Controlling foreigners, passengers, citizens: surveillance and counter-terrorism

French version published in *Cultures et Conflits*, no 58, summer 2005, pp.155-182 (*'Controle des étrangers, des passagers, des citoyens: surveillance et anti-terrorisme'*, also accessible at www.conflits.org/document1829.html)

Valsamis Mitsilegas
Department of Law
Queen Mary University of London
v.mitsilegas@qmul.ac.uk

Introduction

Recent years witnessed calls for the intensification of surveillance and monitoring of the movement of people globally. These calls, led in particular by the US after the 9/11 events, were also echoed in EU Member States. The attacks in Madrid on 11 March 2004 have led to the multiplication and increase in the volume of these echoes, and gave fresh impetus to proposals for concerted action at EU level. Gathered under the heading of 'border security', these proposals called for the transmission of personal data of passengers travelling to the EU from third countries, and from the EU to the US, by airlines to the competent border control and immigration authorities. They also called for the enhancement of document security, by introducing biometric identifiers into visas and identity documents, and the enhancement of the technical capacity and interaction between various databases containing such data, so they can exchange such data more efficiently (in the EU the not so attractive term used for this is 'interoperability').

This intensification of surveillance of movement, realised by both 'widening' (by increasing the transmission of data) and 'deepening' (by introducing biometrics) controls, appears to be at odds with the minimisation of checks within the EU as a borderless area. The standards it entails, but also the manner in which these standards have been proposed and adopted, further raise a number of questions regarding legitimacy, democracy and the protection of fundamental rights in the EU. These questions become more complex in the light of the 'global' dimension of information

gathering and exchange post 9/11. The aim of this paper will be to address these questions, by analysing the negotiations, content and implications of recent EU proposals in the field.

The 'Advance Passenger Information' Directive

The proposal for this Directive was tabled not by the Commission, but by the Spanish Government, in March 2003.[1] Its original draft called on air and sea carriers to transmit a wide range of passenger data to border control authorities at their request, in advance of departure. These data would include *inter alia* the number and type of travel document used, nationality, the passenger's full name and date of birth and the border crossing point of entry into the territory of the Member States. The draft also gave discretion to Member States to require carriers to transmit to immigration authorities similar information on passengers who have not used their return tickets. Non-complying carriers would face monetary sanctions.[2]

Placing additional obligations on carriers was not included in the Commission's plans for developing action to combat illegal immigration. In June 2003, three months after the tabling of the proposal by the Spanish Government, the Commission published a Communication,[3] which would be taken into account by European leaders discussing the development of a common EU policy on illegal immigration in Thessaloniki later that month. It was stated in the Communication that there was no immediate need for new harmonising measures regarding carriers' liability.[4] Likewise, the Conclusions of the Thessaloniki European Council contained no reference to carries' liability, or to the need to intensify the surveillance of passengers.

However, while there was no widespread EU agreement on such initiatives at the time, there were moves by certain Member States to intensify controls on persons moving into –and within – the EU. In the summer of 2003, the (also conservative)

[1] OJ C 82, 5.4.2003, p.23.
[2] Ibid. For a detailed analysis see House of Lords, EU Committee, *Fighting illegal immigration: should carriers carry the burden?*, 5th Report, session 2003-04, HL Paper 29.
[3] *Communication on the development of a common policy on illegal immigration, smuggling and trafficking of human beings, external borders and the return of illegal residents*, COM (2003) 323 final, Brussels 3 June 2003.
[4] Ibid., p.11.

Italian Government tabled two third pillar proposals for a Resolution on security at European Council meetings and other comparable events; and a Decision (later converted into a Resolution) on the use by Member States of bans on access to venues of football matches with an international dimension. These measures were perceived as necessary to address protests during various political events (such as meetings of the European Council or the G7) and hooliganism respectively. They involve enhanced checks on individuals and can result in banning individuals, on the basis of their 'dangerousness', from entry in EU Member States (stopping thus movement even within the borderless Schengen area) or from entry into football stadiums.[5] Both measures call for enhanced police co-operation on the basis of risk-based profiling of individuals. The Resolution on bans from football matches was adopted in November 2003,[6] while the more controversial Resolution on security in Council meetings was adopted on the same day as the carriers' Directive.[7]

The carriers proposal was justified, and ultimately adopted, under Articles 62(2)(a) and 63(3)(b) of the EC Treaty. These serve as the legal basis for the adoption of measures relative to external border controls and illegal immigration respectively. Similarly Article 1 of the finally adopted text[8] states that the Directive 'aims at improving border controls and combating illegal immigration by the transmission of advance passenger data by carriers to the competent national authorities'. However, as the proposal was a Member State, and not a Commission, initiative, it was not accompanied by a detailed Explanatory Memorandum setting out its objectives and how these would be achieved by the provisions included in the proposal.

In the examination of the proposal by the House of Lords EU Committee, this point was raised by a number of witnesses, who questioned the effectiveness of the proposal

[5] The checks under the Resolution on security in Council meetings are additional to the power of Schengen Member States to reintroduce border controls in cases of emergency (Article 2(2) of the Schengen Convention). This may represent a shift from the exceptional reintroduction of blanket border checks to the regularisation, through the Resolution, of controls on specific individuals on a risk analysis basis.
[6] C 281, 22.11.2003, p.1.
[7] C 116, 30.4.2004, p.18.
[8] Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, OJ L 261, 6.8.2004, p.24.

to achieve its stated aims.[9] This point was rebuffed by the UK Government which argued that the draft Directive would assist in the identification of passengers who subsequently arrive undocumented and of passengers who are travelling with lost or stolen passports.[10] This argument did not convince the Committee, which took the view that an adequate case for the need for the proposal had not been made.[11]

Although the text of the Directive – notwithstanding the above objections – states as its aim combating illegal immigration, there have been attempts to frame it also as a national security/counter-terrorism matter. This was undoubtedly the view of the UK Government. In her evidence to the House of Lords EU Committee, Caroline Flint, a Home Office Minister, argued that the proposal 'is all about border control, whether it is illegal immigration or criminals coming in, or people who are a threat to national security'.[12] In her response to the Committee's Report, the Minister reiterated that the Government considers the proposal necessary and justifiable 'for the purpose of identifying known immigration and security threats'.[13]

The framing of the proposal as a counter-terrorism/national security measure would seem to cast doubt to the *legality* of its adoption solely under the first pillar. It could be argued that, similarly to certain Schengen-building proposals, the transmission of Advance Passenger Information, if justified as a border control AND a counter-terrorism measure, would necessitate a dual legal basis in both the first and the third pillar. This would also necessitate two distinct legal instruments, a 'Title IV' (first pillar) Directive and a 'Title VI' (third pillar) Framework Decision.

The framing of the proposal as a national security/counter-terrorism measure would also have substantial implications for the assessment of its *proportionality* to the

[9] Most prominently by the Immigration Law Practitioners' Association (ILPA)- evidence reproduced in *Fighting Illegal Immigration* – see fnote 2.
[10] *Ibid.*
[11] *Ibid,* para. 10. In response to the points made by the Government, the Committee noted that 'It is doubtful, however, whether the transmission of passenger data prior to boarding will assist the identification of such passengers. If they arrive without documents, it will be difficult to identify the flight on which they travelled and so establish a link with the information provided at check-in. It is also doubtful whether the proposal would help to detect passengers travelling with false documents, since it seems unlikely that such people would choose to travel in the identity of someone already on the list of inadmissible passengers.'
[12] *Ibid,* para. 9.
[13] Letter of 1 April 2004, in House of Lords EU Committee, *Government Responses*, 26th Report, session 2003-04, HL Paper 164, p. 13.

intended aim. The proposal has been criticised for being disproportionate to the achievement of its stated aims of enhancing border controls and combating illegal immigration.[14] However, these objections might seem less well founded if the measure was justified as necessary to combat terrorism – an aim that could be argued to necessitate intensive counter-measures and, in this case, justify the routine transmission of personal data to immigration/border authorities. It was indeed a proportionality objection that Caroline Flint was addressing by framing the proposal as a security measure in her response to the House of Lords EU Committee Report. In the same letter, she noted that 'proportionality is inextricably linked to the purpose for which the data is collected'.[15]

These considerations had a direct impact in the negotiations and the *content* of the proposal, most notably in the area of data protection. Article 6 of the Directive (on 'data processing') has been subject to long and controversial negotiations reflecting different national approaches on how far data exchanged under the Directive should be protected. Shortly before the adoption of the Directive, an agreement appeared to have been reached on strict data protection standards, including purpose limitation (transmission of data for the purpose of facilitating the performance of border checks with the objective of combating illegal immigration more effectively), limits to authorities having access to data (border authorities) and to the retention of data (which should be deleted by border authorities within 24 hours from transmission and by carriers within 24 hours from arrival). However, after pressure from the UK, two significant inroads were made to these standards:

- data would be deleted by border authorities within 24 hours from their transmission 'unless the data are needed later for the purposes of exercising the statutory functions of the authorities responsible for carrying out checks on persons at external borders in accordance with national law and subject to data protection provisions under Directive 95/46/EC'
- Member States may also use personal passenger data for law enforcement purposes[16]

[14] See House of Lords Report, fnote 2, pp. 8-9.
[15] See fnote 12 above.
[16] See Council document 7595/04, Brussels, 23 March 2004, where these changes were introduced.

It is clear that these additions render the pre-existing limits to access to and retention of data, as well as purpose limitation, virtually meaningless. Unsurprisingly, the insertion of these additional clauses to the text was hailed as a success by the UK Government, as it would align the Directive to the UK 'multi-agency' approach which links border checks with the fight against illegal immigration, crime and terrorism.[17] This link between immigration controls and law enforcement operations is explicitly made in Article 6 of the Directive, something that seems at odds with the justification of the proposal as a Title IV-immigration and border controls measure. The link between immigration and national security is also made in the Preamble of the Directive, in a provision ironically designed to assuage data protection concerns.[18]

Another field on which the link between the proposal and security considerations has had impact on has been the *democratic scrutiny* of the Directive, the handling of which by the Council and EU Member States left much to be desired. Two factors form the background to this handling of scrutiny. The first is the fact that the proposal was tabled by a Member State, and not by the Commission. According to the Amsterdam Treaty, such proposals in this field would be valid only up to five years after the entry into force of the Treaty (on 1 May 1999). This meant that, if agreement on the Directive was not reached by 30 April 2004, the proposal would fall. The second factor was the Madrid bombings of 11 March 2004. These led almost two weeks later to the European Council Declaration on terrorism, in which the adoption of the API Directive was prioritised.

These factors led to the acceleration of procedures to adopt the Directive, notwithstanding opposition by the European Parliament. The European Parliament had to be consulted on the Directive, but finally the Council adopted the Directive,

[17] See letter by Caroline Flint of 1 April, fnote 12 above. See also the UK border control strategy in the Home Office recently published Five year strategy for asylum and immigration (Cm 6472). The UK Government states therein that it will introduce legislation to enable data exchange between the Immigration Service, HM Customs and the police (para. 58). Extensive reference is made to the UK Government's e-borders programme, which will create 'a joined-up modernised intelligence-led border control and security framework' enabling interagency co-operation 'to maintain the integrity of our border control, target activity against those who have no right to be in the UK and assist in the fight against terrorists and criminals' (annex 1).

[18] Recital 12 notes that it would be legitimate to process transmitted data for the purposes of allowing their use as evidence in proceedings aiming at the enforcement of immigration laws, 'including their provisions on the protection of ordre public and national security'.

without having consulted the Parliament.[19] In the UK, the Government decided to override the parliamentary scrutiny reserve by the House of Lords EU Committee, which expressed its opposition to the measure as drafted. Ms Flint prayed in aid the post-Madrid urgency to adopt the Directive and the institutional difficulties with the proposal being a Member State initiative. She said:

'Against this background, the UK found itself in a doubly difficult position as we approached the end of the negotiation. We did not have parliamentary clearance for this measure and we were alone among Member States in continuing to have substantive reservations about the text itself. In the light of the new urgency to agree the directive, following the Declaration on Countering Terrorism, we intensified our efforts to get agreement to the changes we considered essential. At the March JHA Council, we gained these changes, thanks to the support from two or three key Member States and in the face of considerable opposition from another Member State. In the context of our wider EU relations it would have gone down very badly if we had subsequently blocked adoption of the Directive in April, thus causing it to fall'.[20]

The Directive was thus adopted on 29 April 2004, one day before the Amsterdam deadline would expire. The text no longer requires the transmission of data on return tickets and the Directive only applies to air carriers. But the obligation for them to transmit personal passenger data (such as names and date of birth, but also the departure and arrival time of the flight) to border control authorities remains, and the transmission of such data is subject to the not very strict data protection safeguards mentioned above. By linking border controls and the fight against illegal immigration with the fight against crime and terrorism, the Directive paves the way for the routine transmission of every day personal data to a number of State authorities in EU Member States, which can then start building the profile of all those travelling into the EU.

[19] The background is also discernible in recitals 2-6 of the Directive Preamble. It is stated therein that 'the Council has exhausted all possibilities to obtain in time the opinion of the European Parliament' and that 'under these exceptional circumstances the Directive should be adopted without the opinion of the European Parliament' (recitals 5 and 6 respectively).
[20] Letter by Caroline Flint to Lord Grenfell, 11 May 2004, published in House of Lords EU Committee, *Correspondence with Ministers*, 25th Report, 2003-04, HL Paper 140.

The EC/US PNR Agreement

Responding to the 9/11 attacks, the United States passed legislation in November 2001, requiring air carriers operating flights to, from or through the US to provide US Customs with electronic access to data contained in their automatic reservation and departure control systems.[21] This data, known as Passenger Name Records (PNR), constitutes a record of each passenger's travel requirements and contains all the information necessary to enable reservations to be processed and controlled by the booking and participating airlines. PNR data can include a wide range of details, from the passengers' name and address to their email address, credit card details and on-flight dietary requirements. PNR is thus broader than the API data which airlines flying to the EU were obliged to transmit following the Directive analysed in the previous chapter. Furthermore, US law required giving access to US Customs authorities to airlines' databases (a 'pull' system), unlike the Directive which required airlines to transmit API data by the end of check-in (a 'push' system).

The US legislation is applicable to all flights to the US, including flights from the EU. EU airlines would thus have to comply with the legislation if they did not want to be subject to heavy fines, leading even to the cancellation of landing rights at US airports. However, concerns were voiced in the EU that US legislation was too invasive of privacy and could be in conflict with Community and Member States' data protection standards. The Commission informed the US authorities of these concerns and this led to the entry into force of the US legislation to be postponed until 5 March 2003. At the same time, the Commission began negotiations with US authorities in order to formulate standards governing the transfer of PNR data to the US which would comply with EC data protection standards. In the course of negotiations, the European Parliament adopted a series of Resolutions urging the Commission to ensure that these standards are fully respected.[22] The US requirements

[21] Title 49, US Code, section 44909(c)(3) and title 19, Code of Federal Regulations, section 122.49b. On the US response regarding border security see A. Ceyhan, 'Securite, frontiers et surveillance aux Etats Unis apres le 11 Septembre 2001' in 53 *Cultures et Conflits* downloaded from www.conflits.org
[22] See Resolutions P5_TA(2003)0097 and P5_TA(2003)0429.

were also scrutinised by the 'Article 29 Working Party' on data protection,[23] which was highly critical of US demands.[24]

Negotiations were protracted and lasted well beyond 5 March 2003, when US law formally entered into force vis-à-vis EU airlines. They resulted in an agreement between the Commission and the US authorities on 16 December 2003. Following a series of undertakings by the US authorities, the Commission accepted that US data protection standards in the context of PNR transfers were adequate. The Commission said so in a Communication issued that day, justifying its decision by stating that

'The option of insisting on the enforcement of the law on the EU side would have been politically justified, but…would have undermined the influence of more moderate and co-operative counsels in Washington and substituted a trial of strength for the genuine leverage we have as co-operative partners'. [25]

The Commission called for a global EU approach to the sharing of PNR data. On the issue of EU/US transfers, the Commission noted that the way forward was to establish a legal framework for existing PNR transfers to the US. This would consist of an 'adequacy' Decision by the Commission, certifying that the US data protection standards were adequate, followed by a 'light' bilateral international agreement between the Community and the US.

It is interesting to note that, although the US legislation was prompted by the 9/11 events and is viewed in the US as a counter-terrorism measure, in the EU it was dealt as a first pillar, 'internal market' measure and not as a third pillar, 'counter-terrorism' measure. This is presumably justified by the practical and commercial implications that US law would have on carriers, and served to place the Commission (and not the

[23] The Working Party was established under the 1995 EC data protection Directive (Article 29) and consists of Member States' Information Commissioners. Its role is advisory.
[24] Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data, 11070/03/EN, WP 78. The Working Party urged the Commission to ensure inter alia that the purposes of data transfer and the bodies having access to such data should be specified and that proportionality should be ensured not only in relation to these aspects but also regarding the categories of data to be transferred (including sensitive data) and data retention.

[25] Communication from the Commission to the Council and the Parliament, *Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach*, COM (2003) 826 final, Brussels, 16.12.2003, p.5.

Council or the Presidency/individual Member States) centre-stage in giving it the lead to negotiate the agreement with the US. Making the most of its mandate, the Commission is trying to consolidate its position as the EU and Member States chief representative in negotiating standards in the field – it does not seem accidental that the Communication on PNR also calls for a 'global' EU approach and discussions in international fora such as ICAO – where presumably it will be the Commission, and not the Council or Member States who will take the lead.

The 'first pillar' choice is also significant legally, as it led to the assessment of the 'adequacy' of US data protection standards – and thus the legality of PNR transfers by EU airlines – being made under the 1995 EC data protection Directive.[26] Article 25 of the latter provides for adequacy decisions to be taken not by the Council and the European Parliament under the ordinary EU legislative procedure, but under 'comitology', ie by a Committee consisting of representatives of Member States and chaired by the Commission. This is not the most transparent method of decision-making and leaves little, if any, space for parliamentary scrutiny. In the UK, drafts of the adequacy Decision were not submitted for scrutiny by the Government to the EU Committees of the Houses of Parliament, notwithstanding the existence of specific requests to that effect.[27]

The draft adequacy Decision was examined by the Article 29 Working Party on Data Protection.[28] In an Opinion published in January 2004, the Working Party expressly stated that 'the progress made does not allow a favourable adequacy finding to be achieved'.[29] The Working Party justified this opinion by putting forward in detail a number of objections to the proposed arrangements, the weightiest of them being that:

[26] OJ L 281, 23.11.1995, p. 31.
[27] In a letter to the UK Government of 12 February 2004, Lord Grenfell, Chairman of the House of Lords EU Committee, stated that ' in view of the very serious concerns to which this proposal gives rise, it is of the utmost importance that the Committee is provided with ample time to scrutinise fully the proposal for the Commission 'adequacy' Decision'. Lord Filkin, Minister at the Department for Constitutional Affairs, sent his apologies for the Government not having identified this proposed decision 'as being of such importance as to trigger the exceptional arrangements for the deposit for scrutiny of Commission comitology legislation'. Letter to Lord Grenfell of 26 February 2004. Both published in House of Lords EU Committee, *Correspondence with Ministers*, in fnote 19.
[28] The Working Party has a mandate to do so under Article 30(1)(b) of the data protection Directive.
[29] Opinion 2/2004 on the Adequate Protection of Personal Data contained in the PNR of Air Passengers to be transferred to the United States' Bureau of Customs and Border Protection (US CBP), adopted on 29 January 2004, doc. 10019/04/EN, WP 87.

- transfer of PNR data is an exception to the data protection fundamental principle of purpose specification, taking into account the number and sensitivity of data involved and number of passengers affected –at least 10-11 million per year
- this leaves open the possibility of 'data mining' and entails the risk of generalised surveillance by a third State
- the Undertakings provided by the US authorities are not legally binding – paragraph 47 of them states that they 'do not create or confer any right or benefit on any person or party, private or public'
- the arrangements challenge the principle of 'purpose limitation' – PNR data may be used for preventing and combating terrorism and 'other serious crimes that are transnational in nature' – the reference to 'other serious crime' is vague and the purpose is far broader than combating terrorism
- proportionality – the categories of transferred data are disproportionate
- the use of data derived from PNR data is vague- this can be done for 'legitimate counter-terrorism or law enforcement purposes'- but law enforcement purposes are unspecified
- data retention is excessive – this is three and a half years (from fifty! In the original US requirements)
- transfer to other authorities – a comprehensive list of the relevant authorities to which data may be transferred has not been provided
- there is a need to replace the 'pull' system envisaged in the arrangements by a 'push' system with airlines transmitting data to the US authorities[30]

Notwithstanding its limited role under the comitology process, the European Parliament adopted on 30 March 2004, a Resolution calling on the Commission to withdraw the draft adequacy Decision.[31] The European Parliament drew attention to many of the data protection points made above, and, on the issue of legality, noted that there was no legal basis in the EU permitting the use of PNR commercial data for public security purposes – there was a need, according to the Parliament, for a specific

[30] Ibid. Many of these concerns were taken up by the House of Lords EU Committee in its scrutiny of the proposal – see letter of Lord Grenfell to Lord Filkin of 12 February 2004, in fnote 19.
[31] P5_TA-PROV (2004) 0245

legal basis covering these cases. The draft adequacy Decision might well be a lowering of the data protection standards in the 1995 Directive.

The European Parliament also took the step of requesting an Opinion from the European Court of Justice on the compatibility of the draft PNR international agreement, which would be concluded after the adoption of the adequacy Decision, with the EC Treaty. The European Parliament would wait for the Court's Opinion prior to submitting their opinion on the agreement to the Council under the consultation process of Article 300 TEC. The Council set a deadline for the Parliament's response on 22 April, extending it eventually to 5 May 2004.[32] With the Court case pending, and the Parliament not having submitted its opinion, the Council decided to go ahead with the agreement without having received the Parliament's Opinion. In the Decision authorising the Conclusion of the Agreement, the Council evoked the urgency caused by the uncertainty for carriers and passengers (Preamble, recital 2).

A similar sidelining of parliamentary scrutiny occurred in the UK, where the Government decided, as in the case of the API Directive, to override the parliamentary scrutiny reserve of the House of Lords EU Committee. Lord Filkin justified the Government's decision by adopting a similar reasoning to the Commission. He also emphasised the importance of the agreement for the 'war on terror', stating that:

'the EU has recently reaffirmed its commitment to combating terrorism in the light of the horrific events in Madrid in March. The EU stands four square with the US on this. The present proposal offers the opportunity to demonstrate our commitment. We need to consider very carefully indeed what message we will be sending if we do not take it.'[33]

[32] Letter by Lord Filkin to Lord Grenfell of 27 April 2004, in House of Lords EU Committee, *Correspondence with Ministers*, fnote 20.
[33] Letter by Lord Filkin to Lord Grenfell, 11 May 2004, in House of Lords EU Committee, *Correspondence with Ministers,* fnote 20. The 'war on terror' arguments were also put forward by Lord Filkin in an earlier letter of 27 April, where he also stated that the US assurances offer adequate data protection and 'even were that not the case, the transfers would not necessarily be unlawful'. Ibid.

The Commission adequacy Decision was finally adopted on 14 May 2004.[34] This was followed three days later by a Council Decision authorising the President of the Council to sign the Agreement with the US on PNR transfers on behalf of the Community.[35] The terms of the Agreement and the US Undertakings have not changed from the draft that was so heavily criticised by the Article 29 Working Party and the European Parliament. According to these documents:

- 34 categories of PNR data are required by US Customs – these include name, address and billing address, email address, all forms of payment information, travel itinerary, frequent flyer information, travel status of passenger, no show information, one-way tickets, all historical changes to the PNR and 'general remarks'
- CBP will 'pull' passenger information from air carrier reservation systems until such time as air carriers are able to implement a system to 'push' the data to CBP[36]
- PNR data are used by CBP strictly for purposes of preventing and combating, terrorism and related crimes and other serious crimes that are transnational in nature[37]
- Storage of PNR data will take place for 3,5 years. Data which have not been manually accessed during this period, will be destroyed. Data which have been accessed will be kept for a further 8 years. These provisions will not apply to PNR data which are linked to a specific enforcement record.[38]
- CBP may provide data to other government authorities, including foreign government authorities, with counter-terrorism or law-enforcement functions, on a case-by-case basis, for the purposes of preventing and combating the above mentioned offences[39]

[34] Commission Decision of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection, OJ L 235, 6.7.2004, p.11. The Undertakings of the US Homeland Security Department are annexed in pp. 15 –21. The list of PNR data is annexed in p. 22.
[35] OJ L 183, 20.5.2004, p.83. The text of the Agreement is annexed in pp. 84-85. The Agreement was signed on 28 May 2004.
[36] Undertakings point 13. It is not clear how the legality of pulling data from carriers' systems will be monitored or how it will be ensured that extracting data from airlines' databases is limited to data on passengers on flights to or via the US.
[37] Undertakings point 3.
[38] Undertakings point 15.
[39] Undertakings point 29.

- In the event that a PNR requirement is imposed by the EU, CBP will, strictly on the basis of reciprocity, encourage US-based airlines to co-operate[40]
- The Undertakings will apply for a term of 3,5 years and may be extended/reviewed[41]
- The Undertakings do not create or confer any right or benefit on any person or party. Their provisions do not constitute a precedent for any future discussions with the Commission, the EU or third states[42]

It is thus evident that none of the concerns raised by the Article 29 Working Party has been addressed. The system of PNR transmission covers a vast amount of information and does justice to the WP claim that it constitutes generalised surveillance by a third State, leading to the profiling of individuals. The US requirements are disproportionate and appear to be contrary to fundamental data protection and privacy rights which are well established in Community law. The Commission emphasise the fact that they have achieved concessions from the US side, but the legal force of the US Undertakings is questionable. Concerns regarding the protection of privacy and personal data are exacerbated by the fact that the Agreement would permit the transmission of 'EU' PNR data from the US to third countries – leaving effectively the judgement of whether these countries can adequately protect human rights to the US authorities. The European Parliament has brought an action before the ECJ asking for the annulment of the Decision authorising the Conclusion of the EC/US Agreement, on the grounds of the latter infringing the right to privacy and data protection and breaching the principle of proportionality – but also on legality grounds.[43] The Court's ruling is awaited with great interest.

The Commission negotiations with the US highlight, as in other occasions, the dilemma of whether the EU should choose to co-operate with third countries speaking with one voice if this would mean that its own standards and values would be

[40] Undertakings point 45.
[41] Undertakings point 46.
[42] Undertakings points 47 and 48.
[43] The European Parliament argues that Article 95 TEC (on the internal market) is not the right legal basis for the contested Decision). It also argues that its assent should be required for the adoption of the Decision authorising the conclusion of the international agreement, and not its mere consultation as has happened. This is because, according to the parliament, the agreement constitutes an amendment of the 1995 data protection Directive. See Council doc.11876/04, Brussels, 6 August 2004.

compromised. [44] In the PNR data case, the Commission took the opportunity to represent Member States (by framing the issue as an internal market/first pillar matter) and may claim that arrangements are not one-sided, as the US Undertakings contain a clause on reciprocity. This clause is however conditional upon the implementation of a PNR identification system (similar to the one in the US) by the European Union – this may preempt the decision by the EU institutions on whether such a system is desirable in the EU (or indeed compatible with EC law and fundamental rights). Even if such a system is implemented in the EU, the Undertaking merely states that US Customs will 'encourage' US-based airlines to cooperate.[45]

In the PNR case, like in other cases, the legitimacy of what the EU negotiators have proposed and/or accepted as a compromise has been almost fatally undermined by the lack of transparency and the absence of any meaningful scrutiny by the European Parliament and national parliaments. It is unfortunate that the Commission and the Council chose to go ahead with the adequacy Decision and the Agreement within a tight timetable, notwithstanding the clear opposition from the European Parliament and national parliaments and the critical comments by the Article 29 Working Party. This is yet another example where decisions have been taken under pressure manufactured by an emergency discourse. As in the case of EU measures adopted post-9/11 (such as the European Arrest Warrant), this perceived state of emergency was used to speed up the adoption of far-reaching proposals while minimising democratic scrutiny and control and sidelining thus uncomfortable objections that parliaments (and civil society) would raise. The Commission will, in 2005, present proposals for a common EU approach to the transfer of PNR data – one hopes that these proposals are subject to open and extensive dialogue, and subject to full parliamentary scrutiny in order to ensure that global co-operation does not undermine fundamental principles of EU and national laws. It remains to be seen whether the voice of the EU in the world is strong enough to uphold these principles and promote them in a spirit of 'reciprocity'.

[44] See V. Mitsilegas, 'The New EU/US Co-operation on Extradition, Mutual Legal Assistance and the Exchange of Police Data' in 2003 *European Foreign Affairs Review* 8/4, p.515.
[45] Undertaking 45.

Biometrics and databases

The US response to 9/11, which had 'border security' as one of its centrepieces, was largely replicated by European Union leaders after the Madrid bombings. In the Declaration on combating terrorism of 25 March 2004, the European Council linked the monitoring of the movement of people with the 'war on terror' by stressing that 'improved border controls and document security play an important role in combating terrorism'. There were two elements in this approach: the inclusion of biometrics in EU visas and passports, which should be prioritised and relevant measures be adopted by the end of 2004; and the enhancement of the interoperability between EU databases and the creation of 'synergies' between existing and future information systems (such as SIS II, VIS and Eurodac) 'in order to exploit their added value within their respective legal and technical frameworks in the prevention and fight against terrorism'.

None of these ideas were new. There was growing debate and policy pressure within EU institutions for EU action in the area post-9/11. In the Informal JHA Council in Veria on 28/29 March 2003, Ministers invited the Commission to table a proposal to integrate biometrics in visas. The then JHA Commissioner Antonio Vitorino also put forward the case for biometrics in EU passports. According to the Commission, this was even more necessary given the need to take a common approach towards new US legislation, which requires biometrics in passports of citizens of countries granted a visa waiver as from 26 October 2004. Some months later, in Thessaloniki, the European Council of 19/20 June called for a coherent EU approach on biometrics, 'which would result in harmonised solutions for documents for third country nationals, EU citizens' passports and information systems (VIS and SIS II)' and invited the Commission to present relevant proposals.[46]

The Commission – and subsequently the Council and the European Council – have thus evoked again US requirements in order to legitimise EU action in a contested field – and to broaden this field of action by extending the measures to the passports of EU citizens. By the time of the Madrid bombings, which added the 'war on terror'

[46] See the Explanatory Memorandum in the Commission proposal for a Regulation amending the uniform format for visas, COM (2003) 558 final, Brussels, 24 September 2003.

as a more explicit legitimacy factor for EU action, negotiations were in full force on the inclusion of biometrics in both visas and passports. This was notwithstanding the caution urged by the Article 29 Working Party, which raised the concern that the widespread use of biometric data may desensitise the general public to the effect that such use may have on everyday life and warned against the use of biometric identifiers which may leave physical traces (such as fingerprints) or that can be memorised.[47]

The Hague Programme, adopted by the European Council on 4/5 November 2004 maintained the momentum for the inclusion of biometrics by stating more clearly the link between movement, migration and terrorism – the first part of paragraph 1.7.2, which is worth quoting at length, provides that:

'the management of migration flows, including the fight against illegal immigration should be strengthened by establishing *a continuum of security measures* that effectively links visa application procedures and entry and exit procedures at external border crossings. Such measures are also of importance for the prevention and control of crime, in particular terrorism. In order to achieve this, a coherent approach and harmonised solutions in the EU on biometric identifiers and data are necessary'. [48]

The concept of the '(in)security continuum' in the EU (whereby immigration issues are linked with the fight against crime and terrorism), which was introduced by academics in response to the development of EU JHA policies in the 1990s,[49] thus appears in an official EU policy document – in fact the blueprint for EU action in JHA for the next five years. The difference is that, while the term was launched to highlight concerns regarding the direction of EU action towards discrimination and uncritical enforcement and the dangers for civil liberties this would pose, in the Hague Programme the continuum appears as a legitimate phenomenon, as a necessary response to the post 9/11 world. The controls of movement, crime and terrorism

[47] Article 29 Working Party, Working document on biometrics, adopted on 1 August 2003, doc. 12168/02/EN WP 80.
[48] Emphasis added.
[49] See the seminal work of Didier Bigo, in particular *Polices en Reseaux – l'experience europeenne*, Presses Sciences Po, Paris, 1996.

become one, and such controls are further prioritised and deepened by the use of measures having the maximum intrusiveness into the personal sphere – biometrics.

Political pressure towards the insertion of biometrics into identity documents has led to the adoption, in December 2004, of a Regulation introducing biometric identifiers (in the form of facial images and fingerprints) in EU passports.[50] Similarly to the carriers Directive the legal basis of the Regulation is Article 62(2)(a) TEC, on border controls, and similarly to the Directive, the Regulation was deemed to be a security measure.[51] The Regulation was finally adopted notwithstanding serious objections regarding the appropriateness of the legal basis and the existence of EC competence to adopt binding legislation on the content of identity documents. Existing EU measures take the form of non-legally binding Resolutions; Article 62(2)(a) refers to controls of the external border of the EU and not to the content of EU travel documents; and Article 18(3) TEC explicitly states that Community action to facilitate the exercise of citizenship rights does not apply to provisions on passports, identity cards, residence permits or any such document.[52] In spite of these legality concerns, and concerns on the proportionality of the measure,[53] negotiations on the measure went ahead and a second biometric identifier – fingerprints – was added. In spite of the reactions by the Article 29 Working Party[54], the Regulation was adopted swiftly thereafter in December 2004 – perhaps to pre-empt a greater say of the initially critical European Parliament, which would become a co-legislator with a

[50] Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, OJ L 385, 29.12.2004, p.1.
[51] See letter of 15 July 2004 by Home Office Minister Caroline Flint to Lord Grenfell, Chairman of the House of Lords EU Committee, stating that 'our view is that the current proposal is first and foremost a security measure'.
[52] See again the work of the House of Lords EU Committee: the points were raised in a letter of 21 October 2004 by Lord Grenfell, chairman of the Committee, to Caroline Flint. The UK Government (which ironically was excluded from participation in the Regulation by the Schengen Member States but is pushing ahead with its own domestic use of biometrics) argued that the legal basis is justified as common EU standards will facilitate border controls as the verification equipment at border checks must be capable of reading electronically the data in EU passports – letter by Caroline Flint to Lord Grenfell of 15 July 2004.
[53] On both concerns, see the detailed analysis by Statewatch, prepared by Steve Peers, *The Legality of the Regulation on EU Citizens' Passports*, 26 November 2004, in www.statewatch.org
[54] Letter of 30 November 2004 by Peter Schaar, chairman of the Working Party, to Josep Borrell Fontelles, chairman of the European Parliament. The Working Party expressed its reservations as to the use of 'biometric features such as fingerprints allowing 'one too many' identification and tracing of individuals'. The WP called for the respect of the fundamental right of privacy and of transparency and noted that 'due to the relevance of the measure to all our citizens the Article 29 WP considers it appropriate that public opinion should be widely sought on this matter to demonstrate that the decision-making process is based on a proper and comprehensive assessment'.

right to veto on the biometrics proposal from 1 January 2005 .[55] Work on biometrics in visas and residence permits is also continuing, notwithstanding a series of technical problems that have occurred.

Biometric data will be of value to enforcement agencies if they form part of databases which are easily accessible. It is thus no coincidence that in the EU, as in the US, calls for the introduction of biometrics went hand in hand with calls for facilitating their inclusion in databases and enhancing the 'interoperability' of these databases so that data would be easily exchanged. As mentioned above, biometrics and the interoperability of databases were linked in the European Council on various occasions, the latest being the Hague Programme. Again this is not a new development. The Commission has been developing for some years now the so-called second generation Schengen Information System (SIS II), with the aim of it including more and more detailed data (including biometrics), and enabling the interlinking of alerts and possible synergies with other systems like the Visa Information System (VIS). An example of how central this project is for the Commission is that a new unit on 'large-scale information systems' was created within the JHA DG on 16 December 2002.[56]

Work on the development of SIS II is ongoing, and so is work on the development of the VIS, one of its main potential 'interlocutors'. The JHA Council adopted detailed conclusions on the development of VIS in February 2004, stating clearly that one of the purposes of the system would be to 'contribute towards improving the administration of the common visa policy and towards internal security and combating terrorism'. The Council called for the inclusion of biometric data on visa applicants to VIS for verification and identification purposes, 'including background checks'. It also called for access to VIS to be granted inter alia to border guards and 'other national authorities to be authorised by each Member State such as police

[55] The need for the swift adoption of the proposal has also been justified on the grounds that the US would abandon its visa-waiver programme with its members in the EU which had not introduced biometrics in their passports by a certain date. Like in the PNR case, the EU has managed to obtain an extension to the US deadline for the insertion of biometrics, but this new US deadline will not be met and it is unlikely to be extended by the US (see letter of 31 March 2005 from the Chairman of the US House Judiciary Committee to the Commission and the Council, reproduced in www.statewatch.org).
[56] See the Commission Communication on the development of SIS II – COM (2003) 771 final

departments, immigration departments and services responsible for internal security'. Yet another example of the security continuum in EU policy discourse…

The Council adopted in June 2004 a Decision forming the legal basis for the establishment of VIS[57] and negotiations began to define its purpose and functions and formulate rules on access and exchange of data. There followed a very sceptical Opinion from the Article 29 Working Party, which reiterated its concerns regarding the processing of biometric data in VIS and noted that it has great proportionality reservations regarding the storage in databases of such data for the purpose of carrying out subsequent checks on illegal immigrants (which the February Council appeared to include in the purposes of VIS) – the requirements of the data protection Directive, the WP added, 'may not be circumvented by the introduction of broad, multiple purposes'. The WP raised a series of proportionality concerns regarding the inclusion of biometric data and VIS itself, and noted that some of the aims of VIS overlap with those of SIS II. It also asked to examine in good time proposals on interoperability between these systems.[58]

The Commission has recently tabled a draft Regulation aiming to take further VIS by defining its aims and rules on data access and exchange.[59] The proposal has been the outcome of extensive consultation and the Commission have tried hard to counterbalance the choice of a very invasive form of intervention (biometric data in the VIS) with clearly delimiting access to VIS and including in the text detailed provisions on data protection and a 'proportionality' provision that, while biometric visas can be scanned, they will not be routinely stored in the system. However, the logic of the security continuum can still be discerned, with Article 1(2)(a) of the proposal stating that one of the purposes of VIS is 'to prevent threats to internal security of any of the Member States'. The conclusions of the recent JHA Council of 24 February also raise concerns that the standards set out by the Commission will be

[57] Council Decision of 8 June 2004 establishing the Visa Information System (VIS), OJ L 213, 15.6.2004, p.5.
[58] Article 29 Working Party, Opinion No 7/2004 on the inclusion of biometric elements in residence permits and visas taking into account of the establishment of the European Information system on visas (VIS), doc. 11224/04/EN, WP 96, adopted on 11 August 2004.
[59] Proposal for a Regulation of the European Parliament and of the Council concerning the VIS and the exchange of data between Member States on short-stay visas, COM (2004) 835 final, Brussels 28.12.2004.

dismantled by Member States in negotiations – the Council calls for access to the VIS to be given to national authorities responsible for 'internal security', when exercising their powers in investigating, preventing and detecting criminal offences, including terrorist acts or threats. The Council invited the Commission to present a separate, third pillar proposal to this end. This not only reinforces the 'security continuum' approach, but would effectively sideline the European Parliament, which will co-decide with the Council on the first pillar VIS Regulation but will only be consulted in the third pillar instrument.

Under the banner of 'interoperability', we are moving thus towards a system where EU databases containing significant numbers of sensitive personal data can be interconnected and accessed by a number of different agencies. This is notwithstanding the fact that the various EU databases were constructed to serve very diverse purposes, ranging from the facilitation of the assessment of visa and asylum applications (VIS and EURODAC respectively) to police co-operation and counter-terrorism (aspects of SIS, Europol) – and notwithstanding the fact that they contain quite diverse categories of data. Interoperability – especially if it is justified under the blanket need for a 'war on terror' – renders any safeguard based on purpose limitation regarding access and use of these databases meaningless.

This complexity is further compounded by the fact that EU databases, because of their diversity, are created under different legal bases (first/third pillar) and are governed by different data protection regimes. These are very fragmented in the third pillar, where specific rules and specific supervision arrangements apply to specific bodies holding databases (such as Europol and Eurojust), with no general, across the board, standards or supervision. These piecemeal arrangements appear rather limited and ineffective in a climate where maximum access to personal data is facilitated and operational co-operation between the various agencies at the EU level (such as Europol, Eurojust, the European Borders Agency, the Police Chief's Task Force and SitCen) – but also at national level (including co-operation between police and intelligence agencies) is the centrepiece of EU action in JHA for the next five years.[60]

[60] See in particular the Hague Programme, sections 2.1-2.5.

Conclusion

The above analysis paints a bleak picture of the re-negotiation of the relationship between the individual and the State, in Europe and globally, as regards the control that the State can exert in the individual's private sphere. The net of State surveillance is widening and thickening in a variety of ways. Personal data is now gathered on all the population, and not merely on specific categories of suspect individuals – so surveillance shifts from specific to generalised. More data is collected from various sources, aiming to create a profile of individuals and to track their movements across the globe – their entry and exit in national (and Schengen) territories is monitored and recorded. Information is gathered before, during and after entry in these territories. The quality of information gathered has changed as well, with the State invading further the private sphere by collecting information on the very essence of one's humanity and identity, ie biometrics. Data transmission has shifted from reactive (with private companies responding to law enforcement requests on specific suspects) to proactive – for instance, data on all passengers must be transmitted by airlines to the authorities. All this leads to what Ericson and Haggerty have named 'the disappearance of disappearance', a process whereby 'it is increasingly difficult for individuals to maintain their anonymity or to escape the monitoring of social institutions' [61]– in this case the State abetted by the private sector.[62]

This massive intensification of surveillance has been legitimised by the 'war on terror'. Governments and law makers claim that everything is linked in a 'security continuum' in the post- 9/11 age. One needs to control equally immigration, crime and terrorism, as these phenomena – and their control – are linked. Along with the serious issues of criminalisation of migrants and demonisation of the Other that such an approach may entail,[63] the security continuum appears to pose an overwhelming

[61] K. D. Haggerty and R. V. Ericson, 'The Surveillant Assemblage' in 51/4 *British Journal of Sociology* (2000), p. 619. See also, especially on the shift of monitoring from reactive to proactive, M. Levi and D. S. Wall, 'Technologies, Security and Privacy in the post-9/11 European Information Society' in 31/2 *Journal of Law and Society* (June 2004), p. 194.

[62] David Lyon has pointed out that, despite the focus on developments in the private sector when analysing surveillance, the State remains relevant and can use the information gathered by 'private' surveillance. In 'Surveillance after September 11, 2001' in K. Ball and F. Webster (eds), *The Intensification of Surveillance*, Pluto Press, London, Sterling VA, pp.21-22.

[63] Didier Bigo has talked of 'satellite populations' who are deemed to be 'exceptional' and are thus excluded from their desired destination. See his 'Criminalisation of 'Migrants': the Side Effect of the

challenge to long-established legal principles and fundamental rights. In the current climate of the 'security continuum' it is very difficult to draw any line to safeguard personal data and thus the right to privacy and one's personality. Access by the State to non-police data is deemed proportionate 'to combat terrorism' (one of the many instances where legal standards are being bent or totally disregarded in the name of the 'war on terror'). There needs to be interoperability of various databases, even though these serve different purposes and contain different kinds of data, because all these data may help in the 'war on terror'. And this is why it is deemed essential that law enforcement authorities have access to these databases, even though they do not contain 'crime' data. In these circumstances, how can one possibly speak of 'purpose limitation' to the use of personal data?

Apart from the gloom and justified concerns that these developments may cause, they also pose a number of paradoxes for the EU and its Member States. The first relates to the relationship between the aim of a borderless Union on the one hand, where internal controls are abolished, and the intensification of controls and surveillance on the other (instead of them being abolished altogether). The second paradox relates to the co-existence of a push to create a European identity based on the rule of law and the protection of fundamental rights (with the Charter of Fundamental Rights as its flag) so that Europe can speak with one voice globally, with the willingness (or resignation?) of EU institutions to compromise these very principles when speaking with one voice in the negotiation of global standards. The third paradox relates to the question of whether the EU itself can protect and promote human rights in an age of fear by taking decisions transparently and democratically, while Member States lower standards domestically and are keen to avoid, where possible, parliamentary scrutiny at both the national and the EU level.

These paradoxes may seem hard to resolve, but there is space for optimism in the future. The main 'innovation' of the Hague Programme may have been the provisions on border security and interoperability of databases, but it also calls for the development of an EU data protection framework for the third pillar. While this will not at this stage address the fragmentation between the pillars, it provides Member

---

Will to Control the Frontiers and the Sovereign Illusion' in E. Szyszczak et al (eds). *Irregular Migration and Human Rights*, Brill, Leiden 2004, p.91.

States with an opportunity to revisit the existing data protection arrangements and develop meaningful protective standards, which may have to be adopted to address the more intensive and extensive character of data gathering and surveillance. Current standards are too piecemeal to address the generalised profiling of individuals and greater thought must be given to how to effectively protect the private sphere and whether it would be necessary to give Data Protection Authorities at national, EC and EU level greater powers and greater involvement in policy and law development.

The European Constitution may be a catalyst to increase the protection of the rights of the individual. It incorporates the Charter of Fundamental Rights – which includes a right to data protection – and abolishes the pillars. This will give the opportunity to the European Court of Justice to interpret Union law in the light of the rights to privacy and data protection, and the obligation of the Union to protect and respect fundamental rights. The Constitution may also give the EU a stronger voice in its relations with the outside world, and oblige it to respect EU standards in international relations. But most importantly, the Constitution will make decision-making in these areas more transparent and democratic, and give a say to voices that are currently dissenting but ignored (the European Parliament and national parliaments). Making decision-making more democratic, and involving the public, is crucial if EU action in the field has any legitimacy.

‘