CEPS Policy brief
No. 125 • March 2007

Inquiry into the EU-US Passenger Name Record Agreement

Elspeth Guild

Introduction

The collection, retention, manipulation, exchange and correction of personal data in Europe have once again become a matter of substantial interest. The last time the use of data constituted an important political issue in Europe, in the 1970s, the result (at the European level) was the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, which opened for signature in 1981. This Convention, to which all EU member states are party, still sets the standard for data use in Europe.

The EU adopted Directive 95/46 on data protection, based largely on the Council of Europe's standard, which had to be transposed by the member states by 25 October 1998.[1] The Commission prepared a first report on its transposition in 2003. The European Data Protection Supervisor was created in 2001 to provide an independent body to ensure that the fundamental rights and freedoms of individuals – in particular their privacy – are respected when the EC institutions and bodies process personal data or develop new policies.

Since the attacks in the United States of 11 September 2001, data use has once again moved up the political agenda. The combination of very substantial technological advances in the collection, retention, use and storage of data and the heightened concerns about security provided a new environment for data issues. One of the outcomes of the new environment was the decision by the US authorities to collect and retain data on individuals coming to the US by air – a measure intended to increase US security.[2] This US legal act, however, had consequences for data protection in the EU. In order to provide a common basis for the transmission of personal data by EU transport companies to the US authorities, an agreement was entered into between the EU and US on 28 May 2004 regulating the field. The agreement was attacked before the European Court of Justice by the European Parliament on a number of grounds, not least the inadequacy of protection of individual data. On 30 May 2006, the European Court of Justice found that the agreement had been adopted on the wrong legal basis and gave the parties until 30 September 2006 to adopt a new agreement on the correct basis.[3]

On 6 October 2006, the Council adopted a decision to enter into a new agreement with the USA regulating PNR and the new EU-US agreement was published on 11 October 2006 (though subject to language checks).[4] In this note I will address some of the issues that arise as a result of the new agreement, in particular, the differences between the first agreement and the new one that affect the protection of data.

The key issues regarding the new agreement

The EU and US took the opportunity of the need to adopt a new agreement to include a number of changes to it, despite the fact that the agreement is a temporary one and new negotiations will begin soon to replace it. For the EU, the original PNR provision consists of three main documents – the Council Decision approving signature, the Agreement and the Undertakings of the Department of Homeland Security of 11 May 2004. The new provision includes the Council Decision, which is now substantially developed, the Agreement which largely remains the same (though there are some changes of significance) and a letter of interpretation dated 11 October 2006 from the US Department of Homeland Security, which effectively unilaterally amends the Undertakings in so far as the letter states how the US authorities interpret

[1] It has now been augmented by Directive 2002/58.

[2] The US Aviation and Transportation Security Act 2001.

[3] For a detailed discussion of the issues of the PNR decision, see E. Guild and E. Brouwer, *The Political Life of Data: The ECJ Decision on the PNR agreement between the EU and the US*, CEPS Policy Brief No. 110, Brussels, July 2006.

[4] Council Document 13216/06.

Elspeth Guild is Professor at Radboud University, Nijmegen and Associate Senior Research Fellow at CEPS.

This paper was originally submitted as written evidence to the European Union Select Committee, Sub-Committee F (Home Affairs) of the UK House of Lords.

About CEPS

Founded in Brussels in 1983, the Centre for European Policy Studies (CEPS) is among the most experienced and authoritative think tanks operating in the European Union today. CEPS serves as a leading forum for debate on EU affairs, but its most distinguishing feature lies in its strong in-house research capacity, complemented by an extensive network of partner institutes throughout the world.

Goals

- To carry out state-of-the-art policy research leading to solutions to the challenges facing Europe today.
- To achieve high standards of academic excellence and maintain unqualified independence.
- To provide a forum for discussion among all stakeholders in the European policy process.
- To build collaborative networks of researchers, policy-makers and business representatives across the whole of Europe.
- To disseminate our findings and views through a regular flow of publications and public events.

Assets

- Complete independence to set its own research priorities and freedom from any outside influence.
- Formation of nine different research networks, comprising research institutes from throughout Europe and beyond, to complement and consolidate CEPS research expertise and to greatly extend its outreach.
- An extensive membership base of some 120 Corporate Members and 130 Institutional Members, which provide expertise and practical experience and act as a sounding board for the utility and feasability of CEPS policy proposals.

Programme Structure

CEPS carries out its research via its own in-house research programmes and through collaborative research networks involving the active participation of other highly reputable institutes and specialists.

Research Programmes

Economic & Social Welfare Policies
Energy, Climate Change & Sustainable Development
EU Neighbourhood, Foreign & Security Policy
Financial Markets & Taxation
Justice & Home Affairs
Politics & European Institutions
Regulatory Affairs
Trade, Development & Agricultural Policy

Research Networks/Joint Initiatives

Changing Landscape of Security & Liberty (CHALLENGE)
European Capital Markets Institute (ECMI)
European Climate Platform (ECP)
European Credit Research Institute (ECRI)
European Network of Agricultural & Rural Policy Research Institutes (ENARPRI)
European Network for Better Regulation (ENBR)
European Network of Economic Policy Research Institutes (ENEPRI)
European Policy Institutes Network (EPIN)
European Security Forum (ESF)

CEPS also organises a variety of activities and special events, involving its members and other stakeholders in the European policy debate, national and EU-level policy-makers, academics, corporate executives, NGOs and the media. CEPS' funding is obtained from a variety of sources, including membership fees, project research, foundation grants, conferences fees, publication sales and an annual grant from the European Commission.

E-mail: info@ceps.be
Website: http://www.ceps.be
Bookshop: http://shop.ceps.be

CENTRE FOR EUROPEAN POLICY STUDIES

Place du Congrès 1 • B-1000 Brussels
Tel: 32(0)2.229.39.11 • Fax: 32(0)2.219.41.51

the provision of the Undertaking and makes certain changes to the Undertakings. Twelve issues, summarised below, were identified as key regarding the new agreement and its interpretation.[5]

Push-pull. Under the first agreement, the US authorities (in the form of the Homeland Security Department) had the power to enter the databases of carriers and to pull out information (limited to the 34 specified items in the Undertaking) that it wanted. The reason for this was that European carriers did not have in place the technology to deal with the preferable (from the perspective of data protection) system of 'push' – whereby the US authorities would have to make a request and the carriers would provide the specified information. It was agreed in 2004 that the system would move to a push one as soon as the technology was in place. According to a report by the EU Working Party on Protection of Individuals regarding the Processing of Personal Data, dated 14 June 2006, all the technical requirements are in place for a push system to be implemented. Nonetheless, the new agreement states that US authorities should be allowed to access data directly.

Time limits and frequency. Under the 2004 agreement, the US authorities had only 72 hours before a flight to seek data and a limit on the number of times it can check data. Under the new agreement, the 72-hour limit is no longer final and there is no limit on the number of times the US authorities can check the data.

Purpose limitation. The purposes for which data could be used were already fairly wide in the first agreement, including of course preventing and combating terrorism, related crimes, serious crimes that are transnational in nature, flights from warrants or custody for the designated crimes. In the second agreement as augmented by the letter of understanding, the data may also be used in the context of infectious disease for the protection of vital interests, which itself is subject to a wide scope.

Sharing data. The new agreement and its various associated documents widen substantially the number of agencies with which the US authorities may share data. It is not entirely clear whether the EU authorities have a clear description of the agencies which may be provided with data on EU citizens.

Number and nature of the data. The letter of understanding states that the US authorities must have the option to seek additional data, particularly if the system moves to a push rather than a pull format. This of course raises questions as to whether the US authorities have been strictly complying with the limit on the data they are permitted to obtain under the pull system. The Working Party on Protection of Individuals with regard to the Processing of Personal Data in its report of 14 June 2006 specified that only 19 data items were, its opinion, appropriate for sharing (and the list of 19 differs not only in number but in elements from the list of 34 under the current agreement).

Data retention. Under the initial agreement, data had to be destroyed after 3.5 years (at least in principle). In the new agreement's letter of understanding, the US authorities indicate that as no data will actually have had to be destroyed before the end of the current agreement "questions of whether and when to destroy PNR data collected in accordance with the Undertakings will be addressed by the United States and the European Union as part of future discussions."

Evaluation. A joint evaluation took place in May 2004. The report of this evaluation is not public, though it would be very helpful if it were released, as no doubt it would reassure EU citizens as to the propriety of data use by the US authorities. In the new agreement, doubt is cast over whether there will ever be another joint evaluation.

Data protection. The Council has determined that the US authorities follow satisfactory procedures for protecting EU data. Questions can nevertheless be raised about whether this is in fact the case.

Legal position of EU citizens. Procedures need to be put in place to inform EU citizens of the transfer of their data and to ensure they have information should they wish to complain. A detailed legal analysis is needed to establish the level of protection of data and the potential gaps.

Legal status. It is very unclear what the legal status of the 'letter of understanding' is. It appears not only to interpret the agreement and the Undertakings but to amend them and point to changes the US authorities will seek in the future.

Democratic and parliamentary scrutiny. This is a very intra-EU issue, the result of the European Court of Justice Decision. The new legal base for the agreement does not provide a role for the European Parliament. As preparations are already taking place towards the negotiation of yet another agreement to replace the current one, the European Parliament is concerned about how its views will be taken into account.

Implications for transfer of other data. There are concerns about the consequences of the PNR agreement for other data transfer agreements.

The foregoing issues provide an impressive list of concerns that have been voiced by the European Parliament's rapporteur. However, it does not cover all of the issues that the new agreement raises, in particular, redress and protection of the individual.

Protecting the individual

As a result of the transfer of faulty data from the Canadian authorities to their US counterparts, Maher Arar, a dual Canadian/Syrian citizen was stopped when in transit in New York on his way to Canada, on suspicion of terrorist involvement in September 2002. He was sent to Syria where he was detained and tortured for over a year. When he finally returned to Canada in October 2003, a federal inquiry led by a retired Supreme Court judge was established to determine how this had happened. The inquiry published its findings in September 2006, which exonerated Mr Arar of any suspicion of involvement with terrorist activities and found serious flaws in the manner in which data had been transferred by Canadian services to their US counterparts and on the basis of which Mr Arar was suspected by the US authorities of involvement with terrorism. On 26 January 2007, the Canadian Prime

[5] Letter of 10 October 2006, from Sophie in't Veld, MEP and rapporteur for the EU-US Agreement on PNR, to Commissioner Franco Frattini.

Minister issued a formal apology to Mr Arar and offered him compensation in the amount of CAN$10.5 million.

Inaccurate data transmission can have horrifying consequences for the individual, as in the case of Mr Arar. It can also be very expensive for governments.

The new EU-US PNR Agreement contains an innovation over its predecessor in that it states "this Agreement does not create or confer any right of benefit on any other person or entity, private or public". Is this to be understood as seeking to deprive someone like Mr Arar from obtaining redress in the event that his data are improperly transmitted and used? If so this is a very unfortunate attempt by the parties to deny responsibility for their acts.

The new Council Decision approving the Agreement also contains a new Article 4 that states that member states may exercise their existing powers to suspend data flows to the US authorities in order to protect individuals with regard to the processing of their personal data in two cases:

- Where a competent US authority has determined that the Department of Homeland Security is in breach of the applicable standards of protection; or
- Where there is a substantial likelihood that the applicable standards of protection are being infringed, there are reasonable grounds for believing that the DHS is not taking or will not take adequate and timely steps to settle the case at issue, the continuing transfer would create an imminent risk of grave harm to data subjects, and the competent authorities in the member states have made reasonable efforts in the circumstances to provide DHS with notice and an opportunity to respond.

The first part of this article moves responsibility for determining data breaches to the US authorities in accordance with their laws. As the person who will be affected is the EU citizen, this may not be entirely satisfactory. As was the case for Mr Arar, the US authorities have refused even to entertain the request by the Canadian authorities for information regarding his treatment, let alone participate in determining the truth or compensating Mr Arar for the damage that their action caused him.

The second part of the provision moves responsibility for protection of citizens of the Union to their national governments. In terms of EU solidarity, this is very unfortunate as it clearly and unambiguously breaks the common responsibility of the member states to protect their citizens. Further, it places the bar exceedingly high in respect of a decision to cease participation in the data provision system. It also permits one member state to determine that the US authorities are not applying the required standard of protection but it does not provide for any solidarity from the other member states. If this is a common agreement, then the commitments must be common as well.

If citizens of any member state are at risk of treatment similar to that which the US authorities meted out to Mr Arar, all member states should be engaged in the protection of that citizen and act in solidarity to protect all citizens of the Union against harmful use of personal data.