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'

Privacy International
In co-operation with
European Digital Rights Initiative, the Foundation for Information Policy Research, and Statewatch

With a Commentary from the American Civil Liberties Union on
A Perspective from America
February 2004

Transferring Privacy:

The Transfer of Passenger Records and the Abdication of Privacy Protection

February 2004

Summary

Among the many laws passed in the U.S. in the months after the terrorist attacks of September 11 2001, some have significant effects on other countries. This report outlines the case of passenger data records transfers; from the databases of EU carriers into the databases of the U.S. Department of Homeland Security.

These transfers create problems for the privacy protection of all affected people who are not *U.S. persons*. U.S. privacy law protects U.S. persons; EU privacy law protects personal data in the EU. Once this information is transferred to the U.S., U.S. law applies. The common practice of the European Commission is to establish an agreement on this transfer that includes, among other rights, clear constraints on the use, retention, and further transfer of this data.

The EU negotiated with the U.S. over these data records transfers for most of 2003, and in December 2003 the European Commission announced what it felt was an adequate agreement. In effect, the established agreement fails to meet the interests of privacy protection. The European Commission failed.

The agreement does meet the interests of others, however.

a. The U.S. Department of Homeland Security (DHS) gets access to EU airline database records even though the DHS does not require similar access to U.S. carriers' computer systems and records.
b. The U.S. now has data to test and implement its controversial Computer Assisted Passenger Pre-Screening System, using European passenger data instead of American passenger data. The European Commission believes that the Department of Homeland Security will remove this data once testing is complete. This is an unacceptable risk taken by the Commission.
c. The European Commission is now speaking of creating a centralised database of all passenger records so that the records can then be transferred to the U.S.; creating further privacy and security concerns.
d. The European Commission wishes to see the development of EU-based laws that will grant database access to EU member states for law enforcement purposes. The EU also wishes for access to U.S. passenger data, but has not yet negotiated this with the Americans.
e. After establishing European surveillance laws, the European Commission is also seeking to create a global regime on passenger records surveillance through the UN agency, the International Civil Aviation Organization; thus permitting all countries to gain access to this data.

The case has never been made, however, that this information is necessary or proportionate. We call on the European institutions, including the Parliament, the Commission and the Article 29 Working Party to not only question the adequacy of the legal regime surrounding data records transfers but also the reality of its implementation: a global surveillance system of all travel, not for the purpose of combating terrorism, but generally for law enforcement purposes. We do not consider this to be proportionate, foreseeable, or necessary in a democratic society.

The Commission is thus transformed from a protector of privacy rights into an opportunistic institution seeking to reduce privacy in its own interests. The 'negotiations' with the U.S. failed to uphold European privacy law because the rescinding of EU privacy protection is in the interest of the European Commission. The results of the negotiations are summarised below.

Issue	U.S. Law Requirement	Original U.S. Demands	EU Privacy Requirements	December 2003 Settlement
Purpose of transfer and processing?	'ensuring aviation safety and protecting national security'	'serious criminal offences'	Specific and proportionate; terrorism and serious related crime.	'Terrorism and related crimes' and to 'other serious crimes, including organized crime, of a trans-national nature'
Sharing of Data?	Beginning from the Customs Service, 'may be shared with other Federal agencies for the purpose of protecting national security'	Shared with other Federal agencies for the purpose of protecting national security, or as otherwise authorized by law.	Specific, on a case-by-case basis	Shared within the Department of Homeland Security, e.g. used in development of TSA's CAPPS system. Otherwise still very unclear, although DHS has apparently promised 'no bulk sharing with other agencies'.
How to Access Data?	'carriers shall make passenger name record information available to the Customs Service upon request.'	On-line access to Airline databases to 'pull' whatever information they wish. Includes access to non-U.S. related travel.	Must be limited to what is strictly necessary, and limited access to sensitive information. Sharing only upon consent.	Tentative statements regarding 'push', possibly through a centralised EU institution. Possible reciprocity for the EU.
Breadth of Access to Information?	'PNR'	Broad, at the discretion of U.S. Customs, includes non-U.S. travel information. Estimated 50-60 fields.	Must be limited to what is strictly necessary; no access to sensitive information. Mostly information available on ticket and itinerary.	34 fields. Sensitive data to be filtered by an EU institution that will also grant access to EU member states.
Automated Processing and Profiling?	Unclear.	Data to be used within CAPPS II.	Not possible unless 'logic' of system is understood.	Leave for future agreement; even as European passenger data records are being used to develop the system.
Retention Period?	Undeclared in law.	50 years.	72-hours according to EU regulations, retained for 3 years for billing-disputes only. At most, 'a short period'; 'not more than some weeks, or even months'.	3.5 years.
Right of Redress?	none	None promised.	'Provide support and help to individual data subjects in their exercise of rights' including access to data, and 'Appropriate redress mechanisms for individuals'. Called for judicial or extra-judicial (independent) redress mechanisms.	CPO in DHS; possibly with EU Data Protection Authorities representing EU citizens.
Compliance Reviews?	None	None promised.	Must be ongoing verification of compliance.	Yearly with the co-operation of the EU.

The data transfers are not adequate under EU regulations; and the conditions of transfer are insufficiently strict under European Parliament requirements for any such agreement. Yet the Commission claims that this is adequate under privacy law requirements. This situation must be investigated and rectified.

This inadequate and loose agreement must not be used as a first step to an EU-wide, and even global, surveillance system.

Privacy International (www.privacyinternational.org)
In cooperation with:
European Digital Rights Initiative (www.edri.org)
Foundation for Information Policy Research (www.fipr.org)
Statewatch (www.statewatch.org)
February 2004

I. Introduction

An historic battle is being waged over the issue of the transfer of information about airline passengers between Europe and the United States. And it is not just a conflict between the U.S. and the EU, but a conflict between those on both sides of the Atlantic who value privacy and limits on the ability of governments to invade it, and those who would like to create permanent infrastructures for the regular observation of individuals' travel patterns.

The origin of the conflict is the decision by the Bush Administration to rely heavily on an information-based approach to stopping terrorism. As part of this effort, the U.S. is seeking a sharp increase in the amount of information that airlines must provide to U.S. authorities about their passengers – a requirement that depends on the cooperation of other nations, including Europe, which have strong privacy laws that must be reconciled with the U.S. request.

This report outlines the conflict between European privacy laws and the American request for data, the attempts to resolve that conflict, and the outstanding legal and regulatory problems for civil liberties. We are left with a situation where vague U.S. legal requirements lead to a global surveillance system of travellers' personal information.

II. The U.S. Demand

The origin of the U.S.-EU passenger data conflict was one of the many pieces of legislation passed by the U.S. Congress in the wake of September 11: a law called the Aviation and Transportation Security Act 2001.[1] This law instituted a requirement that foreign carriers "shall make passenger name record information available to the Customs Service upon request", and provided for this information to be shared with other agencies outside of the Transportation Security Administration.[2] The availability of this information was deemed necessary for purposes of "ensuring aviation safety and protecting national security."[3] It is important to note that U.S. carriers do not need to comply with this requirement; only foreign carriers.

Passenger name records, or "PNR," can include vast amounts of information, such as:

- **Identification data:** name, first name, date of birth, telephone number;
- **Transactional data:** the dates of reservations, the travel agent where appropriate, the information displayed on the ticket, the itinerary;
- **Financial data:** credit card number, expiry date, invoicing address etc.;
- **Flight information:** flight number, seat number, etc.;
- **Earlier PNR:** may include not only journeys completed in the past but also religious or ethnic information (choice of meal etc.), affiliation to any particular group, data relating to the place of residence or means of contacting an individual (e-mail address, details of a friend, place of work etc.), medical data (any medical assistance required, oxygen, problems relating to sight, hearing or mobility or any other problem which must be made known to ensure a satisfactory flight) and other data linked, for example, with frequent flyer programmes.[4]

[1] "To improve aviation security, and for other purposes." In *USC*, 49, 597-647, 2001. It is important to distinguish between PNR and passenger manifests. One component of this Act amended Title 49 of the U.S. Code, sec44909, regarding "flights in foreign air transportation" changed the treatment of passenger manifests: the name of passengers, birth date and citizenship, sex, passport number and country of issuance, visa number, and other such information. This "advanced passenger information" is **not** the topic of this report as it is relatively unproblematic.
[2] ATSA, Section 115(c(3)).
[3] Federal Register. *Interim Rule Passenger Name Record Information Required for passengers on Flights in Foreign Air Transportation to or From the United States.* Washington: Department of the Treasury Customs Service, 2002, 19 CFR Part 122. June 25
[4] Article 29 Working Party. *Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States.* Brussels: European Commission, 2002. 24 October.

The European Commission estimates that although there are approximately 2-25 possible fields of PNR data, some of these fields include subsets of information expanding the total to approximately 60 fields and sub-fields.[5]

The Congressional requirement for PNR has been interpreted very widely by the Bush Administration. According to an interim rule of June 2002:

- All carriers must not just provide U.S. Customs with PNR data, but actually give the government direct electronic access to the airlines' computer systems. Each airline was responsible for ensuring that its automated reservation system and/or departure control system could interface with the U.S. Customs Data Center so that U.S. customs agents could log-in and look through files.
- This data must be provided for all flights, not only those destined for the U.S. So long as a carrier is 'engaged in foreign air transportation' to the U.S., U.S. Customs may access PNR information on the carrier's database. (U.S. Customs claims that it would not require PNR for non-US travel, but contends that "as a business decision, the airlines opted not to build filters within their reservation systems to preclude access to travel with no US nexus".[6])
- This data, once 'transferred', may be shared with other federal agencies for the purpose of protecting national security or as otherwise authorized by law. According to the interim rule, this data will then be stored by the U.S. Government for 50 years.

III. The European Law

The problem for the U.S. government is that these demands clash with European privacy protections that have been in place for almost ten years. Under the 1995 EU Data Protection Directive, EU member states must:

- restrict access to data
- limit the purposes for its use, as data may only be used for the purpose it is collected
- minimize the period of retention
- ensure that individuals have access to the data that is held on them
- ensure that individuals have legal recourse
- ensure that the data is protected adequately.

One of the Directive's primary goals was to ensure "not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded."[7]

The importance of "adequacy"

There is one huge stumbling block to the release of this information from Europe to the U.S. authorities. Article 25 of the EU Directive requires that if personal information is going to be sent to other jurisdictions that are not covered by EU laws, these other jurisdictions must have *adequate* privacy laws.[8]

To establish an agreement with the U.S. to allow this transfer of data, an adequacy assessment is generally required. According to the Directive,

[5] European Commission. *Airline passenger data transfers from the EU to the United States (Passenger Name Record) frequently asked questions*. Brussels, 2003, MEMO/03/53. March 12, archived at http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=MEMO/03/53|0|RAPID&lg=EN&display=

[6] U.S. Customs. *Presentation to European Parliament Hearings on Customs Border Protection*. Brussels, 2003. May 6, archived at http://www.europarl.eu.int/comparl/libe/elsj/events/hearings/20030506/apis_pnr.pdf.

[7] "Directive 95/46/EC of the European parliament and of the Council on the Protection of individuals with regard to the processing of personal data and on the free movement of such data." In *Official Journal of the European Communities*, 281/31, 1995.; Preamble paragraph 3.

[8] "The transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited." Ibid., preamble paragraphs 56-57.

> The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.[9]

There are grounds for assessing adequacy, as established by the European Commission's expert group, the Article 29 Working Party.[10] (see box 1) Any agreement with the U.S. for the transfer of personal information would have to meet these requirements.

- **Content Principles:**
  - Purpose limitations: where data can only be collected and processed for a limited number of purposes;
  - data quality and proportionality: the data is accurate and its integrity is maintained;
  - transparent: individuals are provided with information regarding the processing;
  - security: data is secure and protected from arbitrary access;
  - rights of access, rectification, opposition: individuals may gain access to the information held on them, challenge and rectify errors, and challenge its collection and use
  - no onwards transfers to other third countries
- **Particular attention is required to:**
  - Sensitive data: additional safeguards, such as explicit consent, are required for such data, defined by Article 8, "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."
  - Automated Individual decision-making: where the purpose of data transfer is the taking of an automated decision, individuals should have the right to know the logic involved in this decision and other measures should be taken.
- **Procedural/Enforcement Mechanisms:**
  - Good level of compliance: high degree of awareness among data controllers of data protection rights and obligations
  - Provide support and help to individual data subjects in their exercise of rights
  - Appropriate redress mechanisms for individuals

Box 1: Article 29 Working Party, adequacy principles.

The United States does not come close to matching these requirements for "adequacy":

- Federal privacy laws in the U.S. fall far short of these criteria, and in any case apply only to 'U.S. persons'.
- As EU officials are aware, the PNR-transfer is part of a much larger surveillance regime being established in the U.S. – a broader regulatory and technological framework that includes the introduction of biometrics into passports as a condition of continued access to the Visa Waiver Program, data mining and passenger profiling under the "Computer Assisted Passenger Pre-Screening System" (CAPPS II), no-fly lists, and foreigner registration programs.
- This information will be retained by the U.S. authorities for extensive periods.
- The PNR data will be used for an expansive set of purposes – not limited to national security but also for 'other crimes'.
- The PNR data may also be sold to private companies.[11]

The U.S. legal regime would certainly not protect the personal data of EU citizens adequately, and as a result this information can not be transferred out of the EU to the U.S.

IV. The 'Negotiations'

The stakes are high in the conflict over the transfer of passenger data. If no satisfactory arrangement is reached and the EU prevents access to these databases, the consequences could include:

- Retribution against EU airlines and passengers for not adhering to U.S. requirements. The U.S. authorities may opt to conduct 'secondary inspections' of arriving passengers in the U.S., fines for airlines, and even the loss of landing rights.[12] We have already seen the cancellation of specific flights from France and the United Kingdom to the United States; according to the DHS

[9] Ibid. Article 25.2,
[10] Article 29 Working Party. *First orientations on Transfers of Personal Data to Third Countries -- Possible Ways Forward in Assessing Adequacy*. Brussels: European Commission, 1997, XV D/5020/97-ENfinal WP4. 26 June.
[11] Article 29 Working Party. *Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data*. Brussels: European Commission, 2003. June 13.
[12] Bolkestein, F. *Speaking notes for European Parliament LIBE Committee*. Brussels: European Commission, 2003d. September 9 Archived at http://www.statewatch.org/news/2003/sep/Bolkestein-libe-9-09-03.pdf

Undersecretary for Border and Transportation Security, the real failure in these cancellations was the failure of the airline to provide information "sufficiently in advance".[13]

- The U.S. is worried that if the EU refuses to comply then other countries with similar privacy laws but weaker oversight and accountability structures will follow the EU lead. For example, the Czech government has come under pressure on the issue.[14] The Czech Personal Data Protection Office has argued, on this very same issue, that "Privacy is one of the basic values of human life, and personal data is the main gate enabling entry into it (...). Besides, the citizens of countries that experienced a period of totalitarian regimes have behind that a hard experience -- when privacy was not considered of value and was sacrificed to the interest of the state."[15] The Czechs have a weaker negotiating position with the U.S. than the hundreds of millions of Europeans, however.
- The U.S. needs data to use in testing its Computer Assisted Passenger Pre-Screening System (CAPPS II), and is expecting to use European personal records.
- Some within the EU want an agreement structured in such a way that it will empower member states to gain access to PNR as well.

The European Parliament has been particularly active in this area. In a vote of 445-31 (with 21 abstentions), the Parliament called for an agreement between the EU and the U.S., but required strict data protection safeguards.[16] Unless the U.S. can pass an adequacy test for its protection of personal data, the Parliament said, all data transfers must stop.

Throughout 2003 the European Commission's Directorate-General for the Internal Market, which is responsible for data protection, has been in negotiations with the U.S. Department of Homeland Security over these data records transfers. In December 2003, the European Commission reached an agreement with the U.S. However, this agreement does not appear to meet standards set by the European Parliament for any agreement to share data. Moreover, the agreement appears to meet the interest of other Directorate-Generals within the Commission.

As we have seen, ensuring adequate safeguards requires negotiating the key principles of data protection:

A. limiting the purpose of data collection and its use
B. controls on the use of 'sensitive data'
C. clear safeguards and rules on automated processing
D. limiting the retention periods
E. establishing reasonable enforcement mechanisms.

Failure to negotiate satisfactory arrangements on any of these issues means that any transfer would be illegal. Let us examine each of them in greater detail.

A. Limiting the Purpose of Data Collection and Its Use

The history of the negotiations on the transfer of passenger data between the U.S. and the European Commission show a bizarre pattern of conflict and capitulation.

Expansion beyond terrorism to ordinary crimes

In negotiating the purposes for which passenger data may be used, the DHS is interpreting its legal mandate widely, making expansive demands that go far beyond what Congress authorized.

- Under the original law, the purposes of data collection were for aviation and national security.

[13] Parker, G. "Brussels warns US over sky marshals." *Financial Times*, January 16.
[14] CTK. "Czech airlines must give USA personal data of its passengers-CT." *Ceskenoviny.cz*, December 4. Archived at http://www.ceskenoviny.cz/news/index_view.php?id=38931
[15] Bauman, V. "CSA, U.S. in security tussle." *The Prague Post*, December 11, 2003. Archived at http://www.praguepost.com/P03/2003/Art/1211/news6.php
[16] European Parliament. *European Parliament resolution on the Transmission of personal data by airlines in the case of transatlantic flights: state of negotiations with the USA*. European Union, 2003. October 9. Archived at http://www.statewatch.org/news/2003/oct/eppnrresol.pdf

- The list was quickly extended to include unspecified "serious criminal offences". Under the EU's regime, transfer can only take place "where necessary in specific cases for the fight against serious offences directly related to terrorism and that subsequent use of such data continues to be limited."[17]
- Later in the negotiations, the U.S. offered to use data only for crimes that are punishable by a minimum imprisonment term of at least four years.[18] But the Commission was clear on how this continued to be unacceptable: "I continue to emphasise to Mr. Ridge the difficulties we see in using these data for combating ordinary crime, however serious."[19]
- Puzzlingly, the final agreement does not meet any of the Commission's requirements. The Commission noted that the U.S. has agreed to allow the data to be used for 'terrorism and related crimes' and for 'other serious crimes, including organized crime, of a trans-national nature".[20] This ambiguous extension of purpose remains problematic even as the Commission appears willing to accept it.

Bulk sharing with other agencies

The December 2003 statement also included a promise from the U.S. that there will be no bulk sharing of data with other agencies.[21] But considering the size and breadth of the Department of Homeland Security, the key question is what, exactly, constitutes 'other agencies'. DHS is made up of an amalgam of numerous departments with widely varying missions that until recently were separate agencies altogether. A promise not to bulk-share information outside this behemoth of an agency may not be much of a promise.

If this information is limited to Customs, then a detailed Privacy Impact Assessment reviewing all data sharing by the U.S. Customs Agency within the DHS and beyond would be a minimum requirement prior to any finding of adequacy.

Toward Europe's own surveillance infrastructure I: Expanding Purposes

It emerged in the negotiations that the Commission was also concerned with creating a policy similar to the U.S. policy on access to PNR. In fact, the Commission grew reluctant to refuse to the U.S. government access to the data on these very grounds.

The agreement with the U.S. was seen as a precursor to a European policy on access to PNR. When the Commissioner for the Internal Market announced to the European Parliament the new agreement with the U.S., he was accompanied by the Commissioners for Justice and Home Affairs, Transport, and External Relations. At this session, the Commissioner for Justice and Home Affairs, Antonio Vitorino, commented that the EU is

> confronted with the need to complement that agreement with the United States of America by the development of a European Union policy on the use of PNR and of traveller's data more generally within the European Union.[22]

At this very same session, the Transport Commissioner argued for "adopting a community policy in the field of data processing with a view to control immigration".[23] It was then announced that in 2004 a policy would be developed for "our own EU approach to the use of traveller's data for border and aviation security and other law enforcement proposals."

---

[17] Article 29 Working Party. *Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data.* Brussels: European Commission, 2003. June 13, archived at http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp78_en.pdf

[18] Bolkestein, F. *Address to European Parliament Committees on Citizens' Freedoms and Rights, Justice and Home Affairs and Legal Affairs and the Internal Market.* Brussels: European Parliament, 2003a. December 1 Archived at http://europa.eu.int/rapid/start/cgi/guestfr.ksh?p_action.gettxt=gt&doc=SPEECH/03/586|0|RAPID&lg=EN&display=

[19] Ibid.

[20] Bolkestein, F. *EU/US talks on transfers of airline passengers' personal data: Address to European Parliament Committees on Citizens' Freedoms and Rights, Justice and Home Affairs and Legal Affairs and the Internal Market.* Strasbourg: European Parliament, 2003b. December 16.

[21] Ibid.

[22] European Parliament. *Transcription of the committee meeting: European Parliament Committees on Citizens' Freedoms and Rights, Justice and Home Affairs and Legal Affairs and the Internal Market.* Strasbourg: European Parliament, 2003. December 16.

[23] Ibid.

In January 2004, the Irish Presidency announced that the Justice and Home Affairs Committee would work to create a "Directive on the obligation of carriers to communicate passenger data".[24]

The European Commission had thus transformed from an institution that wished to limit the purposes for the processing of PNR by government agencies, into an institution that wished to 'complement' the U.S. call for data for combating terrorism and serious related crime through using this information for border security, immigration, and other law enforcement purposes.

Issue	U.S. Law Requirement	Original U.S. Demands	EU Privacy Requirements	December 2003 Agreement
Purpose	'ensuring aviation safety and protecting national security'	'serious criminal offences'	Specific and proportionate; terrorism and serious related crime.	'Terrorism and related crimes' and to 'other serious crimes, including organized crime, of a trans-national nature'
Sharing of Data	Beginning from the Customs Service, 'may be shared with other Federal agencies for the purpose of protecting national security'	Shared with other Federal agencies for the purpose of protecting national security, or as otherwise authorized by law.	Specific, on a case-by-case basis	Shared within the Department of Homeland Security, e.g. used in development of TSA's CAPPS system. Otherwise still very unclear, although DHS has apparently promised 'no bulk sharing with other agencies'.

B. Controls on the Use of 'Sensitive Data'

The U.S. law regarding access to PNR states that "carriers shall make passenger name record information available to the Customs Service upon request". DHS read into this a requirement that the U.S. be able to actually log-in to airline databases and *pull* down whatever information it wants regarding travellers. Under these requirements, the U.S. government would be able to sift through personal data as it pleases.

This is clearly unacceptable under the EU privacy regime, which requires a limitation on the amount of disclosed information. In their recommendations, the Article 29 Working Party stated that the transfers should be limited to:

> PNR record locator code, date of reservation, date(s) of intended travel, passenger name, other names on PNR, all travel itinerary, identifiers for free tickets, one-way tickets, ticketing field information, ATFQ (Automatic Ticket Fare Quote) data, ticket number, date of ticket issuance, no show history, number of bags, bag tag numbers, go show information, number of bags on each segment, voluntary/involuntary upgrades, historical changes to PNR data with regard to the aforementioned items.

According to U.S. Customs, much of this information is already available on the ticket and the itinerary.[25]

In the face of these requirements, the Commission has urged adoption of a *push* system of transfer. Rather than allowing U.S. agents to log-in to airline computer systems, *push* transfers would involve placing the burden of the transfers on EU airlines, who would have to send the required data to the U.S. agencies. This more restricted mode of access requires airlines to disclose only the *required* information, rather than giving the U.S. authorities access to *all* the information.

Sensitive information

Some of the data that the U.S. is seeking is considered 'sensitive' – data that the EU privacy regime is clear must be ruled out. That includes several fields within the standard PNR records in most airline databases: open or free-text fields (such as "General Remarks" where data of a delicate nature can appear), information concerning frequent-flyers, 'behavioural data', dietary choices, medical conditions and so on.

[24] Council of the European Union. *Work programme for the Article 36 Committee*. Brussels: Presidency of the Council of the European Union, 2004, 5092/04 CATS 2. 7 January.
[25] U.S. Customs. *Presentation to European Parliament Hearings on Customs Border Protection*. Brussels, 2003. May 6.

After much deliberation, the final negotiations reduced the original access from full-PNR records down to 34 fields. And in its report to Parliament, the Commission claimed that the U.S. has conceded that all categories of 'sensitive data' will be deleted.[26] This claim has not yet been verified, particularly as other plans have emerged from the Commission.

Toward Europe's own surveillance infrastructure II: Specifying the Data

The treatment of sensitive information in the negotiations also betrays the European Commission's interests in an EU-policy on the use of PNR. In fact, the Commission grew reluctant to refuse to the U.S. government access to the data on these very grounds.

At the beginning of December 2003, Directorate-General for the Internal Market was concerned with the amount of data that the U.S. was demanding to access.

> The US list has come down from 39 to 34, which is an improvement. But many data elements we had worries about are still in the list. Without an agreed EU policy on the use of PNR, I doubt more progress can be achieved. [27]

Two weeks later, however, the Commission clarified this point. Commissioner Bolkestein informed the European Parliament that the EU must be careful what it refused to the U.S.

> The EU cannot refuse to its ally in the fight against terrorism an arrangement that Member States would be free to make themselves.[28]

Despite the initial 'worries' about the information that would be accessed by the U.S., however, the 34 fields were subsequently considered adequate by the Commission. The final Communication from the Commission later stated that the agreement

> with the US appears to be a sound basis for taking forward work on an EU approach (…). The list of data elements also seems broad enough to accommodate law enforcement needs in the EU. Nothing in the arrangements agreed with the US therefore seems to prejudice the development of an appropriate EU policy.[29]

The Commission argued that it could not restrict U.S. access to information that would be collected for EU use. Put another way, the EU could not say that the U.S. had no right accessing sensitive data that the EU wished for itself for even more expansive purposes (see above). Therefore, the Commission was not negotiating the protection of privacy; it was rather negotiating wiggle-room within an international agreement for the establishment of an EU-level policy.

Toward Europe's own surveillance infrastructure III: Centralising the Infrastructure

The Commission is willing to justify its intricate policy plans based on the demands of the U.S. The Commission previously argued against the U.S. gaining direct access to airline databases, and to 'sensitive data'. Rather it argued that a 'push' system would be ideal, where the required data would be sent to the U.S., and all sensitive data would be filtered by the carriers. In early December the Commission then stated:

> The Commission is also working with the airlines on switching from pull to push as regards the means of transferring the data and on the necessary filters. The airlines are interested in a centralised or grouped approach, which seems also to the Commission to offer advantages in terms of cost and efficiency.[30]

---

[26] Bolkestein, F. *EU/US talks on transfers of airline passengers' personal data: Address to European Parliament Committees on Citizens' Freedoms and Rights, Justice and Home Affairs and Legal Affairs and the Internal Market*. Strasbourg: European Parliament, 2003b.
[27] Bolkestein, F. *Address to European Parliament Committees on Citizens' Freedoms and Rights, Justice and Home Affairs and Legal Affairs and the Internal Market*. Brussels: European Parliament, 2003a. December 1.
[28] Bolkestein, F. *EU/US talks on transfers of airline passengers' personal data: Address to European Parliament Committees on Citizens' Freedoms and Rights, Justice and Home Affairs and Legal Affairs and the Internal Market*. Strasbourg: European Parliament, 2003b. December 16.
[29] Commission of the European Communities. *COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE PARLIAMENT: Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach*. Brussels: European Union, 2003, COM(2003)826final.
[30] Bolkestein, F. *Address to European Parliament Committees on Citizens' Freedoms and Rights, Justice and Home Affairs and Legal Affairs and the Internal Market*. Brussels: European Parliament, 2003a. December 1.

In mid-December, the Vice President of the Commission, who is responsible for Transport, Loyola De Palacio, agreed that a centralised approach would save money for airlines, but would also assist in "adopting a community policy in the field of data processing with a view to control immigration".[31] On this point, the carriers appear to be in agreement: a centralised solution would be cheaper.

The Justice and Home Affairs Commissioner went a step further, however. Commissioner Vitorino goes on to say:

> As a matter of fact, I can even see that a centralized structure inside European Union will be able to provide the necessary guarantees on the liability aspects, the accuracy of the data on the security of transmitted data, the technological means and the filters that Vice-President De Palacio has just mentioned to you, on the supervision by adequate control mechanisms, above all the role of the giant supervisory board and for offering added value to similar initiatives conducted at national levels within the European Union."[32]

This led to the carefully worded final Communication from the Commission. The logic for a centralised system was clearly stated.

> It was also made clear (…) that implementation of a push system could not solve the problem alone. Filters would also need to be installed. These filters entail significant costs for the airlines, which mean that a legal obligation would be desirable to ensure that all airlines are subject to the same requirements. Airlines have also indicated a preference for a centralised system.[33]

But this also involves a legal obligation upon carriers in the EU and abroad.

Toward Europe's own surveillance infrastructure IV: Ensuring Co-operation and Reciprocity

The Commission then saw that a centralised system and an EU policy on PNR would need to be complemented with laws requiring airlines to provide this information, and applying these rules to all carriers, worldwide. According to the final Communication from the Commission:

> It would be difficult to envisage obliging airlines, including US airlines, to adopt such a system, without creating a legal obligation for them to do so. There is currently no EU law or Community policy that obliges airlines to transfer PNR data in this way. A possible framework for the establishment of such a system would be a Community policy on PNR data collection for security and/or immigration purposes.[34]

The breadth of this initiative does not end at the borders of the EU, however. As Palacio stated

> the Commission is not a member of ICAO, the International Authority for Civil Aviation, but we've been pushing hard for an international response to this problem. Transfer of PNR data must be accompanied by a multilateral approach in our view, and we feel that the best approach would be to adopt a worldwide agreement on this.[35]

The Communication states that this was always a part of their approach for resolving the problem with the U.S.

> The transfer of PNR data is a truly international, and not only a bilateral problem. Therefore, the Commission has taken the view that the best solution would be a multilateral one and that the ICAO would be the most appropriate framework to bring forward a multilateral initiative. In September 2003, the Commission decided to accelerate work on

[31] European Parliament. *Transcription of the committee meeting: European Parliament Committees on Citizens' Freedoms and Rights, Justice and Home Affairs and Legal Affairs and the Internal Market*. Strasbourg: European Parliament, 2003. December 16.
[32] Ibid.
[33] Commission of the European Communities. *COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE PARLIAMENT: Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach*. Brussels: European Union, 2003, COM(2003)826final. December 16.
[34] Ibid.
[35] European Parliament. *Transcription of the committee meeting: European Parliament Committees on Citizens' Freedoms and Rights, Justice and Home Affairs and Legal Affairs and the Internal Market*. Strasbourg: European Parliament, 2003. December 16.

> developing an international arrangement for PNR data transfers within ICAO. The Commission services have prepared a working paper to this effect that will be submitted by the Community and its Member States to ICAO shortly.[36]

An agreement on PNR transfer at the ICAO would mean that all members of the ICAO would be transferring PNR between each other. The ICAO is a UN agency.

Reciprocity is thus a key component to this multilateral 'solution', relying on the centralised EU-store of information. According to Commissioner Vitorino,

> this central unity can become the focal point to ensuring the principal of reciprocity for possible information exchanges with authorities from third countries, I believe Frits Bolkestein did not mention this, but reciprocity is a key issue in this agreement with the United States. As I've said to you, at European level we are in the early stages of the development of a EU policy in this area.[37]

This is the language that was included in the final Communication.

> Finally, any possible information exchange with the US authorities should be based on the principle of reciprocity in the transfer of data between the EU and the US, whilst at the same time considering the possibility for the collection and controlled transfer of PNR data through a central European entity.[38]

In summary, the handling of the negotiations over the collected data and purposes for access and makes it clear that the EU is hoping to establish its own infrastructure for monitoring citizens' travel data. The Internal Market Commission argued for an EU policy on access to PNR so that it could ensure that it was not restricting access for the U.S. to something that the EU member states would have access to; while also arguing for a centralized solution to filter out sensitive data. Meanwhile the Transport Commission wishes to establish an international solution through the ICAO for immigration controls, and the Justice and Home Affairs Commission aims to establish a centralized solution for access by EU member states for law enforcement purposes.

Starting with a simple law in the U.S., the European Commission has negotiated a global surveillance system tracking the movement of people.

Issue	U.S. Law Requirement	Original U.S. Demands	EU Privacy Requirements	December 2003 Agreement
Access	'carriers shall make passenger name record information available to the Customs Service upon request.'	On-line access to Airline databases to 'pull' whatever information they wish. Includes access to non-U.S. related travel.	Must be limited to what is strictly necessary, and limited access to sensitive information. Sharing only upon consent.	Tentative statements regarding 'push', possibly through a centralised EU institution. Possible reciprocity for the EU.
Breadth of Access to Information	'PNR'	Broad, at the discretion of U.S. Customs, includes non-U.S. travel information. Estimated 50-60 fields.	Must be limited to what is strictly necessary; no access to sensitive information. Mostly information available on ticket and itinerary.	34 fields. Sensitive data to be filtered by an EU institution that will also grant access to EU member states.

C. Clear Safeguards and Rules on Automated Processing

Another bizarre conclusion to the negotiations involved the use of European data in the U.S. passenger-profiling system, CAPPS II. This system will profile all passengers using various sources of information

[36] Commission of the European Communities. *COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE PARLIAMENT: Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach*. Brussels: European Union, 2003, COM(2003)826final. December 16.
[37] European Parliament. *Transcription of the committee meeting: European Parliament Committees on Citizens' Freedoms and Rights, Justice and Home Affairs and Legal Affairs and the Internal Market*. Strasbourg: European Parliament, 2003. December 16.
[38] Commission of the European Communities. *COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE PARLIAMENT: Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach*. Brussels: European Union, 2003, COM(2003)826final.

including private sector databases that will be exempt from the U.S. Privacy Act – and will thus require little specification of purpose, unassessable proportionality, questionable accuracy, and unlimited collection.[39]

- Early in the negotiations the U.S. actually promised that the data would only be used "only during an enforcement investigation, seizure or arrest will all of one passenger's travel be identified and linked to an enforcement database".[40] They also promised that data will be transferred to other agencies only on a case-by-case basis.[41]
- According to the December 2003 final communication from the Commission, it was agreed that European records would not be included in CAPPS II. This use of data was to be considered in a second round of discussions that would take place after the U.S. Congress authorised the system's development.[42]
- In January 2004 the Department of Homeland Security declared that the EU carriers' passenger records are, in fact, being used to develop CAPPS.[43]

European data is being used to test this American program **even while U.S. carriers refuse to do so** because of increasing concern among U.S. passengers stemming from public disclosures of airlines sharing their data with NASA (in the case of Northwest Airlines) and the Department of Defense (in the case of JetBlue). The DHS has stated that 'testing' does involve processing the data and possibly identifying and profiling specific passengers that may lead to notifying law enforcement authorities.[44]

This is due to further capitulation by the European Commission. The Commission has even promised that it will aim to complete the negotiations regarding CAPPS II within a month of the system receiving the approval of the U.S. government; foreseeing that such a framework "would be based as far as possible on the same undertakings as already agreed." [45] The Commission is set to capitulate further, even though the automated processing of data requires even greater scrutiny for an adequacy assessment. Even as the retention periods and further use purposes of CAPPS are not fully understood, the Commission is already planning on acquiescing.

In addition, it remains an open question whether and how it will be possible to separate out EU citizens' data, the data collected from EU airlines, from the rest of the volumes of data held and processed by this profiling system. If the EU was willing to concede on the transfer of data for serious crimes, its future negotiating position for resisting processing of data for 'travel security' purposes is likely to be weak.

It is unacceptable that EU carriers are handing over data for use for data profiling on a scale that begins to remind one of the Total Information Awareness Program; it is even more unacceptable that the Commission institutions responsible for the protection of privacy in the EU are promising and authorizing the use of personal data for such systems even as the U.S. is not requiring the same of its own carriers.

Issue	U.S. Law Requirement	Original U.S. Demands	EU Privacy Requirements	December 2003 Agreement
Automated Processing and Profiling	Unclear.	Data to be used within CAPPS II.	Not possible unless 'logic' of system is understood.	Leave for future agreement; even as European passenger data records are being used to develop the system.

[39] Laurent, C. *Statement for the Record to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs: Data Protection since 11 September 2001: What Strategy for Europe?* Brussels: Electronic Privacy Information Center, 2003. March 23
[40] U.S. Customs. *Presentation to European Parliament Hearings on Customs Border Protection.* Brussels, 2003. May 6.
[41] Bolkestein, F. *Speaking notes for European Parliament LIBE Committee.* Brussels: European Commission, 2003d. September 9 Archived at http://www.statewatch.org/news/2003/sep/Bolkestein-libe-9-09-03.pdf
[42] Bolkestein, F. *Address to European Parliament Committees on Citizens' Freedoms and Rights, Justice and Home Affairs and Legal Affairs and the Internal Market.* Brussels: European Parliament, 2003a. December 1.
[43] Rodota, S. *Intervention of Mr. Rodota, chair of the Article 29 Committee to the Committee on Citizens Freedom and Rights.* Brussels: European Parliament, 2003. November 25 Archived at http://www.statewatch.org/news/2003/nov/PNR-Rodota25-11-03.pdf
[44] AP. "Background checks for air passengers could start this summer: Homeland Security officials speed timetable for controversial plan." *MSNBC.com*, January 27. Archived at http://www.msnbc.msn.com/Default.aspx?id=4072256&p1=0
[45] Bolkestein, F. *Letter to Tom Ridge.* Brussels: European Commission, 2003, CAB-D/919. December 18, archived at http://www.europa.eu.int/comm/internal_market/privacy/docs/adequacy/pnr/2003-12-18-letter-bolkestein_en.pdf

D. Limiting the Retention Periods

Another key issue of contention between the U.S. and the EU is how long the U.S. authorities may retain this data once it has been transferred. According to EC regulations, data in airline systems should be taken off-line after 72 hours of the completion of booking (i.e. flight arrival) and archived for maximum 3 years for access **only** for billing-dispute reasons.[46] It is the duty of the Commission to enforce this regulation; which it has patently refused to do. Now it is negotiating away its responsibilities.

These regulations were drafted prior to the attention given to PNR for security purposes and the data transfers to the U.S. Even within such a context, however, the Article 29 Working Party argues that retention "should not exceed some weeks or even months following entry to the US".[47]

The U.S. authorities, on the other hand, originally demanded to keep the data for up to 50 years; in subsequent negotiations this number was reduced to seven. Even then, there were concerns. As the Commission said in October 2003:

> Keeping up to 39 data elements on every passenger and crew for seven years, regardless of whether there is any suspicion about them, or whether they have left the United States, is surely excessively intrusive by any standards.[48]

In the current agreement, the retention period has dropped to 3.5 years, along with the expiration of the transfer agreement. According to the Commission, "We have thus managed to link the lifetime of the agreement with the duration of the retention period."[49] But this still exceeds the Working Party's recommendation for a 'short period'.[50]

Once the data is included in the CAPPS II system, the retention period is unknown. It is important to note that many of the systems in use by the Department of Homeland Security, when their retention periods are known, the retention periods are stated to be in the order to 75+ years. The fingerprints and digital photos of EU citizens on visa-based travel to the U.S. are already stored for 75 years. As the PNR transfer is part of a larger programme of surveillance, it is likely that the retention periods will increase.

Issue	U.S. Law Requirement	Original U.S. Demands	EU Privacy Requirements	December 2003 Agreement
Retention Period	Undeclared in law.	50 years.	72-hours according to EU regulations, retained for 3 years for billing-disputes only. At most, 'a short period'; 'not more than some weeks, or even months'.	3.5 years.

E. Establishing Reasonable Enforcement Mechanisms.

European citizens have the right to redress if they believe that their data is being abused. Companies tend to have chief privacy officers who monitor compliance with legal protections of privacy, and each country that has implemented the 1995 Directive has a Privacy Commissioner responsible for acting on behalf of individuals who have concerns regarding their personal information.

---

[46] Council of European Communities. *Council Regulation (EEC) No 2299/89 of 24 July 1989 on a code of conduct for computerized reservation systems.* European Economic Community, 1989. July 24 Archived at http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexplus!prod!CELEXnumdoc&lg=en&numdoc=389R2299

[47] Article 29 Working Party. *Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data.* Brussels: European Commission, 2003. June 13.

[48] Bolkestein, F. "Passenger privacy and the war on terror." *International Herald Tribune*, October 24. Archived at http://www.iht.com/cgi-bin/generic.cgi?template=articleprint.tmplh&ArticleId=114901

[49] Bolkestein, F. *Address to European Parliament Committees on Citizens' Freedoms and Rights, Justice and Home Affairs and Legal Affairs and the Internal Market.* Brussels: European Parliament, 2003a. December 1 Archived at http://europa.eu.int/rapid/start/cgi/guestfr.ksh?p_action.gettxt=gt&doc=SPEECH/03/586|0|RAPID&lg=EN&display=

[50] Rodota, S. *Intervention of Mr. Rodota, chair of the Article 29 Committee to the Committee on Citizens Freedom and Rights.* Brussels: European Parliament, 2003. November 25 Archived at http://www.statewatch.org/news/2003/nov/PNR-Rodota25-11-03.pdf

The Article 29 Working Party has called for enforceable safeguards for the transfer and use of European passenger data by the U.S. authorities. This requires nothing less than "legally binding commitments, and adequate protection in U.S. law".[51]

U.S. law on privacy protection, in contrast, is considered substandard. Even at its best, the U.S. law applies only to U.S. persons. The Commission previously commented on the

> insufficient legal bindingness of US undertakings -- hence our insistence, if rights are not actionable before US courts, on independent extra-judicial redress mechanisms.[52]

These calls have not been addressed.

In discussing the December 2003 U.S.-EU agreement, the Commission had to concede that "it has become clear that Congress does not intend to create such rights".[53] The Commission also noted that at best the EU can expect that regulations will be created to regulate mechanisms for redress. Such an agreement would appear to accept a system under which individuals could complain to the Department of Homeland Security and the Privacy Office within the DHS. The Commission has managed to get the U.S. to accept that compliance reviews must be done jointly, and yearly. According to the Commission, this gives the EU "a way to ascertain how well the US implements its Undertakings."[54] And the Commission claims that the U.S. is willing to recognise the right of EU data protection authorities to represent EU citizens.[55]

Still, the bottom line is that the commission appears to have accepted the position of Chief Privacy Officer (CPO) in DHS, who reports to the Secretary of DHS, as a fair arbiter on such issues. The Commission has admitted that the CPO office is not independent, but is accepting a pledge by the U.S. government that the CPO's rulings on complaints will be binding on the Department. As the Commissioner concedes: "Let us see how all this works in practice."[56] Such a position stands in complete violation of how findings of adequacy are supposed to work.

Issue	U.S. Law Requirement	Original U.S. Demands	EU Privacy Requirements	December 2003 Agreement
Right of Redress	none	None promised.	'Provide support and help to individual data subjects in their exercise of rights' including access to data, and 'Appropriate redress mechanisms for individuals'. Called for judicial or extra-judicial (independent) redress mechanisms.	CPO in DHS; possibly with EU Data Protection Authorities representing EU citizens.
Compliance Reviews	None	None promised.	Must be ongoing verification of compliance.	Yearly with the co-operation of the EU.

Negotiating a Conclusion

On issue after issue, the European Commission has negotiated away protections that European citizens are by law due. Whether on limits on what kind of data is collected, the purpose for which it is collected, the conditions under which it is shared, or what rights of redress citizens will have, the Commission has caved in to American pressure despite the clear requirements of European law. While this occurred, it has emerged that the Commission was not merely failing at the negotiations; it was instead succeeding at establishing its own laws and practices on access to PNR.

---

[51] Article 29 Working Party. *Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data.* Brussels: European Commission, 2003. June 13.
[52] Bolkestein, F. *Speaking notes for European Parliament LIBE Committee.* Brussels: European Commission, 2003d. September 9 Archived at http://www.statewatch.org/news/2003/sep/Bolkestein-libe-9-09-03.pdf
[53] Bolkestein, F. *Address to European Parliament Committees on Citizens' Freedoms and Rights, Justice and Home Affairs and Legal Affairs and the Internal Market.* Brussels: European Parliament, 2003a. December 1.
[54] Ibid.
[55] Bolkestein, F. *EU/US talks on transfers of airline passengers' personal data: Address to European Parliament Committees on Citizens' Freedoms and Rights, Justice and Home Affairs and Legal Affairs and the Internal Market.* Strasbourg: European Parliament, 2003b. December 16.
[56] Ibid.

V. Policy Laundering and Further Threats

The results of the negotiations might appear to be a loss for the European Commission negotiators, but that is only if the process is viewed as a clash between opposing interests and values. In truth, the outcome is a victory for a Commission that is set to increase surveillance of European passengers.

This is another clear case of what is becoming known as "policy laundering," in which government officials use the requirements of other jurisdictions as justification to obtain or enhance powers clearly wished for but otherwise unobtainable. EU member states are now clamouring to gain access to passenger records, something previously prohibited but now being considered due to vague law and overzealous agencies in the U.S.

The synergy between what the EU and the U.S. wishes for is startling: if Europe declares a policy on access to PNR by the member states, then this would aid the transfer agreement with the U.S. In such an eventuality, the Commission argues, the "EU cannot refuse to its ally in the fight against terrorism an arrangement that Member States would be free to make themselves."[57] This is even as the Commission claims that such policies can be established not only to combat terrorism and ensure travel security, but for general law enforcement purposes.

Additional issues

- **Costs of transfers require a centralised solution.** The costs of allowing for access and transfers, likely to be incurred by the airlines themselves, are quite high; possible in the tens of millions of dollars.[58] This is cited to justify a centralised EU approach to minimise these costs, but this would create even more privacy problems.
- **Centralising negotiations also leads to a centralized surveillance system.** Direct U.S. negotiations with individual EU member states would involve developing bilateral agreements. This strategy, which has been termed 'disaggregation', would circumvent the Parliament's requirements and the Commission's adequacy assessments.[59] Supporters of this stratagem contend that a national government can decide to bypass privacy laws for the sake of law enforcement and national security (as many Parliaments have since September 11 2001). Experts say this argument is invalid, however; while national governments may create exceptions to privacy rules for such purposes, they may not transfer the data to another jurisdiction on these grounds.[60] More importantly, however: each agreement would likely be different from one another. If the requirements for data transfers differ from country to country, the costs of setting systems for the transfers would increase, and thus a cross-European technological system would not be possible. The Commission fears such a situation, and is pushing for an adequacy finding at the level of the EU.
- **Circumventing opposition through international agreements.** Already the EU and the U.S. have begun searching for alternative international institutions to further agreements on data transfer. Both the U.S. and the EU plan to or have taken the issue to the UN-level agency, the International Civil Aviation Organization (ICAO). The EU could then ratify such an agreement through the European Parliament (but under the requirements of international co-operation) while also granting access to this data to European law enforcement authorities, and gaining access to the records of non-EU carriers. This is expected to be introduced to the ICAO in March 2004.[61]

This race to the bottom and exceptionalism for the U.S. is the larger trend behind this long list of incursions on due process rights and civil liberties.

---

[57] Ibid.
[58] Goo, S. K. "EU Agrees to Share Airline Passenger Data." *Washington Post*, December 17.
[59] Reuters. "US sees EU deal on air passenger data by year-end." *Reuters.com*, November 24.
[60] Rodota, S. *Intervention of Mr. Rodota, chair of hte Article 29 Committee to the Committee on Citizens Freedom and Rights.* Brussels: European Parliament, 2003.
[61] Bolkestein, F. *Address to European Parliament Committees on Citizens' Freedoms and Rights, Justice and Home Affairs and Legal Affairs and the Internal Market.* Brussels: European Parliament, 2003a. This method of circumventing procedure through international agreements is increasingly common. For example, recently the United Kingdom is working on allowing the extradition of UK citizens to the U.S. without prima facie evidence, even though the U.S. requires such evidence for the extradition of Americans to the UK. The UK government's response to such criticism was that since other European countries are allowed access to UK citizens without prima facie evidence, there is no need to impose more stringent requirements on the U.S. C.f. Eaglesham, J., and Sherwood, B. "Price-fixing suspects risk extradition to US for trial." *Financial Times*, December 14 2003.

VI. Conclusions

The current state of the negotiations leaves European privacy rights at the mercy of the U.S. Department of Homeland Security's interpretations of its mandate granted by an ambiguous statement of law, passed in an uncertain time following catastrophic attacks on U.S. soil.

The European Commission appears to be relinquishing the protection of European privacy rights by declaring promises and assurances from U.S. officials to be adequate protection under the 1995 EU Data Protection Directive. Other countries will certainly follow the U.S. lead – even countries with more stringent PNR demands, such as Australia, now has every right to wonder why the EU is sharing so little with it under such stringent requirements when data is being shared so expansively with the U.S.

Meanwhile, other countries under pressure from the U.S. to weaken their privacy regimes will have lost an ally Europe, and will be forced to transfer data under similar, if not worse, conditions. The result will be to a race to the bottom for global privacy protection.

The Commission has failed on numerous grounds:

- It did not give proper regard to data protection principles in negotiating away many of the key tenets.
- It has not assured adequate protection requirements, clear purpose limitation, non-excessive data collection, limited data retention time, and insurance against further transfers beyond the DHS. Insufficiently independent privacy officers (in the Commission's own words), 3.5 years of retention, and ambiguous statements of offences are inadequate grounds to flout EU privacy law.
- It did not draw sufficient attention to the inequality of the U.S. law as it applies only to foreign carriers, not U.S. airlines operating abroad. In turn, further investigations must be conducted to ensure that U.S. airlines are abiding by EU privacy law.
- It did not demand a clear statement of use by the U.S. government. For quite some time the U.S. DHS has been accumulating PNR from some European carriers, and as yet still has not declared a privacy policy, or conducted a privacy impact assessment. Yet the European Commission believes that the DHS will protect future records adequately, even though it has no basis for such a belief; even though the records of Europeans are being used to develop a comprehensive automated profiling system that is in breach of fundamental privacy principles.
- It should not be promoting a European policy on law enforcement access to this data; it should instead be enforcing previous policy on privacy and airline reservation systems.
- It should not be pushing for a multilateral solution that would transform this situation from a small problem into a global surveillance infrastructure.

Failing to revisit all of these agreements and settlements will thus lead to a global surveillance system of travel. Other countries besides the U.S. will increasingly call for access to EU passenger records. Will the answer continue to be: "The EU cannot refuse to its ally in the fight against terrorism an arrangement that Member States would be free to make themselves"? We wait to see agreements with other 'allies', including Russia, India,[62] Turkey, Tunisia,[63] Malaysia and Thailand.[64]

With its self-interested determination in reducing privacy rights and its inability to stand on principle, the European Commission is selling one of its proudest legal regimes to the lowest bidder. Even as the U.S. government has shown reluctance in the past year to abuse its own citizens' data (e.g. in the testing of CAPPS II), the EU is handing over European personal data for abuse; while simultaneously calling for the abuse of citizens' data for a variety of EU purposes.

These personal data transfers and future plans are inadequately protected and dangerous. We must act now in order to prevent the emergence of a global system of travel surveillance.

---

[62] Keralanext News. "India: India, European Union to cooperate to fight global terrorism." *Keralanext News*, November 29.
[63] Agencies. "Europe to help N. Africa fight poverty and inequality to crush extremism." *Alayam Newspaper*, December 8.
[64] ASEAN-EU. *Joint Declaration on Co-operation to Combat Terrorism*. Brussels: 14th ASEAN-EU Ministerial Meeting, 2003. January 27-28

An American Perspective from the American Civil Liberties Union

The important new report "Transferring Privacy," released today by the European civil liberties groups Privacy International, Statewatch, the Foundation for Information Policy Research, and the European Digital Rights Initiative, is well worth the attention not only of Europeans but of Americans as well. Americans who care about freedom need to know what effect our government's policies are having in Europe - and how those policies are likely to circle back around to affect us.

Since 9/11, the United States has pursued an airline security strategy heavily oriented around the use of information. This has raised objections from Americans across the political spectrum, both because of the enormous privacy threat posed by such an approach as well as its dubious effectiveness in a world where our security agencies are already drowning in data that they can't process. Nevertheless, the U.S. government has pushed ahead with such schemes as the airline profiling plans CAPPS II (for Computer Assisted Passenger Prescreening System), a program built around a secret process for conducting background checks on every person who flies and rating them according to the risk that they supposedly pose to airline safety.

Indeed, the customers of Northwest and Jet Blue Airlines recently have received a jarring reminder of how little regard the U.S. has for their privacy and how little legal protection we have in the United States, when we learned that those airlines had secretly turned over millions of passenger records to the Federal Government for CAPPS II -like experiments.

The problem for the U.S. government, as it seeks to extend the reach of CAPPS II worldwide is that, like virtually every advanced industrial nation except the United States, Europe has in place an overarching privacy directive that gives the force of law to a set of privacy principles that are recognized around the globe as core to the dignity and freedom necessary for a democratic citizenry. Unlike the primitive privacy protections that Americans still live under, European privacy law does not permit personal information to be shared and traded willy-nilly by any government agency with a claim to a role in the war against terrorism.

Sadly, as the report lays out, our government's response to this conflict has been to push the Europeans to betray and abandon their own laws. In fact, the Bush Administration is asking the Europeans for data-sharing on terms that go well beyond what is needed for the airline security purposes it claims to be pursuing - and that go well beyond anything directed by Congress. The conflicts with European privacy rules include its demands for:

- A broad array of information about each traveler, including information that under European law is classified as "sensitive" and cannot be shared;
- The right to retain data for up to 50 years;
- Broad forms of access to information, including the right to direct electronic access to airlines' computer systems; and
- Weak forms of due process for any Europeans who are mistakenly or unfairly targeted by the system.

Americans interested in protecting privacy have always seen Europe as a shining example of the kind of legal regime that we need to fight for here. Unfortunately, instead of the Europeans'

civilized privacy regime rubbing off on the United States, it appears that our Wild West legal regime is instead rubbing off on them.

This report charts in dismaying detail how negotiators at the European Commission have buckled under to American pressure at the cost of their own citizens' privacy interests. After extended negotiations, the European Commission in December 2003 announced that an agreement had been reached with the United States. As the report shows, this agreement is a complete failure at protecting privacy interests:

- The Europeans declared U.S. privacy protections "adequate," a finding required under EU law for sharing data, despite the fact that the United States clearly does not meet the criteria for such a finding;
- Although the EU legal regime only permits data transfer for combating terrorism, the European Commission allowed the United States to use information for regular crimes as well;
- The Commission announced that the December 2003 agreement did not permit the United States to use European data for CAPPS II, and that would be negotiated separately. A few weeks later, however, the U.S. Department of Homeland Security declared that European records will be used to test CAPPS II. This even before a Congressionally mandated study of the likely privacy implications and effectiveness of CAPPS has even been completed;
- The Commission accepted a U.S. offer to retain European data for 3.5 years, far in excess of what EU regulations permit; and
- The Commission accepted a weak due process procedure that is entirely internal to the Department of Homeland Security, whereas EU rules require a true right to redress for citizens who believe their data is being abused.

When it comes to privacy protections, we want to join Europe, not have them join us.

In fact, the report makes it clear that we are not witnessing a battle between Europeans and Americans, but a battle between those in Europe and America who would like to construct an infrastructure for the global tracking and surveillance of individuals' movements, and those in Europe and America who believe that such a course is dangerous to freedom and an unpromising means of stopping terrorists. If our own government prevails in Europe, it will come back to haunt us. According to the report, European anti-privacy forces are pushing to set up their own system for access to travel records; they will of course expect reciprocity from the United States (as will other countries), and personal information about Americans will join the worldwide stream of multilateral data sharing.

As Americans we must not only pressure our own government to stop exporting weak privacy policies abroad, but also to send a loud and clear message to Europeans and others that the Bush Administration's Homeland Security vision does not represent the wishes of most Americans, and that we recognize that the Europeans will be acting in the interests of American citizens, not against them, if they stand tall against our government on this issue.