

P6_TA(2007)0039

PNR-SWIFT

European Parliament resolution on SWIFT, the PNR agreement and the transatlantic dialogue on these issues

The European Parliament,

- having regard to the statements from the Council and the Commission during the debate held in Parliament on 31 January 2007, following the oral question on SWIFT, as well as the negotiations for a new EC-US Passenger Name Record (PNR) agreement,
 - having regard to the letter of reply by the European Central Bank (ECB) of 30 January 2007 to the question of whether the ECB had failed to inform the relevant data protection authorities and the national banks of the US practice of accessing data related to financial transactions generated by SWIFT, as well as to use its power of moral persuasion towards SWIFT in this matter,
 - having regard to the opinion of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data, as foreseen in Article 29 of the Data Protection Directive¹ (the Article 29 Working Party) on the future PNR agreement and to that of the European Data Protection Supervisor (EDPS) as regards the role of the ECB in the SWIFT case,
 - having regard to Rule 103(2) of its Rules of Procedure,
- A. whereas the sharing of data and information is a valuable tool in the international fight against terrorism and related crime,
- B. whereas businesses with operations on both sides of the Atlantic increasingly find themselves caught between the conflicting legal requirements of the US and EC jurisdictions,
- C. whereas the sharing of personal data must take place on a proper legal basis, linked to clear rules and conditions, and must be covered by adequate protection of the privacy and civil liberties of individual citizens,
- D. whereas the fight against terrorism and crime must have proper democratic legitimacy, meaning that data-sharing programmes must at all times be subject to Parliamentary scrutiny and judicial review,

General

1. Stresses that during the last few years several agreements prompted by US requirements and adopted without any involvement of Parliament, notably the PNR agreement, the

¹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

SWIFT memorandum and the existence of the US Automated Targeting System (ATS), have led to a situation of legal uncertainty with regard to the necessary data protection guarantees for data sharing and transfer between the EU and the US for the purposes of ensuring public security and, in particular, preventing and fighting terrorism;

2. Reaffirms that the solutions envisaged so far by the Council and the Commission as well as by private companies do not adequately protect the personal data of EU citizens (as also noted in the letter from Mr Schaar, Chairman of the Article 29 Working Party, regarding the new interim PNR agreement), and that this could constitute a violation of Community as well as national legislation, as in the SWIFT case (see Opinion 10/2006 of the Article 29 Working Party of 22 November 2006 and the EDPS' opinion of 1st February 2007);
3. Notes that in the fight against terrorism the US Congress has for some time asked the US administration to adopt more targeted measures that better ensure privacy and are subject to parliamentary and judicial control (as was demanded when Congress was made aware of the existence of the National Security Agency (NSA) programme of telephone tapping);
4. Confirms its reservations that have recently been shared by Congress as regards the method of profiling and data mining, which consists in accumulating in an indiscriminate manner larger and larger volumes of personal data, as in the case of the ATS used by the US administration;
5. Welcomes the fact that the US administration has recently taken note of these reservations and that it will seek to improve the situation by means of the following steps:
 - (a) the establishment of privacy officers and/or an independent privacy agency within the federal administration, who are to undertake privacy assessments of all initiatives that could potentially impinge on privacy;
 - (b) setting up a mechanism to guarantee US citizens a right of appeal in the event of incorrect use of their data;
6. Believes, however, that these improvements are insufficient as regards data protection for EU citizens and that it would be warmly welcomed if the 1974 Privacy Act could also apply to EU citizens on a reciprocity basis in order for them to have access to their data, with a right of rectification and modification, as well as having access to a legal redress mechanism and to an independent data protection authority;
7. Recalls its belief that such data protection guarantees would facilitate data sharing while ensuring protection of privacy, and that such transfers would in any case need to be based on one or more international agreements similar in structure to that of the EC/US agreement on judicial cooperation in criminal matters and extradition which is currently being examined by Congress;
8. Believes that since such international agreements concern the fundamental rights of EU as well as US citizens, the European Parliament and the national parliaments of the Member States should be fully involved, as should Congress;

9. Insists that in matters of data protection the agreements should strive to achieve a high level of protection as regards risks of abuse and should be supplemented with binding principles at EU level as regards the protection of data for security purposes (third pillar);
10. Stresses the need for the adoption of a framework decision on the protection of personal data in the third pillar; draws attention to the fact that, in the position it adopted unanimously on 27 September 2006¹, it called for such a decision to be comprehensive and ambitious in scope and to provide for data protection rules also covering the exchange of personal data with third countries;
11. Believes that it is necessary to define with the US a common and shared framework to safeguard the necessary guarantees that are needed in the special EU-US partnership in the fight against terrorism, which could also deal with all aspects concerning the free movement of persons between the EU and the US;
12. Expects that this strategy of transatlantic partnership will be discussed at the next EU-US summit on 30 April 2007 and considers that, in this perspective, contacts should be strengthened between Parliament and Congress; requests that:
 - (a) rapporteurs from Parliament be allowed to attend a hearing in Congress on themes that are of mutual interest (the EC-US agreement on judicial cooperation in criminal matters and extradition, ATS, SWIFT);
 - (b) the chairs of the competent Congressional committees be invited with a view to the next transatlantic dialogue (Brussels-Berlin in mid-April 2007) and in any event before the next EU-US spring summit;

As regards the negotiation of the long-term PNR agreement

13. Stresses that, in addition to the points already adopted by Parliament its above-mentioned position of 27 September 2006, a future long-term PNR agreement should be founded on the following principles:
 - (a) evidence-based policy-making: a thorough evaluation must be carried out before a new agreement is concluded; the question of the effectiveness of the current agreement (and the previous one) should be addressed, as should the issue of the costs and competitiveness of European airline companies; the evaluation must address the implementation of the undertakings and the matter of PNR data in ATS;
 - (b) transfers of PNR must be based on a clear purpose limitation principle;
 - (c) justification and proportionality: it would seem that in practice, for law enforcement and security purposes, Advance Passenger Information System (APIS) data are more than sufficient; these data are already collected in Europe in accordance with Council Regulation (EEC) No 2299/89 of 24 July 1989 on a code of conduct for computerized reservation systems², and may therefore be

¹ Texts Adopted, P6_TA (2006)0370.

² OJ L 220, 29.7.1989, p. 1.

exchanged with the US under a comparable regime; behaviour data in the PNR seem to be of limited use, as they cannot be identified if not linked to APIS; the justification for the general transfer of PNR data is therefore not satisfactory;

- (d) a future agreement must be based on an adequacy finding with regard to the protection of personal data; from the EU side, it is clear that rules for the protection of personal data in the third pillar are urgently needed, as well as global standards covering all categories of personal data;
- (e) there must be a regular evaluation of the programme's data protection adequacy and effectiveness, involving Parliament and, if possible, Congress; an annual evaluation must be part of any future agreement; the evaluation report must be made public, and must be submitted to Parliament;
- (f) alternative solutions, such as the Electronic Travel Authorisations within a Visa Waiver Programme, instead of the transfer of PNR by airline companies, must equally comply with EU data protection standards;
- (g) the conditions currently laid down in the US undertakings must become an integral part of the agreement and must be legally binding; a future agreement must have more democratic legitimacy, with the full involvement of the European Parliament and/or ratification by national parliaments;
- (h) in any event, a future agreement must be based on the PUSH system, and the PULL system should no longer be acceptable given that PUSH should already have been introduced under the previous agreement, as soon as it was technically feasible;
- (i) passengers should be informed of the transfer of PNR records and have access to their data, with a right to rectify and modify them, as well as having legal recourse to a legal procedure or to an independent data protection authority;
- (j) expects that the US authorities in the case of an acknowledged terrorist threat are obliged immediately to inform the EU authorities about such suspicion;

As regards the access to SWIFT data

14. Reiterates its concern over the fact that for four years SWIFT, upon receipt of subpoenas, has been transferring to the US administration a subset of data treated in its US system, including data that did not concern US citizens and data not generated on US territory, based on commercial and systemic reasons, to have systematic duplication of the data onto a mirroring information system based in the US, in violation of EU and national data protection legislation;
15. Considers it very worrying that this situation, in breach of the Convention for the Protection of Human Rights and Fundamental Freedoms and the Charter of Fundamental Rights of the European Union, as well as of the Treaties and secondary legislation (Data Protection Directive and Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies

and on the free movement of such data¹), has not been strongly criticised at an earlier stage either by the ECB or by the Group of 10 Central Banks that oversee SWIFT's activities, and that it is only recently that European banks and their customers have been made aware of the situation through press reports;

16. Deeply regrets the fact that, several months after these matters came to light, the Council has not yet taken a stance on this subject affecting so many citizens, consumers and enterprises, and that only seven out of 27 Member States have responded to the questionnaire sent by the Commission to obtain clarification in relation to respect for national and Community data protection laws;
17. Repeats its concerns as regards the current system of supervision of SWIFT whose responsibility belongs to the Group of 10 Central Banks, with oversight by the ECB, but without formal competence; calls on the Council and the ECB to reflect together on the way to improve this system so as to ensure proper functioning of the alert process with full consequences in terms of action to be taken;
18. Endorses the opinion expressed by the EDPS on the role of the ECB and calls on the ECB:
 - as SWIFT overseer, to explore solutions in order to ensure compliance with data protection rules and to ensure that rules on confidentiality do not prevent information from being supplied in good time to the relevant authorities;
 - as user of the SWIFT Net-FIN, to explore solutions to bring its payment operations into compliance with data protection legislation, and to prepare a report on the measures taken no later than April 2007;
 - as policymaker, to ensure, in cooperation with central banks and financial institutions, that European payment systems, including the updated 'TARGET2' system for wholesale payments, fully comply with EC data protection law; calls for the ECB to provide the Parliament with the assessment of such compliance;
19. Reiterates its belief that, under clearly defined conditions, data generated in financial transactions can be used exclusively for judicial investigative purposes in connection with suspicion of terrorism financing and recalls that both the EC and the US in their respective legislation (Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds² and the US Bank Secrecy Act) have implemented Financial Action Task Force (FATF) Recommendation VII;
20. Recalls that, as from 31 December 2006, under FATF Recommendation VII, financial institutions are bound to collect and retain records of certain specified data regarding fund transfers of USD 1 000 or more in Europe (USD 3 000 in the US); any of these records must be submitted or made available to the authorities upon request³;

¹ OJ L 8, 12.1.2001, p. 1.

² OJ L 345, 8.12.2006, p. 1.

³ (See report published on 17 January 2006 by the Financial Crimes Enforcement Network (FinCEN) on the reporting of cross-border wire transfer:
http://www.fincen.gov/news_release_cross_border.html

21. Believes that the EU and the US are fundamental and loyal allies in the fight against terrorism and that this legislative framework should therefore be the basis for the negotiation of a possible international agreement, based on the assumption that SWIFT as a Belgian company is subject to Belgian law and is consequently responsible for the treatment of data in accordance with Article 4(1) of Directive 95/46/EC; points out that the natural consequence would be for SWIFT to be obliged to stop its current practice of mirroring all data concerning EU citizens and enterprises in its US site or to move its alternative database site outside US jurisdiction; urges that this international agreement provide the necessary guarantees against abuse of data for economic and business purposes;
22. Draws attention to the fact that SWIFT provides services outside the EU and the US and therefore considers that any measure adopted should take into account the global aspect of SWIFT's services;
23. Calls on the Commission, which has competence both for data protection and for payment systems legislation, to analyse the potential for economic and business espionage stemming from the current design of payment systems in the broadest sense, thus including, in particular, messaging providers, and to report on ways of tackling the problem;
24. Notes that financial services may be exempted from the Safe Harbour Agreement, as stated by the Article 29 Working Party in its Opinion 10/2006; is concerned over the fact that EU companies and sectors with operations in the US not covered by the Safe Harbour agreement may currently be forced to make personal data available to US authorities, in particular US branches of European banks, insurance companies, social security institutions and providers of telecoms services; calls on the Commission to investigate this as a matter of urgency;
 - o
 - o o
25. Instructs its President to forward this resolution to the Council, the Commission and the governments and parliaments of the Member States, as well as to the US Congress.