Travel Privacy

Since the terrorist attacks of September 11, 2001, one of the greatest fears of security officials in the world has been that would-be terrorists would board commercial airline flights without their malicious intentions being detected in advance. As a result, the US and many of its international allies have placed a high priority on identifying, tracking, and profiling travelers, especially air travelers.

Travelers and workers at transportation facilities such as airports have come to be regarded as objects of suspicion, potential terrorists, and targets of surveillance. Security agencies have sought access to reservations and other travel data collected for commercial purposes; compulsory identification of travelers and travel and transportation workers; mandatory collection of additional traveler data and compilation of personal travel dossiers; and deployment of new technologies for real-time tracking and logging of travelers' movements.

Fear is not necessarily proportional to actual danger,[1] and it's not clear that these policy and procedural changes are the outcome of a considered evaluation of risks, benefits, and trade-offs.[2] But whatever their motivation or effectiveness for their declared purposes, these aviation and transportation "security" measures create substantial potential for both commercial and government misuse of personal travel data. Taken together, they could– if successful – lead to the creation of a global infrastructure of surveillance of the movements of persons, incorporating both the travel industry and government agencies.

Privacy Protection for Commercial Travel Records

The privacy of travel records has been less well protected than that of any comparably sensitive category of commercial data. Existing travel industry norms for personal data handling fail to provide the level of protection provided for other categories of data, and required by generally accepted norms of data protection. Even in jurisdictions where data protection laws include travel data, enforcement against violations by the travel industry has been lax.

Reservation and transaction records created by travel companies for commercial purposes contain intimate personal information about airline (and sometimes intercity train and bus) travelers and their movements, as well as personally identifiable information about third-party ticket purchasers, travel industry personnel involved in making and changing reservations, and other business and personal associates of travelers.[3]

Reservation data or one or more people traveling on the same itinerary is stored in a Passenger Name Record (PNR), which typically contains names of travelers and details of flights, hotels,

---

[1] Edward Hasbrouck, "Travel Safety and Civil Liberties: Fear vs. Danger" (last updated May 2003) <http://hasbrouck.org/articles/fear.html>.

[2] Bruce Schneier, Beyond Fear: Thinking Sensibly about Security in an Uncertain World (New York 2003).

[3] Hasbrouck, "What's in A Passenger Name Record (PNR)?," <http://hasbrouck.org/articles/PNR.html>.

car rentals, and other travel services. PNRs can also contain residential and business postal and e-mail addresses and phone numbers, credit card details, and names and personal information of emergency contacts. Through billing, meeting, and discount eligibility codes, PNRs contain information about memberships and organizational affiliations. Since a single PNR typically is used for an entire travel party, PNRs contain detailed information on patterns of association between travelers. PNRs can contain religious meal preferences and special service requests that describe intimate details of physical and medical conditions (*e.g.*, "Uses wheelchair, can control bowels and bladder") – categories of information that have special protected status in the European Union and some other countries as "sensitive" personal data.

Airlines and travel agencies around the world, even those that compete with each other, have long been part of an integrated global network of reservation systems. Most of these systems predate current norms of data protection. While PNR formats vary, "interline" agreements between airlines, joint industry ticketing and financial clearinghouses, and industry-standard protocols[4] facilitate easy global sharing of PNR data.

Most of the world's airlines and travel agencies outsource hosting of their PNR databases to one of four companies: Sabre, Galileo (a division of the Cendant Corp.), Worldspan, and Amadeus. These Computerized Reservation System (CRS) or Global Distribution System (GDS) companies function both as data warehouses and data aggregators, and have a relationship to travel data analogous to that of credit bureaus to financial data. After the completion of a trip, copies of PNRs are "purged" from live to archival storage systems, and can be retained indefinitely by CRSs, airlines, and travel agencies.

Unlike medical and financial data, travel data has not generally been legally recognized as posing special privacy issues, or afforded any special protection. PNRs and ticketing records had been regarded as simply another category of commercial transaction data.

In many countries airlines and travel agents are overseen by different government agencies than other businesses, and few if any aviation regulatory agencies include data protection divisions or enforcement staff. In the US, for example, most consumer privacy policies are enforced by state and local consumer protection authorities and the Federal Trade Commission (FTC). But enforcement of privacy policies by airlines and travel agencies, and of compliance by airlines and travel agencies with the EU-US Safe Harbor arrangement,[5] is under the exclusive jurisdiction of the Department of Transportation (DOT). The DOT has no staff dedicated to consumer privacy or data protection, and has never brought an enforcement action for violation of a privacy policy or of the Safe Harbor arrangement.

---

[4] Such as the ATA/IATA Reservations Interline Message Procedures - Passenger (AIRIMP). Published annually by the International Air Transportation Association (IATA), Montreal and Geneva; available from IATA at <https://www.iataonline.com/Store/Products/Product+Detail.htm?cs_id=9098%2D28&cs_catalog=Publications>; *see also* <http://www.iata.org/idfs/ps/passenger_standards/reservations_standards_rescom.htm>. The 28th edition of the AIRIMP, effective June 1, 2004, for the first time added standard formats for transmission between travel agencies, airlines, and CRSs of personal data collected solely for government purposes (*see* Section 3.14).

[5] <http://www.export.gov/safeharbor/>.

The International Civil Aviation Organization (ICAO) has adopted a model Code of Conduct on the Regulation and Operation of Computer Reservation Systems (CRS) that aims at safeguarding privacy.[6]

However, the ICAO Code of Conduct on the Regulation and Operation of Computer Reservation Systems has not been widely adopted by ICAO member states. CRSs operate under government regulations in the US[7] and Canada,[8] but those regulations include no provisions related to privacy or data protection.

The European Union Code of Conduct for Computerized Reservation Systems, Article 5 (d), provides that, "personal information concerning a consumer and generated by a travel agent shall be made available to others not involved in the transaction only with the consent of the consumer."[9] But there is no record of any enforcement action ever having been taken under this section, despite a history of widespread and systematic violations by all four major CRSs.

National data protection authorities in Belgium (on the complaint of data subjects, including a Member of the European Parliament)[10] and France[11] have ruled that transfers of PNR data by airlines to US government agencies without passengers' consent are illegal. Additional citizen complaints against airlines for violations of national data protection laws have been made in Spain[12] and the Netherlands.[13] However, no corrective action or change in data sharing practices has been ordered as a result of any of these enforcement proceedings.

Like the ICAO standards, the recommendations of the Passenger Services Conference of the International Air Transportation Association (IATA) are only advisory. In addition, they relate only to the conduct of IATA member airlines and not to travel agencies or CRSs. Even if followed, the IATA recommendations serve more to legitimate than to limit airlines' transfers of passenger data to government agencies.[14]

---

6 *See* Article 11: Safeguarding the Privacy of Personal Data: a) States shall take appropriate measures to ensure that all parties involved in CRS operations safeguard the privacy of personal data; b) Air carriers, system vendors, subscribers and other parties involved in air transportation are responsible for safeguarding the privacy of personal data included in CRSs to which they have access, and may not release such data without the consent of the passenger. ICAO Code of Conduct on the Regulation and Operation of Computer Reservation Systems (CRS), adopted by the Council of ICAO June 25, 1996, effective November 1, 1996, available at <http://www.icao.int/icao/en/atb/ecp/CodeOfConduct.htm>; *see also* Notes on the Application of the Code of Conduct, available at <http://www.icao.int/icao/en/atb/ecp/notes.htm>.

7 Computer Reservations System (CRS) Regulations, 14 CFR Part 255, 69 FR 975, January 7, 2004, available at <http://www.dot.gov/affairs/Computer%20Reservations%20System.htm>.

8 Canadian Computer Reservation Systems (CRS) Regulations, SOR/95-275, June 6, 1995, available at <http://laws.justice.gc.ca/en/A-2/SOR-95-275/>, as amended by Regulations Amending the Canadian Computer Reservation Systems (CRS) Regulations, October 23, 2003), available at <http://canadagazette.gc.ca/partI/2003/20031025/html/regle15-e.html>.

9 Council Regulation (EEC) No 2299/89 of July 24, 1989 on a Code of Conduct for Computerized Reservation Systems, Official Journal L 220 of July 29, 1989, as amended by Council Regulation (EEC) No 3089/93 of 29 October 1993, Official Journal L 278 of November 11, 1993, and Council Regulation (EC) No 323/1999 of 8 February 1999, Official Journal L 40 of February 13, 1999.

10 Letter from P. Thomas, Président, *Commission de la Protection de la Vie Privée*, *Royaume de Belgique*, to Marco Cappato, MEP; January 19, 2004, available at <http://www.radicalparty.org/privacy/etats_un.pdf>.

11 *Commission Nationale de l'Informatique et des Libertés*, "PNR : la position de la CNIL sur le transfert de ces informations nominatives," February 24, 2004, available at <http://www.cnil.fr/index.php?id=1017>.

12 Arturo Quirantes, "Don't Fly My Data," <http://www.ugr.es/~aquiran/cripto/nofly.htm>.

13 Letter from Ulco van de Pol, Vice-President, *College bescherming persoonsgegevens*, to Northwest Airlines, April 6, 2004, available at <http://www.cbpweb.nl/downloads_uit/z2004-0310.pdf>.

14 *See* IATA Recommended Practice 1774, Protection of Privacy and Processing of Personal Data Used In International Air Transport of Passengers and Cargo, defines the purposes for which personal data is presumed to have been provided as including "facilitating

Privacy of Travel Records Since September 11, 2001

Almost immediately after September 11, 2001, airlines and the US government – often in collaboration, and of necessity involving the CRSs in their work – began accessing and using archived PNRs to investigate the hijackings and to test the possibility of identifying "suspicious" travelers through PNR profiling. Most of the major US-based airlines and CRSs, and a variety of US government agencies and contractors, were involved in these investigations and experiments over the next two years.[15] All of these tests were conducted at the time in secret, without notice to, or consent of, the data subjects, and in most cases – except the initial investigation of the events leading up to September 11th without warrants or subpoenas. They were gradually revealed to the public as a result of US Freedom of Information Act (FOIA) requests and lawsuits, Congressional questioning, investigative journalism, and admissions by airlines. Governments, airlines, and CRSs in other countries were pressured by the US to cooperate in providing reservation data for these programs, irrespective of national data protection laws against such use without travelers' prior consent.

These profiling systems and tests have not been shown to be effective in identifying would-be terrorists from reservation data, either alone or in conjunction with other databases.[16] It's impossible to identify from a PNR in what country(ies) the data it contains was collected, so each of these tests probably included data subject to many international jurisdictions. The US government proceeded with these tests without waiting for any of the legal changes needed to harmonize them with any other countries' laws. Nonetheless, the US and some other governments have, after the fact, sought to modify existing data protection rules and industry standards to mandate– or failing that, at least to permit – government access to PNR data in order to attempt to identify "suspicious" travelers.

Currently, only the United States, Canada, Australia and New Zealand have legislation in place that makes government access to airline reservation data mandatory. A number of other States are exploring this process.[17]

---

immigration and customs procedures, and providing such facilitating data to government agencies." The standard contract terms in IATA Recommended Practice 1724, General Conditions of Carriage (Passenger and Baggage), Article 5.3, Personal Data, grant even broader permission for airlines to transfer reservation data to government agencies: "You recognise that personal data has been given to us for the purposes of . . . making available such data to government agencies, in connection with your travel. For these purposes, you authorise us to retain and use such data and to transmit it to . . . government agencies."

15 John Schwartz and Micheline Maynard, "F.B.I. Got Records on Air Travelers", New York Times, May 1st, 2004, available at <http://www.nytimes.com/2004/05/01/politics/01AIRL.html>; American Airlines, "American Airlines Passenger Data Released In June 2002," press release, April 9, 2004, available at <http://www.amrcorp.com/news/april04/09_aai.htm>; Electronic Privacy Information Center (EPIC), Northwest Airlines' Disclosure of Passenger Data to Federal Agencies <http://www.epic.org/privacy/airtravel/nasa/>; US Senate Committee on Governmental Affairs, Pre-hearing Questionnaire for the Nomination of Admiral David Stone to be Assistant Secretary of Homeland Security, Transportation Security Administration, June 24, 2004, answer to question 16 available at <http://govt-aff.senate.gov/_files/062304stone_q16.pdf>; *see also* responses to additional questions http://www.epic.org/privacy/airtravel/stone_answers.pdf; Hasbrouck, "Total Travel Information Awareness" (last updated 25 June 2004), http://hasbrouck.org/articles/travelprivacy.html#testing.

16 General Accounting Office, Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges, GAO-04-385, February 12, 2004, available at <http://www.gao.gov/cgi-bin/getrpt?GAO-04-385.pdf>.

17 Airline Reservation System and Passenger Name Record (PNR) Access by States, Working Paper FAL/12-WP/74, presented by IATA to the 12th Session of the ICAO Facilitation (FAL) Division, Cairo, March 15, 2004, available at <http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp074_en.pdf>.

In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) was amended in 2001 by Bill C-44 to allow Canadian airlines to provide foreign governments with "any information . . . relating to persons on board or expected to be on board the aircraft and that is required by the laws of the foreign state."[18] The PIPEDA was further amended in 2004 by Bill C-7 to expand the exemption of travel data.[19] Bill C-7 in particular provoked considerable criticism, including opposition from the Canadian Bar Association.[20] Both bills were widely characterized as Canada's counterparts to the USA PATRIOT Act. In May 2004, the European Commission approved a conditional finding that the level of protection afforded to PNR data transferred to the US Department of Homeland Security (DHS) Bureau of Customs and Border Protection (CBP) satisfies the standard of "adequacy" required by the EU Data Protection Directive,[21] on the basis of which the Council of the European Community signed an agreement purporting to authorize PNR transfers to the US, if certain conditions were met.[22]

The finding of adequacy was contrary to the formal opinion of the working party of EU national data protection officers.[23] Both the agreement and the finding of adequacy of protection of PNR data in the US prompted extraordinary public controversy within the EU and conflict between EU institutions. Both were denounced by privacy advocates on both sides of the Atlantic.[24] In June 2004, the President of the European Parliament moved the Court of Justice of the European

---

18 An Act to Amend the Aeronautics Act, S.C. 2001, c.38, enacted December 18, 2001, available at <http://laws.justice.gc.ca/en/2001/38>.

19. Public Safety Act, 2002 (enacted 6 May 2004), available at <http://www.parl.gc.ca/37/3/parlbus/chambus/house/bills/government/C-7/C-7_3/C-7TOCE.html>.

20. F. William Johnson, President, Canadian Bar Association, Letter to the Senate Committee on Transport and Communications, March 17, 2003 <http://www.cba.org/CBA/submissions/pdf/04-09-eng.pdf>; *also see generally* Office of the Privacy Commissioner of Canada, Key Issues – Advance Passenger Information/Passenger Name Record <http://www.privcom.gc.ca/keyIssues/ki-qc/mc-ki-api_e.asp>.

21 Commission Decision of 14 May 2004 on the Adequate Protection of Personal Data Contained in the Passenger Name Record of Air Passengers Transferred to the United States' Bureau of Customs and Border Protection, available at <http://europa.eu.int/comm/internal_market/privacy/docs/adequacy/pnr/c-2004-1914/c-2004-1914_en.pdf>.

22 Council Decision of 17 May 2004 on the Conclusion of an Agreement Between the European Community and the United States of America on the Processing and Transfer of PNR Data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, 2004/496/EC, Official Journal L/2004/183/83, May 20, 2004, available at <http://europa.eu.int/cgi-bin/eur-lex/udl.pl?REQUEST=Seek-Deliver&LANGUAGE=en&SERVICE=eurlex&COLLECTION=oj&DOCID=2004l183p00830083>; Agreement Between the European Community and the United States of America on the Processing and Transfer of PNR Data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, Official Journal L/2004/183/84, May 20, 2004, available at <http://europa.eu.int/cgi-bin/eur-lex/udl.pl?REQUEST=Seek-Deliver&LANGUAGE=en&SERVICE=eurlex&COLLECTION=oj&DOCID=2004l183p00840085>.

23 Article 29 Data Protection Working Party, Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP), January 29, 2004, available at <http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp87_en.pdf>.

24 Privacy International, *et al.*, Transferring Privacy: The Transfer of Passenger Records and the Abdication of Privacy Protection; The First Report on "Towards an International Infrastructure for Surveillance of Movement", with a Commentary from the American Civil Liberties Union on "A Perspective from America", February 2004 <http://www.privacyinternational.org/issues/terrorism/rpt/transferringprivacy.pdf>; Trans Atlantic Consumer Dialogue (TACD) , Resolution on Passenger Name Records, Doc No. Internet-30-04, June 2004 <http://www.tacd.org/docs/?id=254>, also available with list of endorsers and supporting references at <http://www.thepublicvoice.org/take_action/pnr-resol-action.html>; *also see generally* Statewatch, Observatory on the Exchange of Data on Passengers (PNR) with USA <http://www.statewatch.org/pnrobservatory.htm>; EPIC, EU-US Airline Passenger Data Disclosure <http://www.epic.org/privacy/intl/passenger_data.html>; Hasbrouck, "Privacy and Travel", The Practical Nomad blog <http://hasbrouck.org/blog/archives/cat_privacy_and_travel.html>.

Communities, on behalf of the Parliament, to annul both the agreement and the adequacy finding.[25]

The stated goal of the US government is the adoption of permanent international standards overriding existing national data protection laws, and mandating access to PNR data by all governments worldwide.[26]

New Measures for Tracking and Monitoring of Travelers

In addition to seeking access to existing PNR's, some governments have sought to require data in PNRs beyond that which would otherwise be entered for commercial purposes; to modify PNR formats to facilitate desired government uses of PNR data; and/or to require airlines to transmit additional Advance Passenger Information (API) data collected solely to satisfy government demands.[27] While API data is typically described as corresponding to the information that could already be gleaned from travelers' tickets and passports, the majority of the categories of PNR and API data sought by the US cannot be obtained from current travel documents.[28]

These governmental initiatives have been led primarily by the US and, within the EU, by Spain.[29] In April 2004, a Spanish proposal that all airlines operating to, or within, the EU be required to collect and transmit to the governments of destination countries information concerning all passengers, was adopted by the Council of the European Union over the objections of the European Parliament committees that had considered it.[30]

Canadian customs and immigration agencies have developed and deployed their own airline reservation profiling software and algorithms, but use "risk management criteria that are common to both countries" to determine what travel data to share with the US.[31]

---

25 "European Parliament Asks Court of Justice to Annul EU-US Passenger Data Deal," June 25, 2004) <http://europa.eu.int/ISPO/ida/jsps/index.jsp?fuseAction=showDocument&documentID=2655&parent=chapter&preChapterID=0-140-194>.

26 For fiscal year 2004, the goal is "to negotiate an agreement with the EU that gives CBP and TSA permanent access to PNR data," and for fiscal year 2005 to "[e]nsure access to PNR data for border and passenger screening on a global basis" as, "Opinions by the public and political leadership in Europe and Eurasia soften on US government] use of PNR." US Department of State, "FY 2005 Performance Summary, Strategic Goal 3: Secure the Homeland by Strengthening Arrangements that Govern the Flows of People, Goods, and Services Between the United States and the Rest of the World," February 2004 <http://www.state.gov/m/rm/rls/perfplan/2005/html/29302.htm>.

27 Advance Passenger Information (API) – A Statement of Principles, Working Paper FAL/12-WP/60, presented by IATA to the 12th Session of the ICAO FAL Division, Cairo, March 10, 2004), available at <http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp060_en.pdf>.

28 Hasbrouck, "'Undertakings' by the USA on Use of Reservation Data", February 2, 2004 <http://hasbrouck.org/blog/archives/000131.html>.

29 Council of the European Union, Initiative of the Kingdom of Spain with a View to Adopting a Council Directive on the Obligation of Carriers to Communicate Passenger Data, January 9, 2004, available at <http://register.consilium.eu.int/pdf/en/04/st05/st05183.en04.pdf>; *also see generally* <http://www.statewatch.org/eu-pnrobservatory.htm>.

30 Council Directive on the obligation of carriers to communicate passenger data, April 27, 2004, available at <http://www.statewatch.org/news/2004/apr/8078pnr.pdf>.

31 Canadian Advance Passenger Information Program, Working Paper FAL/12-WP/38, presented by Canada to the 12th Session of the ICAO FAL Division, Cairo, December 11, 2003, available at <http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp038_en.pdf>.

Australia has mandated that all airlines provide the government with continuous real-time access to their reservations systems, and has implemented an automated profiling system, based on certain elements of PNR and API data, which selects certain reservations for review and possible action by customs officers.[32]

In New Zealand, government access to PNR and API data has been limited to international flights, and law enforcement authorities have used the advance passenger processing system developed by Australia. The New Zealand government has sought, but has not yet obtained, legal authority to issue "do not board" orders to airlines on the basis of automated analysis of PNR and API data.[33]

The US has imposed a requirement for collection and automated transmission of API data on all international flights to the US, and has pursued multilateral agreements on API data transfers with the EU (as part of the PNR agreement), the G-8[34] and, globally, through ICAO.

The model for the global travel data regime sought by the US is the Computer Assisted Passenger Screening System, version 2 (CAPPS-II) that was proposed by the US government for flights to, from, and within the US

In July 2004, the US government announced its intention to dismantle the CAPPS-II program. Department of Homeland Security Secretary Tom Ridge said that privacy concerns surrounding the pilot program coupled with ongoimng Congressional doubts about the effectiveness of the program contributed to the decision. When asked whether the program could be considered "dead," Ridge answered "yes."[35]

However, civil liberties organizations and air travel experts expressed skepticism about the announcement. Some said that CAPPS was simply being renamed or merged into other programs, and that the US government would continue to pursue its essential functionality: mandatory identification of all air travelers, entry of identifying data into reservations, and government access to those reservations.[36] These goals were also endorsed later that month by the "9/11 Commission" in the US, whose first recommendation for how to "protect against terrorist attacks" was "targeting travel" and expanding "travel intelligence collection," *i.e.* surveillance of travelers.[37]

---

[32] Article 29 Data Protection Working Party, Opinion 1/2004 on the level of protection ensured in Australia for the transmission of Passenger Name Record data from airlines, January 16, 2004, available at <http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp85_en.pdf>.

[33] Introduction of Advance Passenger Screening (APS) in New Zealand, Working Paper FAL/12-WP/81, presented by Canada to the 12th Session of the ICAO FAL Division, Cairo, March 20, 2004, available at <http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp081_en.pdf>.

[34] "G-8 Secure and Facilitated International Travel Initiative (SAFTI)," White House press release, June 9, 2004 <http://www.whitehouse.gov/news/releases/2004/06/20040609-51.html>.

[35] Mimi Hall & Barbara DeLolli, "Plan to Collect Flier Data Canceled," USA Today, July 14, 2004, available at http://www.usatoday.com/news/washington/2004-07-14-fly-plan_x.htm.

[36] Hasbrouck, "CAPPS-II Is Dead. Long Live CAPPS-II!" <http://hasbrouck.org/blog/archives/000282.html>.

[37] Final Report of the National Commission on Terrorist Attacks Upon the United States, Chapter 12: What to do? A Global Strategy, July 22, 2004, available at <http://www.9-11commission.gov/report/911Report_Ch12.pdf>. (The 9/11 Commission also endorsed the proposed ICAO standard for RFID/biometric passports and the US-VISIT program, among other travel surveillance schemes).

The US has sought permission from other countries including the EU and Canada for use of data collected in those countries for CAPPS-II.[38] The "Undertakings" by the US, which were a condition for the European Commission's finding of adequacy of passenger data protection in the US, specifically declare that the US may use data from the EU in CAPPS-II tests,[39] although that authorization refers specifically to "CAPPS-II," and thus may be invalidated by the change of the program's name.

CAPPS-II or its successor would be a system of automated identity- and reservation-based profiling unlike any other airline passenger screening or security system in the world.[40] CAPPS-II would profile each passenger and assign them a risk or "suspiciousness" score on the basis of their identity as determined from their PNR. That will not be possible unless each passenger (a) is identified, (b) has a reservation, and (c) has sufficient information entered in their reservation to identify them uniquely. CAPPS-II will therefore have the effect of prohibiting anonymous or unreserved travel, and mandating entry of specified identifying information about each passenger in his or her PNR.[41]

The US has proposed to use secret security directives to impose both the requirement for travelers to display evidence of their identity and the requirement for airlines and travel agents to create a PNR containing specified identifying information for each traveler, concealing the details of the requirements from the public and frustrating judicial review.[42]

As the US Communications Assistance to Law Enforcement Act (CALEA) did with the infrastructure of transport of information, CAPPS-II and other government travel security initiatives would require the embedding of "intelligence gathering" capabilities into the infrastructure of transportation of people, imposing as an unfunded mandate on the travel industry whatever changes, at whatever cost, are required to provide that surveillance functionality. Even airlines that support CAPPS-II have been concerned about the cost of the changes it would require to reservation data structures, messaging formats and protocols, and business procedures worldwide, especially if those costs are not reimbursed by governments.[43] While the US government has suggested that it might cut back on the use of other, non-travel commercial databases in the profiling component of its revised and/or renamed successor to CAPPS-II, the

---

38 Chris Strohm, "US, Canada Launch Talks on Sharing Citizen Data," GovExec.com, January 30, 2004 <http://www.govexec.com/dailyfed/0104/013004c1.htm>.

39 Commission Decision of 14 May 2004, *supra*.

40 Hasbrouck, "What's Wrong With CAPPS-II? (And What Should Be Done about It?)" (last updated June 25, 2004) <http://hasbrouck.org/articles/CAPPS-II.html>.

41 Hasbrouck, "CAPPS-II Will Require 3 New Directives," December 10, 2003) <http://hasbrouck.org/blog/archives/000084.html>.

42 Gilmore v. Ashcroft, Case No. C-02-3444 SI (N.D. Cal., filed July 18, 2002), case documents available at <http://www.freetotravel.org/legal.html>; Frontier Travel v. TSA, (D. Alaska, filed May 24, 2004), case documents available at <http://www.alaskafreedom.com/akn/case.html>.

43 IATA, Airline Reservation System and Passenger Name Record (PNR) Access by States, *supra*; Advance Passenger Information (API) – A Statement of Principles, Working Paper FAL/12-WP/60, *supra*; James C. May, President and CEO, Air Transport Association (ATA), Testimony Before the US Senate Committee on Commerce, Science, and Transportation at a Hearing on Aviation Security, June 22, 2004, available at <http://commerce.senate.gov/hearings/testimony.cfm?id=1245&wit_id=1923>; May, Status of the Computer Assisted Passenger Prescreening System ("CAPPS II"), Testimony Before the Aviation Subcommittee of the House Committee on Transportation and Infrastructure, March 17, 2004, available at <http://www.house.gov/transportation/aviation/03-17-04/may.html>; Hasbrouck, "Why CAPPS-II Would Cost a Billion Dollars", February 13, 2004 <http://hasbrouck.org/blog/archives/000149.html>; Hasbrouck, Comments Re: Docket Number DHS/TSA-2003-1, "Passenger and Aviation Security Screening Records" (PASSR), September 30, 2003, available at <http://hasbrouck.org/articles/Hasbrouck_TSA_comments-30SEP2003.pdf>.

intelligence gathering component and its required changes to airline databases would remain as extensive and costly as ever.

CAPPS-II would incorporate existing US "no-fly" and other airline passenger "watch lists." As part of its international initiatives for government access to, and trans-border sharing of, PNR and API data, the US government has sought to establish a global system for exchanges of traveler watch list information, and to exempt it from requirements of disclosure, due process, and judicial review.[44] PNR data obtained through CAPPS-II would also be included in the lifetime "biographic and biometric travel history" created and maintained on each foreign visitor to the US under the US-VISIT system.[45]

The information required by CAPPS-II would be, by design, the information needed to ensure that all passengers can be uniquely identified from reservations, and, as a result, that reservations for separate trips can be indexed into lifetime travel histories. Under CAPPS-II, travel companies in the US, including the CRSs which host most airline reservations, would be permitted to retain all of this information indefinitely after passing it on governments, and use it to construct their own permanent files on travelers. These records could be accessed by government agencies at any time, even if the government itself did not retain the CAPPS-II data.

Secure Flight

On August 26, 2004, The Department of Homeland Security's Assistant Secretary for the Transportation Security Administration David Stone announced that the government would begin testing Secure Flight, its new passenger prescreening system, in November. Admiral Stone stated that commercial airlines would be ordered in September to turn over "historical" PNR data for TSA to use in the testing phase of Secure Flight.[46]

The new program, slated for deployment early next year, will focus on comparing Passenger Name Records (PNRs) against expanded "selectee" and "no fly" lists maintained by the government. If a traveler's PNR matches information on a watch list, commercial data aggregators will be relied upon to verify the traveler's identity. TSA will administer the program, removing all passenger screening responsibility from the airlines.

Though TSA plans to implement a redress process for travelers improperly flagged by Secure Flight, it is unclear how this process will work. The government has long used "selectee" and "no fly" lists for aviation security purposes, but passengers have experienced great difficulty clearing their names when improperly flagged. In 2002, EPIC obtained through the Freedom of Information Act dozens of complaint letters sent to TSA by irate passengers who felt they had been incorrectly identified for additional security or were denied boarding because of the watch

---

[44] EPIC, "Documents Show Errors in TSA's 'No-Fly' Watchlist", April 2003 <http://www.epic.org/privacy/airtravel/foia/watchlist_foia_analysis.html>; ACLU, "ACLU Challenges Government No-Fly List" <http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=15422&c=206>; ACLU, "ACLU Seeks Government Accountability For No-Fly List" <http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=15422&c=206>.

[45] Hasbrouck, "USA Will Keep Visitor Travel Histories for 100 Years" <http://hasbrouck.org/blog/archives/000103.html>.

[46] EPIC Alert 11.16[1], August 27, 2004, available at http://www.epic.org/alert/EPIC_Alert_11.16.html.

lists. The complaints describe the bureaucratic maze passengers encounter if they happen to be mistaken for individuals on the list, as well as the difficulty they encounter trying to exonerate themselves.[47]

Biometric Passports

Foreign visitors will be required to identify themselves with passports satisfying ICAO machine-readable travel document (MRTD) standards,[48] which may also include secretly and remotely readable RFID chips containing digitally encoded biometric data.[49] US travelers will be allowed to obtain "registered travel" tokens or credentials only by having biometric data recorded, and by submitting to a background check of government and commercial databases.[50] The motivation to register can only be that unregistered travelers will be subjected to longer delays and/or more intrusive searches and screening.[51]

Although the overwhelming emphasis has been on air travel, some of these measures and others are now being extended to other transportation modes, starting with trains and buses. Already intercity train and bus passengers in the US are required to display "valid photo identification" to purchase tickets and on boarding.[52]

A government-required RFID/biometric Transportation Worker Identification Credential (TWIC) is being tested for eventual issuance to more than 10 million workers in transportation facilities in the US, including airports, seaports, rail and truck terminals, etc.[53] The TWIC was, however, intended in the future to identify all users of transportation systems, *i.e.* travelers.[54] Eventually, all persons on transportation vehicles or in transportation facilities may be required to carry government-issued RFID/biometric identification credentials.

---

47 *See* EPIC FOIA documents on "selectee" and "no fly" watch lists, available at <http://www.epic.org/redirect/watchlist_foia.html>. *See generally*, EPIC, "Passenger Profiling Page," available at <http://www.epic.org/privacy/airtravel/profiling>.

48 Enhanced Border Security and Visa Entry Reform Act of 2002, Pub. L. No. 107-173, Sec. 303(b)(1); Machine Readable Travel Documents, ICAO Doc. 9303 (Montreal, 5th ed. 2003); *also see generally* ICAO New Technologies Working Group, Technical Reports <http://www.icao.int/mrtd/download/technical.cfm>.

49. ICAO, Report of the Twelfth Session of the Facilitation (FAL) Division (Cairo, Egypt, 22 March – 1 April 2004) <http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12Report_en.pdf>; Privacy International, ACLU, *et al.*, An Open Letter to the ICAO: A Second Report on "Towards an International Infrastructure for Surveillance of Movement," March 30, 2004 <http://www.privacyinternational.org/issues/terrorism/rpt/icaoletter.pdf>; Barry Steinhardt, Witness Testimony at the hearing on "Radio Frequency Identification (RFID) Technology: What the Future Holds for Commerce, Security, and the Consumer," Subcommittee on Commerce, Trade, and Consumer Protection, Committee on Energy and Commerce, US House of Representatives, July 14, 2004, available at <http://energycommerce.house.gov/108/Hearings/07142004hearing1337/Steinhardt2150.htm>; *also see generally* Privacy International, About the Open Letter to the ICAO, March 2004 <http://www.privacyinternational.org/issues/terrorism/rpt/icaobackground.html>; ICAO, Twelfth Meeting of the Facilitation Division (Cairo, 22 March 2004 - 1 April 2004) <http://www.icao.int/icao/en/atb/fal/fal12/>; ICAO Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD) <http://www.icao.int/mrtd/>.

50 TSA, Registered Traveler Pilot Combined Synopsis Solicitation, HSTS02-04-R-RET002, posted April 5, 2004, available at <http://www.eps.gov/EPSData/DHS-BT/Synopses/35287/HSTS02-04-R-RET002/RTCSSFinal.doc>.

51 The travel industry "Simplifying Passenger Travel" initiative has been developing and testing, in several countries, schemes for biometric/RFID credentials that could be used for both commercial and government functions. These combine elements of the functionality of electronic tickets, boarding passes, ticket payment credit or debit cards, frequent flyer cards, and registered traveler identification credentials. Simplifying Passenger Travel Interest Group <http://www.simplifying-travel.org>.

52 *E.g.*, Amtrak, Important Information About Amtrak Passenger Security available at <http://www.amtrak.com/idrequire.html>.

53 TSA TWIC Program <http://www.tsa.gov/public/display?theme=68>; Hasbrouck, Transportation Worker Identification Credential (TWIC), April 6, 2004 <http://hasbrouck.org/blog/archives/000189.html>.

54 US Dept. of Transportation, Credentialing Direct Action Group, National Transportation Worker ID Card (TWIC) Functional Requirements Draft, January 23, 2002, available at <http://www.apta.com/government_affairs/regulations/documents/workerid.pdf>.

The Case of US-VISIT: a New Tool for Monitoring Travelers

The Department of Homeland Security deployed the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) at 115 airports and 15 major seaports on January 5, 2004.[55] When this practice began, the general response was one of shock and alarm. Brazil, China, Greece[56] and Switzerland[57] were among countries that protested against their citizens being fingerprinted by the Department of Homeland Security. Brazil even threatened reciprocity.[58]

This border security program is intended to improve the United States' capability to collect information about foreign nationals who travel to the US, as well as control the pre-entry, entry, status, and exit of these travelers. US-VISIT is expected to be operational at every US air, land and seaport by the end of 2005.[59] Some information in US-VISIT will be kept for 100 years,[60] and all information may be disclosed to any law enforcement agency in the US and any other country.[61]

When a visitor subject to US-VISIT applies for a visa to travel to the US, he is fingerprinted and photographed at an overseas US consular office.[62] This biometric information is then checked against more than 20 interfacing government databases to determine the likelihood that the visitor is a criminal or terrorist.[63] When the visitor arrives at a US port of entry, he is again fingerprinted and photographed to verify that he is the same person who was issued the visa.[64] The program will eventually be expanded to fingerprint visitors when they exit the US, as well.[65]

US-VISIT did not apply to visitors to the US traveling through the Visa Waiver Program until September 20, 2004 when the program was expanded, the program was expanded to include Visa Waiver travelers arriving at air and seaports.[66] The general response to this expansion of US-VISIT was very quiet, possibly because the enlargement of the program was a result of the proposed extension of the biometric passport deadline.[67] If any Visa Waiver program countries do not implement biometric passports by October 2004, US law requires that these countries be removed from the Visa Waiver program, resulting in all nationals being forced to get visas.

---

55 Department of Homeland Security, Travel & Transportation: US-VISIT <http://www.dhs.gov/dhspublic/interapp/content_multi_image/content_multi_image_0006.xml/>; *see also* EPIC's US-VISIT web page <http://www.epic.org/privacy/us-visit/>.

56 Kathiminerini English Edition, "New Twist in US Visa Process," May 6, 2004.

57 Swissinfo, "Swiss Criticize Tougher US Border Checks," April 5, 2004.

58 Raymond Colitt, "Brazil Stands Firm on Fingerprinting of US Visitors," Financial Times, January 12, 2004.

59 Department of Homeland Security, Travel & Transportation: US-VISIT <http://www.dhs.gov/dhspublic/interapp/content_multi_image/content_multi_image_0006.xml/>.

60 Notice of Privacy Act System of Records, 68 Fed. Reg. 69412 (December 12, 2003).

61 Interim Final Rule and Notice, 69 Fed. Reg. 467 (January 5, 2004). *See also* US-VISIT Program, Increment 1, Privacy Impact Assessment, December 18, 2003, at 6, 13, available at <http://www.dhs.gov/interweb/assetlibrary/VISITPIAfinal3.pdf>.

62 Department of Homeland Security, Travel & Transportation: US-VISIT, *supra*.

63 Interim Final Rule and Notice, 69 Fed. Reg. 476 (January 5, 2004).

64 Department of Homeland Security, Travel & Transportation: US-VISIT <http://www.dhs.gov/dhspublic/interapp/content_multi_image/content_multi_image_0006.xml/>.

65 *Id*.

66 *Id*.

67 Press Office, "Departments of Homeland Security and State Request Extension for Biometric Passport Requirement, Visa Waiver Program Travelers to Be Enrolled in US-VISIT," Department of Homeland Security, April 2, 2004.

Earlier, the Department of Homeland Security indicated that it intended to link CAPPS II and US-VISIT when both programs are fully operational to ensure that "the processes at both border and airport points of entry and exit are consistent."[68] It is likely that US-VISIT will now be linked with Secure Flight.

Other countries are considering similar systems now that the US has expanded US-VISIT. The EU has proposed a similar system involving fingerprints, enhanced by the fact that EU countries will also have fingerprint-based biometric passports, creating a database of biometrics on over 450 million people.

Key Developments Threatening Travel Privacy

- Lack of enforceable legal protection for travel data comparable to that for financial, medical, or other sensitive categories of personal information
- Government demands for access to reservations and other commercial travel data and exemption of travel-related data from existing privacy and data protection regulations
- Compulsory identification of travelers (through biometrics, compulsory carrying or display of credentials, etc.) and compulsory entry of identifying data into reservations
- Indexing of reservations and travel transactions into lifetime personal travel dossiers
- Inclusion of secretly and remotely readable RFID chips in passports, tickets, "registered traveler" credentials, or other travel documents
- Profiling of travelers, denial of freedom of travel, slower or more intrusive searches, or other differential treatment of travelers on the basis of watch lists, profiles, or as a "registered traveler" status
- Integration of commercial and government databases about travelers; integration and conversion of travel industry infrastructure into an infrastructure of surveillance

[68] Interim Final Privacy Act Notice, 68 Fed. Reg. 45265 (August 1, 2003).