Transferring Privacy and Inadequate Adequacy

Commission Fails in 'Negotiations'

On May 17, 2004 the European Commission approved the transfers of passenger data ('PNR') from the databases of EU carriers to the U.S. Department of Homeland Security. This 'approval' involved deeming the negotiated agreement as 'adequate' under EU privacy law.

This agreement is based on smoke and mirrors. The agreement was repeatedly deemed inadequate by legal experts and the European Parliament. The Commission was repeatedly admonished for its failure to uphold EU laws. The U.S. Department of Homeland Security repeatedly asked for more than it was statutorily authorized to. And yet, the negotiating credibility of the Commission is diminished as EU privacy law is rewritten.

This report outlines how the European Commission failed outright at protecting European interests and upholding EU laws within the negotiations with the U.S. Government. As a result, the U.S. Government managed to get the Commission to concede European privacy rights and to burden EU carriers, even while U.S. carriers and U.S. citizens are exempt from these rules.

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, and is not even part of the current agreement.
c. The European Commission is now considering the creation 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. There are no grounds in American law for such transfers from U.S. carriers.
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 Parliament and the European Court of Justice 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 European Commission has 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	Prior EU Privacy Requirements	Final 'Adequate' Agreement
Access to What?	'Passenger Name Records'	At the discretion of U.S. Customs, includes non-U.S. travel information. Estimated 50-60 fields of data.	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.
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'. To be used by the EU for customs and immigration.
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', but not legally binding.
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.
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. Not legally binding.
Compliance Reviews?	None	None promised.	Must be ongoing verification of compliance.	Yearly with the co-operation of the EU.

This agreement 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 data transfers are not adequate under EU law; 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 is logically impossible, and dishonest.

This inadequate and loose agreement is to be used as a first step to an EU-wide, and even global, surveillance system. The Commission has long been working at establishing a centralised register of EU travellers, and is using this agreement as the basis for gaining access to this data arbitrarily.

Other countries will certainly follow the U.S. lead. Even countries with more restrained PNR demands, such as Australia, now have every right to wonder why the EU is sharing so little under such stringent requirements when data is being shared 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 many grounds:

- It did not give due 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..
- 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,[1] Turkey, Tunisia,[2] Malaysia and Thailand.[3]

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, dangerous, and hypocritical.

---

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