be collected for all passengers, including US citizens and lawful permanent residents. In its comments[7], EPIC concludes that such proposal raises significant issues under the US Privacy Act and the US Constitution. Not only is the INS proposed rule deficient under the Privacy Act, but by collecting and sharing travel data about citizens, it also is potentially in violation with the right to travel[8] and the right to associate anonymously[9], as these rights are protected by the US Constitution. The INS has proposed an "unprecedented practice of collecting and maintaining detailed information about the international travel of US citizens absent particularized suspicion."[10]

1.2.2. The DOT's Aviation Security Screening Records system presents risks for travelers' privacy

The Department of Transportation ("DOT") issued two notices on January 15, 2003 by which it seeks to create a new system of records (the "Aviation Security Screening Records"[11] ("ASSR")), pursuant to its obligations under the Privacy Act of 1974

---

[4] Pursuant to the US Privacy Act, government agencies have to issue new regulations through the publication of notices every time they intend to establish new systems of records.

[5] The Privacy Act regulates the way government agencies may process US citizens' governmental records and personal data.

[6] Immigration and Naturalization Service, "Proposed Rule on Manifest Requirements Under Section 231 of the Act", 68 Federal Register 292, January 3, 2003. This legislation is the basis for the current talks between US Customs and the European Commission.

[7] See EPIC, Comments before the Immigration and Naturalization Service on the Manifest Requirements Under Section 231 of the Act (INS No. 2182-01), February 3, 2003, http://www.epic.org/privacy/airtravel/ins_manifest_comments.pdf.

[8] "The INS has failed to explain its rationale for collecting information about the international travel of citizens, thus raising questions as to the legitimacy of the burden such collection would impose on the exercise of th[e] constitutionally-protected right [to international travel]. *Ibid.*, at 4.

[9] It would (…) be constitutionally suspect for the INS (and the government generally) to collect travel data for the purpose of determining or monitoring the associations of citizens. Manifest information clearly can be used for such purposes; the INS acknowledges, for instance, that it seeks to "analyze the patterns and associations of alien smugglers on a real-time basis." 68 Fed. Reg. at 300. A governmental desire to track individuals' movements, and its attempts to do so through a blanket provision that collects and archives travel information from all travelers, would clearly violate the right to associate anonymously, a right that would be burdened by a government program specifically designed to monitor associations. (…) The Supreme Court has long recognized a right to associate anonymously. (…) To the extent that the proposed collection of personally identifying information would enhance the government's ability to track the movements and associations of United States persons, it would clearly implicate individuals' right to travel internationally and to associate anonymously." *Ibid.*, at 4.

[10] *Ibid.*, at 4.

[11] The ASSR database would contain PNR, associated data and reservation and manifest information. It would also include financial data (e.g., credit card transactions), transactional data (for instance, any

("Privacy Act")[12]. The DOT has proposed to exempt the ASSR from certain record keeping obligations under the Privacy Act, stating that it may limit disclosures about the system because it is being used for law enforcement purposes. The two notices extend the scope of the rights that the Privacy Act grants DOT by providing that DOT may share the information it collects in its databases to law enforcement authorities and various other domestic and international governmental agencies.

EPIC, along with several other civil liberties advocacy groups, filed comments with the DOT to oppose the passenger profiling system established by the TSA, mainly for lack of transparency and accountability. They have criticize the US government for failing to fulfill its legal obligations under the Privacy Act and have strongly recommended, either to withdraw the ASSR regulations as they are set out in the DOT's Privacy Act Notice, or to complement it with more details about how the Notice can comply with the Privacy Act.[13]

The ASSR regulations[14]'s proposed exemptions to the Privacy Act, as they would be established by the DOT's Notice, is contrary to the Privacy Act's main aim of providing various specific procedural safeguards to protect individuals' privacy and promoting accountability by government record-holders. More particularly, the Notice does not comply with specific provisions of the Privacy Act:

- *the collection requirement*: while the Privacy Act requires an agency to collect data directly from the subject as far as possible, the TSA has provided no information about where the data will be collected from and whether the data will be collected following lawful procedures based upon a showing of particularized suspicion. As an example, categories of information collected by the TSA could include private third party companies' individual's credit history or credit rating, which accuracy has often been challenged.
- *the access and correction rights requirement*: while the Privacy Act requires an agency to provide data subjects with such rights, the DOT's Notice explicitly denies the right of access to the system of record for the "purposes of determining if the system contains a record pertaining to a particular

---

electronic purchase or service), proprietary and public source information available in government and private industry databases, which could reveal sensitive personal information.

[12] Privacy Act (1974). Public Law 93-579, 5 U.S.C. §552, available at http://www4.law.cornell.edu/uscode/5/552.html.

[13] *See* EPIC, Comments before the Department of Transportation in the Matter of Privacy Act Notice Concerning Aviation Security Screening Records (DOT/TSA 010 – OST-1996-1437), February 24, 2003, http://www.epic.org/privacy/airtravel/tsacomments2.24.2003.html; Electronic Frontier Foundation, PrivacyActivism, Privacy Rights Clearinghouse, CASPIAN, and Michael Stollenwerk, Comments before the Department of Transportation, Docket No. OST-1996-1437, "ASSR Regulations – Proposed exemptions from the Privacy Act of 1974", March 14, 2003, http://www.eff.org/Privacy/TIA/20030314_cappsII_comments.pdf; American Civil Liberties Union, Comments before the Department of Transportation, Docket No. OST-1996-1437, " 'Aviation Security Screening Records' 68 Fed. Reg. 2101 (January 15, 2003)", February 24, 2003, http://www.aclu.org/Privacy/Privacy.cfm?ID=11909&c=130; Center for Democracy and Technology, Comments before the Department of Transportation, Docket No. OST-1996-1437, "Comments of the Center for Democracy and Technology on Aviation Security Screening Records System, 68 Fed. Reg. 2101 (January 15, 2003)", February 24, 2003, http://www.cdt.org/security/usapatriot/030224cdt.pdf

[14] Notice of Proposed Rules, published in the Federal Register, January 15, 2003 (Volume 68, Number 10) ("The Notice").

individual"[15], and therefore, deprives individuals of their ability to verify the accuracy of their records or correct any data errors.

- *the justification requirement of § 552(a)(k)*: while the Privacy Act considers specific exemptions from the Act's procedural safeguards only where a federal agency can demonstrate that they are justified because they can be considered as "properly classified information"[16] or "investigatory material compiled for law enforcement purposes"[17], the DOT's Notice does not provide any of these justifications.[18] This may amount to an attempt to avoid accountability and public scrutiny, since there is no mechanism provided that could be used to review the information to assess the appropriateness of the TSA's claim to exemption.
- *the purpose specification requirement*: The Privacy Act provides that only relevant data be collected and for a limited purpose.[19] The TSA has not provided any clarity on the actual purpose of this data collection, or whether the creation of a Passenger Database is narrowly tailored to that purpose. Also, there does not appear to be any restriction on potential uses of the Passenger Database by other local, state, federal, or even international, governmental agencies.
- The *proportionality requirement*: while the Privacy Act's spirit and intent requires that the scope of exemptions not be disproportionate with the categories of exemptable records, the TSA Notice invokes the narrowly interpreted exemptions of § 552 (k)(1) and (2) to exempt the entire ASSR system of records.[20] This may show that the TSA may attempt to get a blanket exemption for the entire system of records by using exemptions of narrow interpretation. The Notice, because it does not disclose anything about the specific categories of information to be recorded, makes it impossible to assess whether the exemptions are correctly interpreted.
- The *accuracy requirement*: part of the purpose behind the Privacy Act was to ensure that information the government did collect about individuals was accurate.[21] The poor quality of data in the various commercial databases such as credit reports has been well documented.[22] The CAPPS-II database would appear to be as big as the biggest commercial databases in place.[23]

---

[15] 5 U.S.C. § 552(a)(k).
[16] 5 U.S.C. § 552(a)(k)(1).
[17] 5 U.S.C. § 552(a)(k)(2).
[18] The Notice merely states that "the system may be used, generally, to review, analyze, and assess threats to transportation security and respond accordingly."
[19] 5 U.S.C. § 552(e)(1).
[20] The wording of the Notice, while it invokes both of those exemptions "to the extent that ASSR contains [the relevant category of exempted information]", fails to identify what proportion of the records in the system are either "properly classified" or "investigatory material compiled for law enforcement purposes".
[21] Privacy Act of 1974 Congressional Findings, Section (b)(4).
[22] See *e.g.*, PIRG, Mistakes Do Happen: Credit Report Errors Mean Consumers Lose, http://www.pirg.org/reports/consumer/mistakes/ (finding that over 70% of credit reports have errors, with 30% having serious errors.)
[23] The CAPPS-II contract suggests the possible size of such a database, if indeed it is related to the CAPPS-II initiative. See Presolicitation Notice, DTSA20-03-R-00780, published on January 29, 2003. A commercial database such as MasterCard's database of 1.7 billion cardholders and all their transactions in a year contain about 40 terabytes of data. Data Diets, CIO Magazine, January 1, 2003, http://www.cio.com/archive/010103/et_company_content.html (last visited on March 19, 2003).

There is a serious likelihood that the use of multiple-source commercial databases would result in a number of incorrect determinations because of the bad data stored in these databases.

Additional critiques of DOT's Notice:

- The TSA could collect a very extensive range of records on *all* travelers. Categories of individuals affected by TSA's new system of records cover two classes of individuals to whom apply different collection requirements. For airline passengers,[24] the information to be collected is limited to the Passenger Name Records "and associated data" and reservation and manifest information of passenger carriers. On the other hand, for individuals flagged as risky for national security[25], the categories are broader since they include "risk assessment reports, financial and transactional data, public source information, proprietary information, and information from law enforcement and intelligence sources." The distinction between passengers is only theoretical since the TSA does not specify the criteria it will use to assess whether some passengers are deemed risky while others are not. In practice, the TSA may well authorize itself to collect the broad range of data from *all* travelers.
- The DOT's Notice expands the secondary purposes for which the data may be shared by providing federal, state or local agencies access to the Passenger Database to make hiring decisions, grant licenses, and issue security clearances. There appears to be no limit on the possible applications for that database.
- The Notice does not demonstrate that the ASSR system will be effective in achieving its intended purpose. Barring data subjects from accessing and correcting their records and is very likely to generate many inaccuracies and errors, make the system less secure, and prevent the system from learning from its own mistakes when making risk assessments.

The TSA has not given enough information to the public and Congress to give opportunities for public debate and congressional scrutiny. TSA has not been responsive to EPIC's Freedom of Information Act ("FOIA") requests. The way TSA intends to operate its ASSR system of records shows a serious lack of accountability and transparency that violates the most basic requirements of the Privacy Act, even though that legislation was enacted precisely to counter government secrecy, promote meaningful public accountability, and provide data subjects with an opportunity to contest inaccurate or abusive record holding practices.

1.3. Risks of passenger profiling systems for European travelers' privacy

There is no protection for non-US citizens under the US Privacy Act. If US citizens can legitimately be concerned about the scope of tracking schemes like the one proposed by the INS and the TSA, non-US citizens can be even more concerned since

[24] "[I]ndividuals traveling to, from, or within the United States by passenger air transportation."

[25] "[I]ndividuals who are deemed to pose a possible risk to transportation or national security, a possible risk of air piracy or terrorism, or a potential threat to airline or passenger safety, aviation safety, civil aviation or national security."

they do not benefit from the legal protection that the Privacy Act can provide American citizens later. If EU travelers wanted to assert their rights and seek remedies for privacy violations in the United States, their access to justice would likely be much more burdensome than it is for US citizens.

As the TSA purports to use private contractors for various purposes in its profiling endeavors, such as for carrying out the storage or data-mining of travelers' data, there is a high risk that the information be released to other private companies and the commercial sector in general, and later, be used for secondary purposes unrelated to the combat against terrorism and the protection of air travel safety. The disclosure of non-fly lists by the Federal Bureau of Investigations has been reported as having had a negative impact on people looking for a job in the private sector.

2. Future threats to travelers' privacy

2.1. "Total Information Awareness"

The TIA project, part of the Defense Advanced Research Projects Agency's Information Awareness Office, purports to capture the "information signature" of people so that the government can track potential terrorists and criminals involved in low-intensity/low-density forms of warfare and crime. The goal is to track individuals through collecting as much information about them as possible and using computer algorithms and human analysis to detect potential activity. The project calls for the development of "revolutionary technology for ultra-large all-source information repositories," which would contain information from multiple sources to create a "virtual, centralized, grand database." This database would be populated by transaction data contained in current databases such as financial records, medical records, communications records, and travel records as well as new sources of information and intelligence data.[26]

TIA has been strongly criticized by the US Congress because of concerns that the program would intrude on individual privacy, and be contrary to the longstanding principle that law enforcement needs cause before it can investigate its citizens. Furthermore, TIA had been developed in total secret, outside any congressional oversight and without any specific authorization. The Congress reacted by voting to block funding for the initiative unless DOD provided it a detailed analysis of the program and its civil liberties implications.[27]

Where it appears that TIA has been somewhat constrained by Congress, the same does not hold true with respect to non-US citizens. Congress, in fact, has not limited the use of TIA for spying on non-Americans. TIA promoters are left free to test their new

[26] A key component of the TIA project is to develop data-mining or knowledge discovery tools that will sort through the massive amounts of information to find patterns and associations. TIA aims to fund the development of more of such tools and data-mining technology to help analysts understand and even "preempt" future action. For more details, see EPIC's "TIA" web page at http://www.epic.org/privacy/profiling/tia.

[27] 108 H.J. Res. 2 Consolidated Appropriations Resolution FY 2003, included Senated Amendment No. 59.

profiling tools on Europeans. Nothing would then prevent passenger data obtained through CAPPS-II from being fed into a huge TIA profiling database for purposes related, or unrelated, to the combat against terrorism or the protection of airline travel security. In this respect, "Echelon", the US National Security Agency's ambitious surveillance scheme of global communications, can hardly dispel such fears.

2.2. CAPPS-II

2.2.1. A controverted profiling system

CAPPS-II is based on the same concept as the Department of Defense's Total Information Awareness ("TIA") program. The scope of the content and uses of the ASSR database suggests that there is a link between TIA and CAPPS-II. TSA's CAPPS-II looks like a new version of TIA, but in the field of airline travel. CAPPS-II would scour travelers' personal information for patterns, associations and trends that could—theoretically at least—reveal terrorist activity. Not much has been disclosed about this new system by its promoters but what is known is already troubling.

CAPPS-II is a new security and profiling system that the United States DOT is proposing to air travelers. The TSA proposes to collect passenger manifest information[28] on all airline travelers and store it in a large centralized database. It would then forward the passenger's identifying information to commercial information services and have them construct a risk score, based on computer models provided by the TSA that would be determined by analyzing passengers' data. Those data would be obtained from data mining of airline-ticket information, government records, law enforcement systems of record, commercial financial and transactional databases, public source information and proprietary data. Risk scores would help determine whether a passenger could board a flight. CAPPS-II would allow airport authorities to look up a computer that would search if a person were to be identified as a possible suspect. The information would be forwarded to the appropriate law enforcement agencies. Before boarding the plane, passengers would be assigned one of three rankings printed in code on their boarding passes: green would require routine security, yellow, "added checks", while red would bar passengers from flying and subject them to law enforcement investigation. The red code would be reserved for those on terrorist watch lists.

[28] "Passenger manifest information" includes "Passenger Name Records ("PNR") and associated data." This includes date and time of flights, flight number, destination, reservation and payment information. "PNR" refers to "Passenger Name Record". This may include date of birth, address, phone number, reservation number, date(s) of travel, travel agency/agent, ticket information, traveling companions, form of payment for ticket such as credit card number, itinerary information, carrier information for the flight such as the flight number and date of intended travel and PNR history. (*See* Interim Rule, Fed. Reg., June 25, 2002. Passenger Name Record Information Required for Passengers on Flights in Foreign Air Transportation to or from the United States, p. 42,710.) "PNR history" can include very sensitive information about religious or ethnic origin (through the choice of meals), data relating to the place of residence or contact information (including phone numbers and addresses of friends and family), and medical data relevant to disability accommodations (oxygen, sight, hearing, or mobility).

The media have started revealing worrisome details about CAPPS-II that show how much profiling is considered[29] and how many applications the system could be extended to.[30]

2.2.2. Primary and secondary purposes of CAPPS-II

"The intent of the CAPPS-II program is to improve the ability to identify threats to aviation security by analyzing and evaluating multiple-source data on every ticketed passenger on every airline to determine whether the passenger poses a security risk or threat to the traveling public."[31]

Federal, state or local agencies could subsequently use the information gathered for reasons unrelated to the combat against terrorism and airline travel security, for instance when they would consider providing licenses, contracts, grants or other benefits to petitioners.

2.2.3. CAPPS-II raises privacy risks for European travelers

Although CAPPS-II particularly puts American travelers' privacy at risk because of its data mining based on information that most Europeans would not have to worry about (e.g., credit reports and credit history, proprietary and public source information available in the United States), European travelers should be aware of the severe threats that a system like CAPPS-II can raise for their privacy in the United States.

The sophisticated profiling system raises specific policy issues that have to be thought of before allowing the free and unrestricted flow of all Europeans' passenger data to US law enforcement:

- what will be the rights of individuals to control their personal data once they have been transferred in the United States?;
- what recourse will be available for a European wrongly identified as presenting a security threat or denied a flight to the United States?;
- where CAPPS-II's deep data-mining based profiling raises constitutional issues such as equal protection, due process, the fourth and first amendments (including the right to travel), protected by the American judicial system, will Europeans enjoy rights and remedies similar to Americans'?

---

[29] "In recent months, the [TSA] hired four teams of technology companies. Their mission was to demonstrate how artificial intelligence and other powerful software can analyze passengers' travel reservations, housing information, family ties, identifying details in credit reports and other personal data to determine if they're 'rooted in the community' –or have an unusual history that indicates a potential threat.". *See* Robert O'Harrow Jr., *Air Security Focusing on Flier Screening, Complex Profiling Network Months Behind Schedule*, WASH. POST, Sept. 4, 2002.

[30] "Eventually the TSA, which says it is building privacy protections into the system, intends to extend its use to screen truckers, railroad conductors, subway workers and others whose transportation jobs involve the public trust. See Robert O'Harrow Jr., *Aviation ID System Stirs Doubt – Senate panel Wants Data on Impact on Passenger Privacy*, WASH. POST, March 14, 2003, at A16, also available at http://www.washingtonpost.com/wp-dyn/articles/A23084-2003Mar13.html.

[31] Presolicitation Notice, DTSA20-03-R-00780, published on January 29, 2003.

3. Reactions in the American public, US Congress, and the travel industry

In the United Stated, the public, the travel industry, Congress and civil liberties groups have sharply objected to the US government's passenger profiling plans, mainly criticizing the lack of accountability and transparency of the Transportation and Security Administration and asserting that it could subject American travelers to intensive and intrusive background checks without appropriate controls on the ways the information would be used, and without adequate justification of their necessity.

CAPPS-II and TIA have been subject to much criticism among civil liberties groups and various advocacy organizations. In January of this year, a coalition wrote to Congress about TIA to encourage its Members to inquire about the new proposed system.[32] The letter also noted that CAPPS-II raised similar questions. In March, another coalition wrote to the Committee on Commerce, Science and Transportation to support an amendment that required the Secretary of the Homeland Security to answer questions about CAPPS-II.[33]

EPIC filed several FOIA requests to obtain more information about CAPPS-II and TIA. All requests have thus far not been answered.[34]

On March 11, the Senate Commerce Committee, through an amendment[35] by Sen. Ron Wyden (Democrat Member of Congress from Oregon), asked the Transportation Security Administration to report to Congress on the privacy and civil liberties implications of the controversial CAPPS-II air passenger profiling system. The amendment requires the tough questions about CAPPS-II to be addressed in the report.[36]

The airline and travel industry has not stayed quiet either. Airline companies consider that the new profiling requirements of the Advance Passenger Information System[37]

---

[32] Letter to Chairperson Collins, Senate Government Affairs Committee, dated January 14, 2003. Signatories included the American Civil Liberties Union, Eagle Forum.

[33] Coalition letter to the Senate Commerce, Science and Transportation Committee Urging Support to the Wyden Amendment to S. 165, the Air Cargo Security Act (March 13, 2003), http://www.aclu.org/SafeandFree.cfm?ID=12089&c=206&Type=s.

[34] Cfr www.epic.org/privacy/airtravel for more details.

[35] http://www.epic.org/privacy/airtravel/wyden_capps_amdt.pdf.

[36] Questions include: who will have access to the data gathered on individual travelers, and who will make decisions concerning access?; how will the TSA treat the security threat-related scores assigned to travelers; whether they may be shared with other governmental, non-governmental, or commercial entities?; what role private entities, such as airlines, outside vendors and contractors, will have in implementing and operating the system, and to what extent passenger data will be shared with them?; what safeguards will be implemented to ensure that the system will be sued as originally intended?; what procedural recourse will be available to travelers who believe they have been wrongly barred from flying?; what oversight will be implemented to ensure privacy and other civil liberties issues are addressed on an ongoing basis? Cfr Robert O'Harrow, *Aviation ID System Stirs Doubts – Senate panel Wants Data on Impact on Passenger Privacy*, WASH. POST, March 14, 2003, at A16, also available at http://www.washingtonpost.com/wp-dyn/articles/A23084-2003Mar13,html.

[37] APIS: is a system where commercial air carriers collect and submit biographical data from a passport, visa or other travel document at a foreign port and transmit this information electronically to the Immigration and Naturalization Service ("INS") and the United States Customs Service ("USCS") in

("APIS") "threaten to cause big delays at check-in and raise ethical questions about a passenger's right to privacy of information". [38] They assert that the new requirements will cause "an administrative nightmare" and be "financially punitive".[39] The Association of Corporate Travel Executives, a group of 2,500 travel managers, agencies and industry executives from more than 30 countries feels that the government plans are an "invasion of their personal privacy".[40] A survey made early March 2003 of members of the Association of Corporate Travel Executives showed strong opposition to the program and government distrust.[41] In the United Kingdom, the Institute of Travel management, which represents UK corporate travel buyers, criticized the US action as ineffective to solve real security concerns.[42]

The American public has showed so much anger that a web site, boycotting Delta for its intention to test the CAPPS-II program, allegedly received more than 250,000 unique visits since it was launched at the beginning of March, and generated more than 3,000 e-mails from travelers.[43] In a *Biz Class* survey, a vast majority of readers expressed their opposition to any system that would scour their personal histories and credit standing.[44] Last year, the media disclosed that the FBI had been circulating a "no-fly list" to several law enforcement agencies and private companies. Several members of the public felt that they had been incorrectly placed on a watch list and did

---

advance of the commercial aircraft's arrival in the United States. Manifest Requirements Under Section 231 of the Act (INS No. 2182-01), January 3, 2003, 68 Fed. Reg. 292.

[38] Amon Cohen, *Security Sting at the Check-in – New US Demands for Passenger Data threaten Delays and an Invasion of Privacy*, FINANCIAL TIMES, February 25, 2003, Section Inside Track, at 12

[39] *Ibid.*

[40] David Jones, *Travel Industry and Privacy Groups Object to a US Screening Plan for Airline Passengers*, N.Y. TIMES, March 6, 2003, at section C, page 2.

[41] "82 percent of the 255 respondents considered the program an invasion of privacy. The same percentage said they would not trust the government's handling of personal data that would be collected." *Ibid.* "The survey also showed that 64 percent of respondents thought the program would discourage commercial flying, while 79 percent said that they would avoid flying on any airline that uses the system." *Ibid.* "If you go to buy a handgun, the only thing they check is your criminal record", a spokesman of the Association stated. "But if you buy an airline ticket, they're going to be checking your financial records and criminal records. Why would you have a more stringent procedure for buying an airline ticket than buying a gun?". *See* Joe Sharkey, *A Safer Sky or Welcome to Flight 1984?*, N.Y. TIMES, March 11, 2003.

[42] "Any self-respecting terrorist would be able to overcome anything that goes in a PNR. No one has given us a detailed reason why this is needed. The knock-on effect is some people are going to decide they won't travel to the US", Tom Stone, vice-chairman of the UK organization said, *see* Amon Cohen, *Secret EU Agreement Lets US Snoop on Transatlantic Flyers*, THE TIMES (London), March 20, 2003.

[43] The web page (http://www.BoycottDelta.org/) explains which specific data Delta requires from their passenger and how Delta uses this data. It *also* points out which effect this data collection and credit report verification may have on passengers. The website indicates that collected data will be stored for up to 50 years and that, according to US credit report regulations, the personal credit rating may be severely damaged. *The* web page *goes on* accus*ing* Delta for an illegiti*mate invasion of privacy and calls every* client *or potential Delta client to boycott the company.* See Keith L. Alexander, *Seeing red on Security System*, WASH. POST, March 11, 2003, at E01.

[44] "A vast majority of readers said they were opposed to computers delving into their personal histories, including credit standing and possible criminal past, in the interests of heightened security aboard a flight." *Ibid.*

not know how to correct the record, or were concerned that they were put on the list for their political opinions.[45]

The TSA has not thus far given appropriate answers to its critics.[46] The agency says that any credit or other personal information collected by the system will come from "commercially available databases, the same kind that marketers use"[47], but seems to forget the distinction made in the US legislation between databases processed by private companies and governmental agencies. Some of its answers do not inspire much trust in future potential uses of the system.[48]

4. EPIC's assessment of the EU-US Joint Statement

The US/EU Joint Statement violates EU data protection laws for several reasons[49]:

- The exemption of Article 13 of the Directive, through its words "necessary measure", can be applicable only in the context of specific investigations. Article 13 can therefore not be invoked to limit the obligations of the Directive where the transfer of passenger data is systematic as it is the case in the transfer of EU passengers' data to the USCS. If US law enforcement authorities intend to collect travelers' data, they should limit themselves to ask information only in cases where they have sufficient evidence to believe that certain EU travelers may pose a threat to air travel safety or constitute a terrorist threat.
- The special categories of personal data[50] protected by Article 8 of the Directive should not be transferred to US authorities without the data subject's "explicit consent" or without substantial public interest.
- The USCS's promise to abide by the Directive's data quality principles of Article 6 should be strictly enforced. However, the USCS currently infringes Article 6 since it processes every EU passenger's data without having to justify of any specific and legitimate purpose and allows itself to process the data later for purposes incompatible with the original ones.
- The US FOIA legislation cannot, through its exemptions, fully protect the disclosure of European travelers' personal data to third parties, especially in the context of judicial proceedings. Even though the USCS treats PNR information as law enforcement sensitive, and confidential personal information[51], administrative and judicial authorities may not interpret FOIA

[45] EPIC filed a request on October 3, 2002 after learning about those complaints. After exhausting all administrative remedies in waiting for a response, EPIC filed suit on December 12, 2002 to compel the disclosure of the information. See http://www.epic.org/privacy/airtravel/tsa_foia_suit.pdf.

[46] See James M. Loy, *Privacy Will Be Protected*, USA TODAY, March 11, 2003, http://www.usatoday.com/news/opinion/editorials/2003-03-11-oppose1_x.htm.

[47] Joe Sharkey, *A Safer Sky or Welcome to Flight 1984?*, N.Y. TIMES, March 11, 2003.

[48] For those who are concerned because they are behind on child-support payments or have poor driving records or outstanding parking tickets, the TSA ha[s] some reassuring words: They would not be forbidden to fly, said TSA spokesman Brian Turmail. *See* Keith L. Alexander, *Seeing red on Security System*, WASH. POST, March 11, 2003, at E01.

[49] *See generally* http://www.epic.org/privacy/intl/passenger_data.html.

[50] Such as the choice of meal which may reveal religious, ethnic or medical information.

[51] See Annex to the European Commission/US Customs Talks on PNR Transmission (Brussels, February 17-18, 2003) ("Joint Statement").

exemptions the same way allowing some personal data to be disclosed in the context of a FOIA request;

- Sharing of personal data by USCS with other US government agencies: USCS regulations allow the sharing of PNR information to other agencies "for the purpose of protecting national security" and "as otherwise authorized by law"[52], which allows wide sharing to agencies, contrary to what the USCS states in the Joint Statement.[53]

5. EPIC's suggestions and recommendations

If US traveler profiling programs raise serious privacy concerns about how they will intrude into US citizens' privacy, they raise even more concerns about how they will be applied to EU passengers. The US government has not been very transparent until now to disclose the scope of the profiling programs it has started carrying out. It has not demonstrated that circumstances exist that would warrant the impairment of the right to privacy. The government has not demonstrated either that its proposed programs would likely increase public security to an extent that would warrant exceptions to individuals' privacy.

Since the Privacy Act has not been complied with by the DOT and the INS when they sought blanket exemptions from the Privacy Act, there should be no transfer of data from the EU to the US until the legality of DOT and INS Privacy Act notices has been determined.

The following questions should be answered before proceeding further with a general transfer of all EU travelers' personal data:

- Whether the US government's passenger profiling endeavors to deter terrorism and ensure air travel safety are *adequate* and *proportionate*.
- Who will have *access* to EU travelers' data, and who will make decisions concerning access among US law enforcement authorities and agencies?
- Whether passenger data and related risk scores may be *shared* by DOT , INS and the USCS with other governmental, non-governmental, or commercial entities.
- What are the specific measures taken by US law enforcement to process *special categories of data*, as they are protected by Article 8 of the Data Protection Directive?
- Whether and for what period of time the data gathered on individual travelers will be *retained*?; Retaining data of persons deemed as a risk for air travel safety for 50 years is excessive.
- What role *private entities*, such as airlines, outside vendors and contractors, will have in implementing and operating the system, and to what extent passenger data will be shared with them?

[52] CFR, Section 122.49b(d).

[53] "US Customs may provide information to other US law enforcement authorities only for purposes of preventing and combating terrorism and other serious criminal offences, who specifically request PNR information from US Customs. *See* Point 5(e) of the Joint Statement.

- What *safeguards* will be implemented to ensure that the system will be implemented as originally intended? TSA databases should not be used for secondary purposes, such as marketing, or to target criminality that is not related to the combat against terrorism and the protection of air travel safety. Access should be restricted to agencies involved in the combat against terrorism.
- What *procedural recourse* will be available to EU travelers who believe they have been wrongly barred from flying, since the Privacy Act does not apply to non-US citizens?
- What *oversight* will be implemented to ensure privacy and other civil liberties issues are addressed on an ongoing basis? As a minimum, there should be regular public reporting requirements answering whether TSA profiling schemes have been effective, and whether and how they have reduced air travel safety; and how many complaints have been filed with the agency for misuse of data and inaccuracies.
- *Transparency of processing*: all records in travel profiling systems should be accessible to all EU travelers if they have reasons to believe that their records are inaccurate or that they have been denied the right to fly unfairly.

Respectfully submitted,

Cédric Laurant,
Policy Counsel
Electronic Privacy Information Center
1718 Connecticut Avenue, N.W., Suite 200
Washington, DC 20009
United States of America
(202) 483-1140
http://www.epic.org