EUROPEAN PARLIAMENT 2009 - 2014

Committee on Civil Liberties, Justice and Home Affairs

2009/0190(NLE)

3.2.2010

***

DRAFT RECOMMENDATION

on the proposal for a Council decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program (05305/1/2010REV – C7-0004/2010 – 2009/0190(NLE))

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Jeanine Hennis-Plasschaert

PR_AVC_art90

Symbols for procedures

*	Consultation procedure
***	Consent procedure
***I	Ordinary legislative procedure (first reading)
***II	Ordinary legislative procedure (second reading)
***III	Ordinary legislative procedure (third reading)

(The type of procedure depends on the legal basis proposed in the draft act.)

Amendments to a text

In amendments by Parliament, amended text is highlighted in ***bold italics.*** In the case of amending acts, passages in an existing provision that the draft act has left unchanged, but that Parliament wishes to amend, are highlighted in **bold**. Any deletions that Parliament wishes to make in passages of this kind are indicated thus: [...]. Highlighting in *normal italics* is an indication for the relevant departments showing parts of the legislative text for which a correction is proposed, to assist preparation of the final text (for instance, obvious errors or omissions in a given language version). Suggested corrections of this kind are subject to the agreement of the departments concerned.

CONTENTS

Page

DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION

on the proposal for a Council decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program
(05305/1/2010REV – C7-0004/2010 – 2009/0190(NLE))

(Consent)

The European Parliament,

– having regard to the proposal for a Council decision (COM(2009)0703 and 5305/1/2010REV),

– having regard to the text of the agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program (16110/2009),

– having regard to its resolution of 17 September 2009 on the envisaged international agreement to make available to the United States Treasury Department financial payment messaging data to prevent and combat terrorism and terrorist financing,[1]

– having regard to the request for consent submitted by the Council pursuant to Article 218 (6)(a) in conjunction with Articles 82(1)(d) and 87(2)(a) of the Treaty on the Functioning of the EU (C7-0004/2010),

– having regard to Rules 81 and 90(8) of its Rules of Procedure,

– having regard to the recommendation of the Committee on Civil Liberties, Justice (A7-0000/2010),

1. Withholds its consent to the conclusion of the Agreement;

2. Requests the European Commission to immediately submit recommendations to Council in view of a long term agreement with the United States dealing with the prevention of terrorism financing; reiterates that any new agreement in this area should comply with the new legal framework established by the Treaty of Lisbon and the now binding Charter of Fundamental Rights of the European Union, and renews the requests made in its resolution of 17 September 2009, particularly in paragraphs 7 to 13;

3. Instructs its President to forward its position to the Council, the Commission and the governments and parliaments of the Member States and the government of the United States of America.

[1] *Texts adopted;* P7_TA-PROV(2009)0016.

EXPLANATORY STATEMENT

1. Background

After 11 September 2001 terrorist attacks, the US Treasury developed the 'Terrorist Finance Tracking Program' (TFTP), under which it required, by means of administrative subpoenas, also SWIFT[1] to transfer financial messaging data. Many of these data originate in EU Member States.

Mid 2006 US media disclosed the existence of the TFTP causing significant controversy in the EU. As a consequence, Council and Commission (EC) engaged in discussions with US Treasury early 2007. Following these discussions, US Treasury made a series of unilateral commitments to the EU in June 2007 (the so-called TFTP Representations).

In March 2008 the EC announced that it had designated Judge Jean-Louis Bruguière as the so-called 'eminent' European person in charge of verifying US compliance with the TFTP "Representations". A first report was produced in December 2008. Judge Bruguière has just produced his second and final report. Your rapporteur received a copy (classified EU restricted) on Monday 1 February 2010.

Until recently SWIFT stored messages on two identical ("mirror") servers in order to enhance data resilience, located in Europe and the US. In October 2007, however, SWIFT announced its new messaging architecture according to which, as from 1 January 2010, intra-EU message data (including messages exchanged between countries connected to the European zone) will now exclusively be processed and stored within Europe.

As far as the TFTP is concerned, the net effect is that a significant part of the data which have formed the basis of TFTP subpoenas will no longer be stored in the US, shutting-off US access to much of the SWIFT data it received under the former architecture.

Following a US request the Council decided to negotiate an (interim) international agreement. **On 30 November 2009 Council signed an EU-US interim agreement on the processing and transfer of financial messaging data for the purposes of US TFTP** (FMDA) to be provisionally applied as from 1 February 2010 and expire on 31 October 2010 at the latest.

Under the provisions of the Lisbon Treaty **the European Parliament's consent to the formal conclusion of this interim agreement is required.** The European Parliament gives consent or not (while it will not be possible to renegotiate because the international agreement is already signed).

[1] Society for Worldwide Interbank Financial Telecommunication, established under Belgian law is a secure messaging provider for financial transactions, with around 8500 clients, of which around7800 are financial institutions.

2. The importance of transatlantic cooperation for counter-terrorism purposes

Above all it must be clear that your rapporteur supports an open, democratic, strong, Atlanticist, outward-looking EU that is capable of acting shoulder to shoulder as a true counterpart to the US, not counterweight. Without a doubt, the EU and the US are closer to one another than either is to any other major international actor.

Your rapporteur wishes to recall that Parliament welcomed the "Washington Declaration" (28 October 2009) on enhancing transatlantic cooperation in the area of Justice, Freedom and Security within a context of respect for human rights and civil liberties, and places strong emphasis on the need for transatlantic cooperation. She underlines the necessity for continued and stronger cooperation between US and EU legislators on issues of common concern and is convinced that the framework of transatlantic cooperation for counter-terrorism purposes should be further developed and improved.

Since 11 September 2001 the EU and the USA have negotiated several agreements covering JHA issues. Each agreement was being negotiated individually with many of the same problems, notably in relation to personal data - and legal protection. To overcome these recurrent difficulties Parliament required (and since 2003) the definition of a coherent EU legal framework for data protection as well as the negotiations for a transatlantic binding agreement on this issue.

On 6 November 2006 an EU-US High Level Contact Group was set up in order to discuss "privacy and personal data protection in the context of the exchange of information for law enforcement purposes as part of a wider reflection between the EU and the US on how best to prevent and fight terrorism and serious transnational crime". On 28 May 2008 the Group produced its final report setting out very general principles. The US-EU JHA Ministerial, meeting on 12 December 2008, stated that it had identified a wide range of common principles plus certain outstanding issues relating to privacy and personal data protection, and that their aim is to start negotiation of a binding international agreement as soon as possible.

Your rapporteur is of the opinion that such a binding international agreement, and not just a list of principles if it were to have any added value, is of crucial importance. The agreement is to be applied to individual requests and, where appropriate, automated bulk transfers. Moreover, the December 2008 statement is a political commitment only, and will need to be acted upon. According to the 'Stockholm Programme' adopted on 10 December 2009 negotiations on a binding international agreement should start in the coming months.

As far as the TFTP is concerned, it must be considered as a departure from European law and practice in how law enforcement agencies would acquire individuals' financial records for law enforcement activities, namely individual court-approved warrants or subpoenas to examine specific transactions instead of relying on broad administrative subpoenas for millions of records.

As mentioned earlier the leak of the programme (by US media, mid 2006) led, and understandably so, to a storm of protest in the EU - in particular as regards the TFTP's perceived lack of compatibility with the obligations under the Data Protection Directive (95/46/EC) as well as Member States' laws implementing that Directive.

Furthermore, what might have kicked off as an urgent temporary measure (in reply to 9/11) became *de facto* permanent without specific approval or authorisation by EU authorities or a real transatlantic evaluation of its impact and forward looking transatlantic negotiations covering at the same time security, judicial cooperation and data protection impact. Clearly, such proceedings did not help in building up mutual trust for transatlantic cooperation on counter-terrorism purposes.

With the proposed FMDA, an open-ended arrangement, it cannot be denied that the EU continues to outsource its financial intelligence service to the US. In that respect, your rapporteur agrees with SWIFT that the current debate is not about SWIFT as such but about **how Europe could cooperate with the US for counter-terrorism purposes and how financial messaging data providers are requested to contribute to this fight**, or indeed more generally the law enforcement use of data collected for commercial purposes.

She also believes that European legal requirements for the fair, proportionate and lawful processing of personal information cannot be compromised and that the EU and its Member States, up to now, have been insufficiently strong and clear to set their own objectives.

Finally, it is not difficult to imagine that accepting the proposed FMDA (as it stands) could lead down the slippery slope of accepting other requests for commercial data with (f.e.) Skype, PayPal and other companies in the information-telecommunication field being potentially interesting for law enforcement purposes.

3. Legal considerations FMDA (non-exhaustive)

Having in mind the main elements of the 17 September 2009 European Parliament resolution on the matter, your rapporteur would like to make the following comments on the text of the agreement:

On the principle of proportionality: SWIFT cannot, for technical and governance reasons, search the 'content' of the messages, and thus cannot search data based on criteria like names, addresses and/or invoice numbers of individuals. Therefore if SWIFT were to receive a (Article 4, FMDA) request to produce data related to e.g. an individual, SWIFT will not be able to produce that specific data because of technical reasons. SWIFT could provide instead 'data in bulk'. These messages may eventually contain the specific data (e.g. the name or the address of an individual) that the authority needs for counter terrorism purposes. So, by the very nature of SWIFT it is not possible to refer to so-called limited requests.

The above-mentioned implies that SWIFT has to transfer all, or virtually all, of its data to US Treasury. **That violates the basic principles of data protection law**, i.e. the principles of necessity and proportionality. This cannot be subsequently rectified by mechanisms of oversight and control.

NB: the EU's rules on tracking of terrorist financing activities are based on reporting of suspicious or irregular transactions by individual financial operators.

In fact, it would be better to **allow SWIFT to provide itself with the necessary equipment**

to make targeted searches itself in the data it stores and processes, rather than having all its data transferred in bulk to the US. That would also preserve the parallel with what the EU does in the field of data retention by telecom service providers.

The FMDA does not expressly provide that **transfer requests be limited in time**. Equally, the FMDA does not expressly provide that transfer requests be **subject to judicial authorisation**, nor does it define sufficiently **the conditions for sharing TFTP data with third countries** by the US. **The public control and oversight** of the authorities' access to SWIFT data is not defined even if the FMDA functioning is under the control of the US Congress Oversight Committees.

The FMDA provides for the erasure of all non-extracted data after a specified period. However, the information extracted "shall be subject to the retention period applicable to the particular government (...)". The FMDA provides **no indication of what these retention periods are**.

The rights of **access, rectification, compensation and redress outside the EU** for data subjects are not defined adequately.

The FMDA **does not guarantee European citizens and companies the same rights and guarantees under US law as they would enjoy in the territory of the EU**. Furthermore, the FMDA does not indicate under what circumstances an individual or company outside the territory of the US **is to be informed of the fact that an unfavourable administrative decision** has been taken against him/it.

While Council insists that "it is in the EU's interest to ensure the sustainability of the TFTP notwithstanding SWIFT's new architecture, and thus to ensure legal certainty for the transfer of relevant data to the US Treasury Department, as Member State Services have been the main beneficiaries of TFTP leads", **it is impossible to claim true reciprocity**. True reciprocity would require the US authorities to allow the EU authorities to obtain and use financial payment messaging and related data stored in servers in the US.

Furthermore, in relation to the proposed FMDA, **Council failed to clarify the precise role of the 'public authority' to be designated with the responsibility to receive requests from US Treasury** (taking into account in particular the nature of the powers vested in such an 'authority' and the way in which such powers could be enforced).

The expression "intended not to derogate" (article 13, FMDA) does not correspond to any Treaty provision or term of art in EU law, **and its meaning is frankly obscure**.

4. Inter-institutional relations

By requesting Parliament's consent for the conclusion of the FMDA in conditions in which it was impossible for practical reasons for Parliament to react before the provisional application came into operation, the Council has in effect set Parliament a deadline in breach of the spirit of Article 218(6)(a) TFEU, and undermined in part the legal effect and the practical impact of Parliament's decision in the consent procedure, in particular as regards its provisional application.

Information on the implementation of FMDA is of direct relevance to the negotiation and conclusion of the long-term agreement foreseen in Article 15(4) of the FMDA, and Parliament is therefore entitled to have access to such information.

It should be clear that Parliament is to be "fully and immediately informed at all stages of the procedure". The *ratio legis* of such a duty to inform is not to allow Parliament passively to take note of the actions of the other institutions, but to afford it the opportunity of bringing some influence to bear on the Commission and the Council as regards the content of the agreement, in order to facilitate its consent on the final text. The duty of parliamentary information is, moreover, a reflection of the more general duty on the institutions to "practice mutual sincere cooperation".

Therefore all relevant information and documents must be made available for the deliberations in Parliament, including the opinion of the Council Legal Service and the intelligence underlying the two reports of Judge Jean-Louis Bruguière (in line with the applicable rules on confidentiality).

5. Possible scenario in the aftermath of no consent

If Parliament refuses consent, the FMDA would not enter into force and the provisional application thereof would terminate upon notification by the EU tot the US authorities.

The most obvious route to continue the data exchange is in the framework of the EU-US Agreement on Mutual Legal Assistance, a more general instrument than the FMDA. For those Member States which have a bilateral agreement with the US on mutual legal assistance, the Agreement on Mutual Legal Assistance supplements, rather than replaces, the bilateral agreement.

This Agreement is not limited to terrorist offences; as regards requests for bank information, it is sufficient that the request concern "an identified natural or legal person suspected of or charged with a criminal offence", though the State may restrict the categories of offences in respect of which it will provide assistance. The information may include records of specified bank "accounts or transactions" in the possession of banks or non-bank financial institutions. The information request must, in particular, identify the person, indicate the grounds for suspecting he has committed a crime and show how the information relates to the criminal investigation or proceeding.

The transfer of data to the US will be governed by the domestic law of the Member State(s) concerned.

6. Recommendation FMDA and way forward

Based on the above-mentioned, your rapporteur would recommend Parliament to **withhold** its consent.

However, she does expect Council and Commission to swiftly and ambitiously push Europe's forward looking strategy on counter-terrorism. The security of European citizens cannot be

compromised nor the protections for citizen's data, the certainty of the legal framework within which companies operate and the commercial level playing field**. At all times it must be clear that it is an EU responsibility and that a European solution is to be found**. The Netherlands and Belgium cannot end up being 'the dupe' of all this.

The targeted exchange and use of data for counter-terrorism purposes is and will remain necessary. Identifying security gaps should be at the centre of our attention. The importance of intelligence-gathering is self-evident. And the same goes for the correct integration and understanding of the gathered intelligence (connecting the dots). The public must be able to have trust in both, data and security claims. 'Getting it right' the first time around should be the objective.

The European Parliament requests the European Commission to submit recommendations for the immediate opening of (new) negotiations with the United States on both, **financial messaging data for counter-terrorism investigations** and **privacy/personal data protection in the context of the exchange of information for law enforcement purposes**.

It requests Council to express, in reply, its view with regard to the content of the negotiating directives it will adopt further to such recommendations. Obviously, the concerns of - and recommendations made by the European Parliament as well as the EDPS and Working Group Article 29 are expected be reflected.

It also invites Council and Commission to envisage a solution which could complement (and eventually even substitute) the Mutual Legal Assistance Treaty (MLAT) between the US and the EU, e.g. by spelling out the implications of the exchange of information which is predominantly intelligence-based rather than an example of the information exchanged under the ordinary MLA cooperation. By exploring such a strategy attention should be given to a 'European' solution for the supervision of data exchange, i.e. to determine an EU independent (judicial) authority which would be empowered to verify the TFTP operations (and even to block the TFTP system). The prerequisite for this European solution is a binding international agreement on privacy and personal data protection in the context of the exchange of information for law enforcement purposes.

It might be worth inviting The Financial Action Task Force (FATF) to submit recommendations as well.