

## Travel Privacy

Since 11 September 2001, one of the greatest fears of security officials in the U.S. has been that would-be terrorists would board commercial airline flights without their malicious intentions being detected in advance. As a result, a high priority has been placed 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 mandatory government access to reservations and other travel data already 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,<sup>1</sup> and it's not clear that these policy and procedural changes are the outcome of a considered evaluation of risks, benefits, and trade-offs.<sup>2</sup> 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 will -- 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 and government protections for travel data fail to provide the level of protection provided for other categories of data, and required by the general principles of fair information practices.

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.<sup>3</sup>

---

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

<sup>2</sup> Bruce Schneier, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World* (New York 2003).

<sup>3</sup> Hasbrouck, "What's In A Passenger Name Record (PNR)?" (last updated 25 June 2004), <<http://hasbrouck.org/articles/PNR.html>>.

A Passenger Name Record (PNR) typically contains names of travelers and details of flights, hotels, car rentals, and other travel services. PNR's 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, PNR's contain information about memberships and organizational affiliations. Since a single PNR typically is used for an entire travel party, PNR's contain detailed information on patterns of association between travelers. PNR's can contain religious meal preferences and special service requests that describe intimate details of physical and medical conditions ("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 such as the ATA/IATA Reservations Interline Message Procedures - Passenger (AIRIMP)<sup>4</sup> 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 PNR's are "purged" from live to archival storage systems, and can be retained indefinitely by CRS's, 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. Prior to September 11, 2001, neither privacy advocates and data protection authorities nor government surveillance and security agencies had made travel records a priority. PNR's and ticketing records have 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 U.S., for example, most consumer privacy policies are enforced by state and local consumer protection authorities and the Federal Trade Commission. But enforcement of privacy policies by airlines and travel agencies, and of compliance by airlines and travel agencies with the Safe Harbor arrangement on data protection with the EU, 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.

---

<sup>4</sup> 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](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](http://www.iata.org/idfs/ps/passenger_standards/reservations_standards_rescom.htm)>.

The International Civil Aviation Organization (ICAO) has adopted a model Code of Conduct on the Regulation and Operation of Computer Reservation Systems (CRS), including the following 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.<sup>5</sup>

However, the ICAO Code of Conduct on the Regulation and Operation of Computer Reservation Systems has not been widely adopted by ICAO member states. CRS's operate under government regulations in the U.S.<sup>6</sup> and Canada<sup>7</sup>, 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."<sup>8</sup> 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 CRS's.

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 CRS's. Even if followed, the IATA recommendations serve more to legitimate than to limit airlines' transfers of passenger data to government agencies. 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 immigration and customs procedures, and providing such facilitating data

---

<sup>5</sup> ICAO Code of Conduct on the Regulation and Operation of Computer Reservation Systems (CRS), adopted by the Council of ICAO 25 June 1996, effective 1 November 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>>.

<sup>6</sup> Computer Reservations System (CRS) Regulations, 14 CFR Part 255, 69 FR 975 (7 January 2004), available at <<http://www.dot.gov/affairs/Computer%20Reservations%20System.htm>>.

<sup>7</sup> Canadian Computer Reservation Systems (CRS) Regulations, SOR/95-275 (6 June 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 (23 October 2003), available at <<http://canadagazette.gc.ca/part1/2003/20031025/html/regle15-e.html>>.

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

to government agencies".<sup>9</sup> 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.

### *Privacy of Travel Records Since 11 September 2001*

Almost immediately after 11 September 2001, airlines and the U.S. government -- often in collaboration, and of necessity involving the CRS's in their work -- began accessing and using archived PNR's to investigate the hijackings and to test the possibility of identifying "suspicious" travelers through PNR profiling. Most of the major U.S.-based airlines and CRS's, and a variety of U.S. government agencies and contractors, were involved in these investigations and experiments over the next two years.<sup>10</sup> 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 Freedom of Information Act (FOIA) requests and lawsuits, Congressional questioning, investigative journalism, and admissions by airlines.

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.<sup>11</sup> It's impossible to identify from a PNR in what country(s) the data it contains was collected, so each of these tests probably included data subject to many international jurisdictions. The U.S. government proceeded with these tests without waiting for any of the legal changes needed to harmonize them with any other countries' laws. Nonetheless, the U.S. 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.

---

<sup>9</sup> Note to Article 3.1.2; included as Annex 1 to Working Document on IATA Recommended Practice 1774, Article 29 Data Protection Working Party, 5032/01/EN/Final WP 49 (14 September 2001), available at <[http://europa.eu.int/comm/internal\\_market/privacy/workinggroup/wp2001/wpdocs01\\_en.htm](http://europa.eu.int/comm/internal_market/privacy/workinggroup/wp2001/wpdocs01_en.htm)>. Note that IATA is a trade association representing member airlines, and ICAO is an international treaty organization representing national member governments.

<sup>10</sup> Hasbrouck, "Total Travel Information Awareness" (last updated 25 June 2004), <<http://hasbrouck.org/articles/travelprivacy.html#testing>>; John Schwartz and Micheline Maynard, "F.B.I. Got Records on Air Travelers", New York Times, 1 May 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, 9 April 2004), available at <[http://www.amrcorp.com/news/april04/09\\_aai.htm](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/>>; U.S. 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 (24 June 2004), answer to question 16 available at <[http://govt-aff.senate.gov/\\_files/062304stone\\_q16.pdf](http://govt-aff.senate.gov/_files/062304stone_q16.pdf)>; see also responses to additional questions, <[http://www.epic.org/privacy/airtravel/stone\\_answers.pdf](http://www.epic.org/privacy/airtravel/stone_answers.pdf)>.

<sup>11</sup> General Accounting Office, Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges, GAO-04-385, 12 February 2004, available at <<http://www.gao.gov/cgi-bin/getrpt?GAO-04-385.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."<sup>12</sup> The PIPEDA was further amended in 2004 by Bill C-7 to expand the exemption of travel data.<sup>13</sup> Bill C-7 in particular provoked considerable criticism, including opposition from the Canadian Bar Association.<sup>14</sup> 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 U.S. Department of Homeland Security (DHS) Bureau of Customs and Border Protection (CBP) satisfies the standard of "adequacy" required by the EU Data Protection Directive,<sup>15</sup> on the basis of which the Council of the European Community signed an agreement purporting to authorize PNR transfers to the U.S., if certain conditions were met.<sup>16</sup>

The finding of adequacy was contrary to the formal opinion of the working party of EU national data protection officers.<sup>17</sup> Both the agreement and the finding of adequacy of protection of PNR data in the U.S. prompted extraordinary public controversy within the EU and conflict between

---

<sup>12</sup> An Act to Amend the Aeronautics Act, S.C. 2001, c.38 (enacted 18 December 2001), available at <<http://laws.justice.gc.ca/en/2001/38>>.

<sup>13</sup> 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](http://www.parl.gc.ca/37/3/parlbus/chambus/house/bills/government/C-7/C-7_3/C-7TOCE.html)>.

<sup>14</sup> F. William Johnson, President, Canadian Bar Association, Letter to the Senate Committee on Transport and Communications, 17 March 2003, <<http://www.cba.org/CBA/submissions/pdf/04-09-eng.pdf>>

<sup>15</sup> 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](http://europa.eu.int/comm/internal_market/privacy/docs/adequacy/pnr/c-2004-1914/c-2004-1914_en.pdf)>.

<sup>16</sup> 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, available at <<http://europa.eu.int/cgi-bin/eur-lex/udl.pl?REQUEST=Seek-Deliver&LANGUAGE=en&SERVICE=eurlex&COLLECTION=oj&DOCID=20041183p00830083>>; 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, available at <<http://europa.eu.int/cgi-bin/eur-lex/udl.pl?REQUEST=Seek-Deliver&LANGUAGE=en&SERVICE=eurlex&COLLECTION=oj&DOCID=20041183p00840085>>.

<sup>17</sup> 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), 29 January 2004, available at <[http://europa.eu.int/comm/internal\\_market/privacy/docs/wpdocs/2004/wp87\\_en.pdf](http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp87_en.pdf)>.

EU institutions. Both were denounced by privacy advocates on both sides of the Atlantic.<sup>18</sup> In June 2004, the President of the European Parliament moved the EU Court of Justice, on behalf of the Parliament, to annul both the agreement and the adequacy finding.<sup>19</sup>

The goal of the U.S. for fiscal year 2004 is "to negotiate an agreement with the EU that gives CBP and TSA [Transportation Security Administration] permanent access to PNR data," and for fiscal 2005 to "Ensure 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 USG [U.S. government] use of PNR".<sup>20</sup>

According to IATA:

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 ..., and it is likely that more such requirements will be imposed in the coming two years....

There is a consensus within the industry that access to PNR data by any government agency is in fact an intelligence gathering operation.... Accordingly, the air transport industry firmly supports the premise that the costs associated with access to airline reservation data should be borne solely by the government(s) requesting those data.<sup>21</sup>

### *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 PNR's 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

---

<sup>18</sup> 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](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](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](http://hasbrouck.org/blog/archives/cat_privacy_and_travel.html)>.

<sup>19</sup> "European Parliament Asks Court of Justice to Annul EU-US Passenger Data Deal" (25 June 2004), <<http://europa.eu.int/ISPO/ida/jsp/index.jsp?fuseAction=showDocument&documentID=2655&parent=chapter&preChapterID=0-140-194>>.

<sup>20</sup> U.S. 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>>.

<sup>21</sup> *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 (15 March 2004), available at <[http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp074\\_en.pdf](http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp074_en.pdf)>.

demands.<sup>22</sup> These initiatives have been led primarily by the U.S. and, within the EU, by Spain.<sup>23</sup> 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 U.S. cannot be obtained from current travel documents.<sup>24</sup>

The U.S. has imposed a requirement for collection and automated transmission of API data on all international flights to the U.S., and has pursued multilateral agreements on API data transfers with the EU (as part of the PNR agreement), the G-8<sup>25</sup>, and globally through ICAO.

The model for the global travel data regime sought by the U.S. is the Computer Assisted Passenger Screening System, version 2 (CAPPS-II) proposed by the U.S. for flights to, from, and within the U.S. The U.S. has sought permission from other countries including the EU and Canada for use of data collected in those countries for CAPPS-II.<sup>26</sup> The "Undertakings" by the U.S., which were a condition for the EC finding of adequacy of passenger data protection in the U.S., specifically declare that the U.S. may use data from the EU in CAPPS-II tests.<sup>27</sup>

CAPPS-II would be a system of automated identity- and reservation-based profiling unlike any other airline passenger screening or security system in the world.<sup>28</sup> 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 won't 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 require the prohibition of anonymous or unreserved travel, and mandatory entry of specified identifying information about each passenger in their PNR.<sup>29</sup>

The U.S. 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

---

<sup>22</sup> 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 (10 March 2004), available at <[http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp060\\_en.pdf](http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp060_en.pdf)>.

<sup>23</sup> 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, 9 January 2004, available at <<http://register.consilium.eu.int/pdf/en/04/st05/st05183.en04.pdf>>; also see generally <<http://www.statewatch.org/eu-pnrobbservatory.htm>>.

<sup>24</sup> Hasbrouck, "'Undertakings' by the USA on Use of Reservation Data", 2 February 2004, <<http://hasbrouck.org/blog/archives/000131.html>>.

<sup>25</sup> "G-8 Secure and Facilitated International Travel Initiative (SAFTI)", White House press release, 9 June 2004, <<http://www.whitehouse.gov/news/releases/2004/06/20040609-51.html>>.

<sup>26</sup> Chris Strohm, "U.S., Canada Launch Talks on Sharing Citizen Data", GovExec.com, 30 January 2004, <<http://www.govexec.com/dailyfed/0104/013004c1.htm>>.

<sup>27</sup> Commission Decision of 14 May 2004, *supra*, note 15.

<sup>28</sup> Hasbrouck, "What's Wrong With CAPPS-II? (And What Should Be Done about It?)" (last updated 25 June 2004), <<http://hasbrouck.org/articles/CAPPS-II.html>>.

<sup>29</sup> Hasbrouck, "CAPPS-II Will Require 3 New Directives" (10 December 2003), <<http://hasbrouck.org/blog/archives/000084.html>>.

create a PNR containing specified identifying information for each traveler, concealing the details of the requirements from the public and frustrating judicial review.<sup>30</sup>

As the U.S. 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.<sup>31</sup>

CAPPs-II would incorporate existing U.S. "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 U.S. 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.<sup>32</sup> 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 U.S. under the US-VISIT system.<sup>33</sup>

The information required by CAPPs-II is, by design, the information needed to ensure that all passengers can be uniquely identified from reservations, and thus that reservations for separate trips can be indexed into lifetime travel histories. Under CAPPs-II, travel companies in the U.S., including the CRS's which host most airline reservations, will 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 does not retain the CAPPs-II data.

---

<sup>30</sup> Gilmore v. Ashcroft, Case No. C-02-3444 SI (N.D. Cal., filed 18 July 2002), case documents available at <<http://www.freetotravel.org/legal.html>>; Frontier Travel v. TSA, (D. Alaska, filed 24 May 2004), case documents available at <<http://www.alaskafreedom.com/akn/case.html>>.

<sup>31</sup> IATA, *supra* notes 21 and 22; James C. May, President and CEO, Air Transport Association (ATA), Testimony Before the U.S. Senate Committee on Commerce, Science, and Transportation at a Hearing on Aviation Security, 22 June 2004, available at <[http://commerce.senate.gov/hearings/testimony.cfm?id=1245&wit\\_id=1923](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, 17 March 2004, available at <<http://www.house.gov/transportation/aviation/03-17-04/may.html>>; Hasbrouck, "Why CAPPs-II Would Cost a Billion Dollars", 13 February 2004, <<http://hasbrouck.org/blog/archives/000149.html>>; Hasbrouck, Comments Re: Docket Number DHS/TSA-2003-1, "Passenger and Aviation Security Screening Records" (PASSR), 30 September 2003, available at <[http://hasbrouck.org/articles/Hasbrouck\\_TSA\\_comments-30SEP2003.pdf](http://hasbrouck.org/articles/Hasbrouck_TSA_comments-30SEP2003.pdf)>.

<sup>32</sup> EPIC, "Documents Show Errors in TSA's 'No-Fly' Watchlist", April 2003, <[http://www.epic.org/privacy/airtravel/foia/watchlist\\_foia\\_analysis.html](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>>.

<sup>33</sup> Hasbrouck, "USA Will Keep Visitor Travel Histories for 100 Years", <<http://hasbrouck.org/blog/archives/000103.html>>.

Foreign visitors will be required to identify themselves with passports satisfying ICAO machine-readable travel document (MRTD) standards,<sup>34</sup> which are proposed to include secretly and remotely-readable RFID chips containing digitally encoded biometric data.<sup>35</sup> U.S. travelers will be allowed to obtain "registered traveler" tokens or credentials only by having biometric data recorded, and by submitting to a background check of government and commercial databases.<sup>36</sup> The motivation to register can only be that unregistered travelers will be subjected to longer delays and/or more intrusive searches and screening. 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.<sup>37</sup>

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 U.S. are required to display "valid photo identification" to purchase tickets and on boarding.<sup>38</sup>

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 U.S., including airports, seaports, rail and truck terminals, etc.<sup>39</sup> The TWIC was intended to "accommodate future needs to address identification of users of the transportation system," i.e. travelers.<sup>40</sup> Eventually, all persons on transportation vehicles or in transportation facilities may be required to carry government-issued RFID/biometric identification credentials.

---

<sup>34</sup> 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>>.

<sup>35</sup> 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](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", 30 March 2004, <<http://www.privacyinternational.org/issues/terrorism/rpt/icaoletter.pdf>>; *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/>>.

<sup>36</sup> TSA, Registered Traveler Pilot Combined Synopsis Solicitation, HSTS02-04-R-RET002, posted 5 April 2004, available at <<http://www.epsg.gov/EPSSData/DHS-BT/Synopses/35287/HSTS02-04-R-RET002/RTCSSFinal.doc>>

<sup>37</sup> Simplifying Passenger Travel Interest Group, <<http://www.simplifying-travel.org>>.

<sup>38</sup> e.g. Amtrak, Important Information About Amtrak Passenger Security, <<http://www.amtrak.com/idrequire.html>>.

<sup>39</sup> TSA TWIC Program, <<http://www.tsa.gov/public/display?theme=68>>; Hasbrouck, Transportation Worker Identification Credential (TWIC), 6 April 2004, <<http://hasbrouck.org/blog/archives/000189.html>>.

<sup>40</sup> U.S. Dept. of Transportation, Credentialing Direct Action Group, National Transportation Worker ID Card (TWIC) Functional Requirements Draft, 23 January 2002, available at <[http://www.apta.com/government\\_affairs/regulations/documents/workerid.pdf](http://www.apta.com/government_affairs/regulations/documents/workerid.pdf)>.

*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 or profiles
- Integration of commercial and government databases about travelers; integration and conversion of travel industry infrastructure into an infrastructure of surveillance

[Draft by Edward Hasbrouck for inclusion in Privacy and Human Rights 2004, forthcoming, Privacy International and the Electronic Privacy Information Center, London and Washington. This draft of 2 July 2004 is at <<http://hasbrouck.org/articles/PHR2004-travelprivacy-draft.pdf>>. Copyright ©2004 Edward Hasbrouck, <[edward@hasbrouck.org](mailto:edward@hasbrouck.org)>, <<http://hasbrouck.org>>.]