

# Een vlucht passagiersgegevens.

*Over privacy als slachtoffer van de strijd tegen het terrorisme*

*In dit artikel wordt een beknopt overzicht gegeven van de eisen die de Amerikanen stellen met betrekking tot de overdracht van passagiersgegevens en de rol die de Europese Commissie daarbij gespeeld heeft. Daarbij ligt de nadruk op het "joint statement" van 18 februari 2003 en de afspraken van december 2003. Vervolgens wordt de toelaatbaarheid van de verschillende varianten van gegevensverstrekking beoordeeld in het licht van de relevante wetgeving, met name de privacyrichtlijn. Ook het omstreden CAPPS II systeem komt aan bod. Een en ander mondt uit in een eindoordeel over de toelaatbaarheid van de thans voorliggende voorstellen en de rol die de Commissie daarbij gespeeld heeft.*

Lodewijk Asscher\*

## 1. Inleiding

Het spreekt vanzelf dat de Amerikanen sinds de aanslagen van 11 september 2001 groot belang hechten aan vliegveiligheid en daarmee aan effectieve controle van passagiers. De *Aviation and Transportation Security Act* van 19 november 2001 en de *Enhanced Border Security and Visa Reform Act* van 14 mei 2002 hebben tot doel dat aspect van de Amerikaanse binnenlandse veiligheid te vergroten. Belangrijk onderdeel is de verplichting aan luchtvaartmaatschappijen die op de VS vliegen gegevens over de passagiers elektronisch te verstrekken. Luchtvaartmaatschappijen die niet aan deze eis voldoen lopen het risico een boete te krijgen van maximaal \$5000 per reiziger of om landingsrechten op de VS te verspelen.

## 2. De overdracht van passagiersgegevens: geschiedenis

De Amerikaanse douane eist sinds begin 2003 daadwerkelijk toegang tot de reserveringssystemen van luchtvaartmaatschappijen in de Europese Unie. Om mogelijke vragen over de verhouding van nieuwe maatregelen tot het privacyrecht weg te nemen gaven de Europese Commissie en de Amerikaanse douane een gezamenlijke verklaring uit, het zogenaamde *joint statement* van 18 februari 2003.<sup>1</sup> De Commissie gaf aan dat er voldoende waarborgen waren dat de privacy van passagiers beschermd bleef en dat er voldoende vertrouwen bestond in de intenties van de Amerikaanse douane. De bijlage bij het joint statement liet echter een andere werkelijkheid zien. Zo mochten de ontvangers van de persoonsgegevens ter gene zijde van de oceaan de bestanden doorgeven aan andere diensten in het kader van de terrorismebestrijding en de bestrijding van andere criminaliteit. Sommige gegevens zouden 50 jaar bewaard worden, terwijl onduidelijk was aan de hand van welke criteria passagiers geweigerd zouden worden.

Het Europees Parlement sloeg de Commissie in maart 2003 met een zeer kritische resolutie om de oren.<sup>2</sup> Daarin wordt opgeroepen de toegang tot de reserveringssystemen op te schorten.

---

\* mr L.F. Asscher is onderzoeker bij het Instituut voor Informatierecht, Universiteit van Amsterdam.

<sup>1</sup> Joint Statement by the European Commission/US Customs talk on Passenger Name Record (PNR) transmission, Brussels, 17/18 february 2003. [http://europa.eu.int/comm/external\\_relations/us/intro/pnr-joint03\\_1702.htm](http://europa.eu.int/comm/external_relations/us/intro/pnr-joint03_1702.htm).

<sup>2</sup> Resolutie van het Europees Parlement over de overdracht van persoonsgegevens door luchtvaartmaatschappijen bij transatlantische vluchten: de stand van zaken bij de

De mogelijkheid de Europese Commissie voor het Hof van Justitie te dagen werd nadrukkelijk aan de orde gesteld. De Commissie gaf aan het joint statement toch al niet als definitieve oplossing te hebben gezien maar als tussenstap. Hernieuwde besprekingen met de Amerikaanse autoriteiten werden aangekondigd.

Sindsdien vond in juni 2003 een conferentie plaats tussen de EU en de VS waarop over dit onderwerp is gesproken. In december 2003 werden de resultaten bekend van hernieuwde onderhandelingen tussen de Europese Commissie en de Amerikaanse autoriteiten.<sup>3</sup> In december 2003 verscheen tevens de *Commission's communication on the transfer of Passenger Name Record (PNR) data: a global EU approach*.<sup>4</sup> In januari kwam daar een nieuwe lijst Amerikaanse beloften bij.<sup>5</sup> In een toespraak tot het Europees Parlement liet eurocommissaris Bolkestein weten tevreden te zijn met de behaalde onderhandelingsresultaten.<sup>6</sup>

De artikel 29 Werkgroep heeft inmiddels drie keer geadviseerd over de overdracht van PNR gegevens. In een eerste advies uit oktober 2002 en een advies uit juni 2003 is de Werkgroep zeer kritisch over de Amerikaanse maatregelen.<sup>7</sup> In het advies van juni 2003 werd gereageerd op de toenmalige stand van onderhandelingen met de Verenigde Staten.<sup>8</sup> Het meest recente advies komt hieronder aan de orde.

De Commissie streeft er thans naar te komen tot een besluit in de zin van artikel 25 lid 6 van de richtlijn en tot het sluiten van een internationale overeenkomst. Doel is daarbij om dat alles tot stand te brengen per maart 2004 hoewel de Commissie zelf aangeeft dat dat streven wel eens te optimistisch zou kunnen blijken te zijn.<sup>9</sup>

### 3. Passagiersgegevens en derde landen

De uitvoer van persoonsgegevens naar derde (dat wil zeggen niet-EU) landen is slechts dan toegestaan indien in die landen een aanvaardbaar (adequaat) niveau van privacybescherming geldt. De verschillen tussen het Europese en het Amerikaanse privacyrecht zijn aanmerkelijk.<sup>10</sup> Op grond van de richtlijn zijn ondernemingen die persoonsgegevens willen uitvoeren naar derde landen verplicht zich ervan te vergewissen of die derde landen een adequaat niveau van gegevensbescherming kennen.<sup>11</sup> Als er geen sprake is van een adequaat beschermingsniveau kan de Commissie onderhandelingen aanknopen. Als daaruit blijkt dat het derde land afdoende maatregelen heeft genomen om een adequaat niveau te bereiken kan

---

onderhandelingen met de VS, PE 336.423\ 79.

<sup>3</sup> <http://www.useu.be/Terrorism/USResponse/Dec1603PNRAgreement.html>.

<sup>4</sup> Communication from the Commission to the council and the parliament, transfer of Air Passenger Name Record (PNR) data: a Global EU Approach.

<sup>5</sup> Undertakings of the United States Bureau of Customs and Border Protection and the United States Transportation Security Administration of 12 January 2004.

<sup>6</sup> Frits Bolkestein Member of the European Commission in charge of the Internal Market, Taxation and Customs 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, 16th December 2003, DN: SPEECH/03/613.

<sup>7</sup> Article 29 Data Protection Working Party, Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States, Adopted on 24 October 2002; Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data, Adopted on 13 June 2003.

<sup>8</sup> Undertakings of the United States Bureau of Customs and Border Protection and the United States Transportation Security Administration of 22 May 2003.

<sup>9</sup> COM (2003) 826, p. 7.

<sup>10</sup> Zie over dit onderwerp onder andere A.J. Nieuwenhuis, *Tussen privacy en persoonlijkheidsrecht. Een grondrechtelijk en rechtsvergelijkend onderzoek*, Nijmegen: Ars Aequi Libri 2001, p. 65 e.v.; P.H. Blok, *Het recht op privacy. Een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht*, Amsterdam: Boom 2002, p. 243 e.v. Niet is gezegd dat de Amerikaanse bescherming per definitie altijd slechter hoeft uit te vallen voor burgers dan de Europese.

<sup>11</sup> Richtlijn 95/46/EG van 24 oktober 1995, OJ L 281/31, 23 november 1995.

dat in een besluit worden vastgelegd. Bij dat besluit moet op grond van artikel 25 lid 6 van de richtlijn dan wel in overeenstemming met artikel 31 van de richtlijn advies worden gevraagd aan een speciaal Comité.

De Commissie heeft in het *joint statement* de Europese toezichthouders opgeroepen zich niet te bemoeien met de kwestie van de passagiersgegevens en de luchtvaartmaatschappijen die over zouden gaan tot het verlenen van toegang tot hun databanken niet te bestraffen. Hiermee werd duidelijk dat de Commissie ook zelf van mening was dat de gemaakte afspraken in strijd waren met het Europese privacyrecht.

Basale beginselen van het recht op privacy zoals doelbinding, inzage- en correctierecht waren in de aanvankelijke verklaring volstrekt onvoldoende gewaarborgd. Zo zouden reizigers informatie over de over hun in de databanken berustende gegevens moeten vragen op grond van de *Freedom of Information Act* (de Amerikaanse wet Openbaarheid van Bestuur) en was het vervolgens een discretionaire bevoegdheid van de Amerikaanse autoriteiten om aan zo'n verzoek al dan niet gehoor te geven. Er was geen enkele sprake van onafhankelijk toezicht op de wijze waarop met de gegevens zou worden omgegaan of op de rechtmatigheid van de handelingen die met de PNR gegevens verricht zouden worden.

Volgens de artikel 29 Werkgroep moet uit de Privacyrichtlijn en uit artikel 8 EVRM worden afgeleid dat beperkingen van fundamentele rechten met betrekking tot de verwerking van persoonsgegevens in de EU alleen toegestaan zijn als ze noodzakelijk zijn in een democratische samenleving en indien dat gebeurt ter bescherming van een van de publieke belangen die limitatief zijn opgenomen. Dit sluit haarfijn aan bij de beroemde uitspraak van het EHRM uit 1978 in de zaak *Klass*: “*Nevertheless, the Court stresses that this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate.*”<sup>12</sup>

Alleen al de gigantische omvang van het aantal betrokkenen bij de plannen roept vragen op over de proportionaliteit van een dergelijk systeem. Het gaat om tenminste 10 tot 11 miljoen reizigers per jaar.<sup>13</sup> Volgens de Werkgroep is een minimumeis voor elk besluit dat zou worden genomen in het kader van artikel 25 lid 6 van de Privacyrichtlijn dat de ondergrenzen van zowel artikel 8 EVRM als artikel 13 van de richtlijn gerespecteerd blijven. Dat betekent dat eisen van proportionaliteit en subsidiariteit niet zomaar via een dergelijk besluit buiten werking kunnen worden gesteld.

Voor de proportionaliteit is ook het verschil tussen een *push* en een *pull* systeem relevant. Bij een *pull* systeem – zoals gewenst door de Amerikanen, krijgen de Amerikaanse autoriteiten direct toegang tot de databanken en kunnen dus de door hun gewenste gegevens zo uit de databank ‘trekken.’ Bij een *push* systeem ligt de verantwoordelijkheid voor het verstrekken van de gegevens aan Europese kant en worden de gegevens dus richting VS ‘geduwd.’ Op eerste gezicht is een *push* systeem aanmerkelijk proportioneler dan een *pull* systeem, vooral omdat de controle over welke gegevens worden uitgevoerd, blijft berusten binnen de Europese Unie. Aan de andere kant heeft de Commissie in haar recente voorstellen en uitlatingen hieruit een andere vergaande conclusie getrokken. Om een betrouwbaar *push* systeem te creëren zou volgens de Commissie een centrale opslag van de gegevens nodig

---

<sup>12</sup> EHRM 6 september 1978 (*Klass*), para. 49. Toegegeven zij dat de inbreuk die in *Klass* besproken werd ernstiger is dan bij de overdracht van passagiersgegevens.

<sup>13</sup> 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), p. 3.

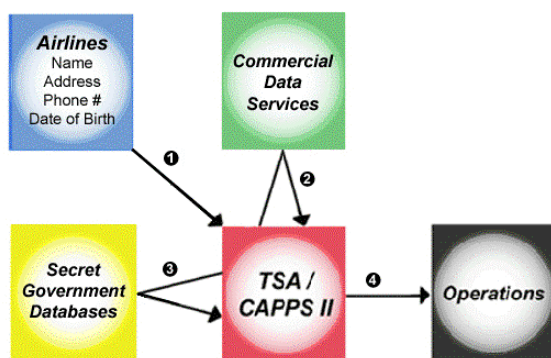
zijn.<sup>14</sup> Dit zou het effect hebben van een parallelle Europese databank en daarmee een dubbele aantasting van de privacy. Een dergelijke databank zou dienstig kunnen zijn in de Europese strijd tegen illegale immigratie – ik zou het bijna *war on immigration* noemen. Er lag al een Spaans voorstel voor een op PNR gegevens gebaseerd systeem, inmiddels wordt gesproken over een mogelijke richtlijn van die strekking.<sup>15</sup> In dat kader is het opvallend dat de Commissie inmiddels officieel streeft naar het creëren van een multilateraal kader voor de verstrekking van passagiersgegevens binnen de Internationale Luchtvaart Organisatie.<sup>16</sup>

#### 4. Doel van de verwerking

Het doel van de verwerking van de gegevens is belangrijk in het kader van de proportionaliteit. Een van de bezwaren tegen de afspraken van februari 2003 was dat de gegevens konden worden gebruikt inzake ‘*serious criminal offences.*’ Inmiddels is dat vervangen door “*terrorism and related crimes and to other serious crimes including organized crime, of a trans-national nature.*’ Hoewel deze doelomschrijving preciezer is dan die in de februari afspraken, meent de artikel 29 Werkgroep dat dit nog steeds te vaag is. Daarbij wordt vooral gewezen op de ruime categorie van andere ernstige misdrijven. Vast staat dat het doel dus veel ruimer blijft dan de enge focus op de strijd tegen het terrorisme.<sup>17</sup> Het is de vraag of deze doelomschrijving precies genoeg is en of hiermee ook voldoende de noodzaak is aangegeven van de doorgifte van dit soort gegevens.

#### 5. CAPPS II

Bij een toets aan het doelbindingsbeginsel komt al gauw CAPPS II om in het vizier. Het *Computer Assisted Passenger Prescreening System* is een computersysteem dat tot doel heeft door koppeling van verschillende gegevensbestanden snel tot een profiel te komen van een potentiële luchtreiziger. Het systeem moet uiteindelijk alle 100 miljoen Amerikaanse vliegpassagiers automatisch controleren. Vervolgens ligt in de rede dat het systeem wordt uitgebreid naar Europese en andere passagiers en wellicht ook naar informatie met betrekking



tot vluchten die geen directe band hebben met de Verenigde Staten. Het systeem werkt ongeveer als volgt. Van iedere passagier worden tenminste vier gegevens doorgegeven: Naam, adres, telefoonnummer en geboortedatum. Vervolgens worden die vier gegevens beoordeeld door en aan de hand van commerciële databanken.<sup>18</sup> Daaruit moet dan volgen of de opgegeven identiteit een bestaande is. Dan volgt een zogenaamde “risk assessment

<sup>14</sup> COM (2003) 826, p. 11.

<sup>15</sup> Initiative of the Kingdom of Spain with a view to adopting a Council Directive on the obligation of carriers to communicate passenger data, (2003/C 82/08)

<sup>16</sup> COM (2003) 826, p. 5.

<sup>17</sup> Opinion 2/2004, p. 6.

<sup>18</sup> Het gaat daarbij om bedrijven die gespecialiseerd zijn in het natrekken vande identiteit van consumenten zoals in de VS Choicepoint.

function.” Het is onbekend welke databanken daarbij betrokken worden, maar informatie van de veiligheidsdiensten ligt voor de hand. Resultaat van deze veiligheidsbeoordeling is een profiel voor iedere passagier waaruit blijkt of hij een hoog, een laag of een onbekend risico vormt. In eerdere versies ging men ervan uit dat zo'n profiel vertaald zou worden in een kleurcode voor iedere reiziger, waarbij groen goed, rood slecht, en geel verdacht zou zijn. Laatste stap van CAPPS II is dat dit veiligheidsoordeel wordt teruggekoppeld aan de luchthavens. Vervolgens komt de passagier met hoog risico niet aan boord, kan de passagier met een laag risico wel gewoon meevliegen, en wordt de passagier met het onbekende risico uitgebreider ondervraagd en/of gefouilleerd. Zie voor de gevolgde stappen bijgaand schema.<sup>19</sup>

Het grootste probleem met CAPPS is dat onduidelijk blijft hoe het systeem in de praktijk werkt. De veiligheidsbeoordeling vindt ergens in een ondoorzichtig gebied plaats en kan op geen enkele manier worden gecontroleerd of gecorrigeerd. Daarnaast kun je je afvragen of het systeem effectief zal zijn in de strijd tegen het terrorisme. Identiteitsdiefstal kan zelfs de amateurterrorist helpen om het systeem eenvoudig te omzeilen, reden voor burgerrechtenorganisatie ACLU (*American Civil Liberties Union*) om CAPPS te vergelijken met de beruchte Franse Maginot linie waar de legers van Hitler eenvoudigweg om heen trokken. Het risico is groot dat de gebruikte informatie op termijn fors zou worden uitgebreid. Andere informatie die 'relevant' is voor de strijd tegen het terrorisme is zo toegevoegd. Verder is niet voorzien in rechtsmiddelen voor de – misschien ten onrechte getroffen – passagiers, niet in correctiemechanismen, niet in onafhankelijk toezicht. Het gevaar is groot dat dit systeem zal leiden tot discriminatie jegens bepaalde groepen reizigers.

De artikel 29 Werkgroep acht ieder gebruik van persoonsgegevens in het voorgestelde CAPPS II systeem of om dat systeem te testen uitgesloten. De Werkgroep adviseert expliciet in het uiteindelijke besluit van de Commissie op te nemen dat van gebruik van Europese PNR gegevens in CAPPS II of voor aan CAPPS gerelateerde testen is uitgesloten. Daarnaast merkt de Werkgroep op dat het niveau waarop de VS verplichtingen aangaat in het kader van de passagiersgegevens onvoldoende is. De beloften van de *United States' Bureau of Customs and Border Protection* (US CBP) zijn wat dat betreft onvoldoende. Inmiddels is bekend geworden dat ook onder de decemberafspraken gegevens van Europese passagiers gebruikt kunnen worden voor het testen van CAPPS II.<sup>20</sup>

## **6. Delen van de passagiersgegevens met andere diensten**

Het delen van de informatie met andere diensten is eveneens een gevoelig onderwerp waarover weinig duidelijkheid bestaat. In eerste instantie zou de informatie worden opgehaald en bewaard door de Amerikaanse douane. Onder omstandigheden zou informatie worden gedeeld met andere diensten zoals de FBI, ter bestrijding van het terrorisme en andere ernstige misdrijven. Er was niet voorzien in een toetsingsmechanisme of een controle op wie onder welke omstandigheden toegang zou krijgen tot de informatie. In het advies uit 2003 vroeg de artikel 29 Werkgroep al eens om een precieze lijst van diensten met wie de passagiersgegevens gedeeld zouden kunnen gaan worden. Een dergelijke lijst is tot op heden nooit beschikbaar gekomen. Wel wordt aangegeven dat de gegevens kunnen worden

---

<sup>19</sup> Het schema is afkomstig uit: “The Five Problems With CAPPS II: Why the Airline Passenger Profiling Proposal Should Be Abandoned”, ACLU, 25 augustus 2003.

<sup>20</sup> Undertakings of the United States Bureau of Customs and Border Protection and the United States Transportation Security Administration of 12 January 2004, onder 8.

doorgegeven indien “required by law” is. Dat kan echter betekenen dat die *laws* nog gemaakt worden of dat de gegevens worden uitgewisseld met andere landen.

## 7. Bewaartemijnen van passagiersgegevens

In de bijlage bij de *joint statement* was opgenomen dat de gegevens niet langer zouden worden bewaard dan noodzakelijk. Noodzakelijk is in deze een tamelijk vage norm. Hoe lang de persoonsgegevens in een derde land worden bewaard is ook relevant voor het besluit tot vaststelling van een adequaat beschermingsniveau, zo blijkt uit artikel 25 lid 2 van de Richtlijn. De termijn van 50 jaar was evident disproportioneel. In de decemberafspraken wordt gesproken van een bewaartermijn van drie en een half jaar. Ook die termijn is in het licht van wat in de Europese Unie gebruikelijk is nog zeer lang te noemen.

In de decemberverklaring is overeengekomen dat de US CBP de gegevens van een bepaalde vlucht voor de vastgestelde doelen gedurende 3,5 jaar mag bewaren.<sup>21</sup> Gegevens die tijdens die periode handmatig zijn bekeken mogen nog eens 8 jaar langer worden bewaard. Dit is ook volgens de artikel 29 Werkgroep een verbetering ten opzichte van de eerder voorgestelde bewaartemijnen. Desondanks betwijfelt de Werkgroep of bewaren binnen de thans voorliggende termijnen voldoet aan de eisen van proportionaliteit en noodzakelijkheid in een democratische samenleving. Bovendien vindt zij de aanvullende bewaartermijn van 8 jaar disproportioneel zolang aan die aanvulling geen concreet onderzoek ten grondslag ligt. Immers, die aanvulling maakt het zeer eenvoudig de termijn te verlengen. De Werkgroep haalt hier met instemming het naar haar zeggen beter toegesneden Australische voorbeeld aan waarbij gegevens alleen bewaard mogen blijven wegens verdenking van een misdrijf of een concreet onderzoek naar een vermeend misdrijf.<sup>22</sup>

## 8. Rechten van betrokkenen

Het Europese privacyrecht bevat een sterke rechtsbeschermingscomponent. Aan de betrokkenen wordt op grond van de richtlijn het recht toegekend op inzage en correctie. Artikel 10 van de richtlijn vereist dat duidelijke en precieze informatie aan de betrokkenen wordt verstrekt over de identiteit van de verantwoordelijke, het doel van de verwerking en andere relevante informatie zoals het recht op toegang en correctie. De artikel 29 Werkgroep adviseert in dat licht om later precies vast te stellen hoe passagiers kunnen worden geïnformeerd over de verwerking van passagiersgegevens. Het toegangsrecht was aanvankelijk zeer beperkt. In die procedure zijn weliswaar verbeteringen aangebracht, toch is het toegangsrecht nog altijd te beperkt. Zo strekt het zich niet uit tot die gegevens die het gevolg zijn van nadere verwerking door de douane of andere diensten.<sup>23</sup> Ook het recht op correctie is op zijn best krakkemikkig. De op dat punt toepasselijke *Privacy Act* uit 1974 geldt alleen voor Amerikaanse staatsburgers of inwoners van de VS. Tenslotte is ook de formulering van een klachtrecht nog onvoldoende vorm gegeven.

---

<sup>21</sup> De vastgestelde doelen: *terrorism and related crimes and to other serious crimes including organized crime, of a trans-national nature*, zie par. 4.

<sup>22</sup> 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), p. 8-9.

<sup>23</sup> 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), p. 9-10.

Tenslotte is er nog een probleem rond het beginsel van datakwaliteit. Bij de recente afgelastingen van vluchten van en naar de VS was steeds sprake van *matching* tussen de lijst met passagiersgegevens en de lijsten met in Amerika gezochte personen. Naderhand bleek dat er sprake was van persoonsverwarring doordat mensen dezelfde naam hadden of dat er simpelweg onjuiste gegevens werden gekoppeld. Aan dit aspect is tot nog toe nauwelijks aandacht besteed.

## 9. Conclusies

De artikel 29 Werkgroep stelt in haar conclusie verbeteringen te zien ten opzichte van eerdere afspraken. Toch gaat een positief advies over de adequaatheid van de bescherming de Werkgroep duidelijk te ver. De Amerikaanse burgerrechten organisatie ACLU schrijft naar aanleiding van de jongste ontwikkelingen dat de doorgifte van passagiersgegevens niet meer iets is tussen de Verenigde Staten en Europa. Nee, door de nieuwe aanpak van de Europese Commissie is het veel meer iets tussen burgers die hechten aan hun privacy aan de ene kant en de federale autoriteiten in de VS en Europa aan de andere kant. Daarbij is het des te wranger dat de gegevens met betrekking tot de Europese passagiers nu gebruikt kunnen gaan worden in het CAPPS II testprogramma.<sup>24</sup>

Vastgesteld moet worden dat de in december 2003 gepresenteerde afspraken nog altijd niet voldoen aan de minimale vereisten die daaraan in redelijkheid op grond van het Europese privacyrecht gesteld moeten worden.

Daarnaast valt in algemene zin op te merken dat de Commissie er geen blijk van heeft gegeven erg te hechten aan de privacyrechten van Europese burgers. Die indruk is nog versterkt nu het *alterior motive* van de strijd tegen illegale immigratie boven tafel is gekomen. Door in het *joint statement* alvast feitelijk in te stemmen met alle Amerikaanse eisen is de onderhandelingsruimte van de Commissie effectief geminimaliseerd.

In de moeizame strijd voor een effectieve bescherming tegen het terrorisme mét het behoud van burgerrechten na 11 september hebben we klaarblijkelijk weinig van 'onze' commissaris Bolkestein te verwachten. De oproep van de Commissie aan de privacytoezichthouders zich nergens mee te bemoeien is potsierlijk en heeft juridisch geen effect. Het zou goed zijn als de toezichthouders - inclusief het College bescherming persoonsgegevens - zich actiever gaan opstellen om de privacy van Europese reizigers te waarborgen.

---

<sup>24</sup> Vgl. "An American Perspective from the American Civil Liberties Union, addendum to "Transferring Privacy", Privacy International, februari 2004.