Library Briefing
Library of the European Parliament
28/04/2011

EU response to the US Terrorist Finance Tracking Programme

For the United States, the Terrorist Finance Tracking Programme is an essential element of its counter-terrorism policy. It relies on 'data sets' obtained under subpoena from the SWIFT worldwide messaging system, allowing it to track financial transactions from across the world, and initially including Europe.

In 2009, SWIFT moved its European transaction data to Europe, forcing the US to negotiate with European governments for continued access to the data. The move also coincided with the increase in the power of the European Parliament under the Lisbon Treaty. An interim agreement, supported by the Council and Commission, was rejected by the EP on the grounds that it failed to correctly balance security and civil liberties.

The EU-US Financial Messaging Data Agreement was finally signed in June 2010, following further negotiations with the US, and including additional data protection provisions in comparison to the rejected text.

Two reports on the first six months of the new agreement have, however, placed doubts on the new data protection safeguards. In particular a report on Europol's role has raised serious concerns from a number of MEPs. Europol has, in turn, strongly defended its own performance.

In this briefing:

Background

The Terrorist Finance Tracking Programme (TFTP) was one of a number of instruments introduced by the US government in the aftermath of the September 2001 attacks. It is designed to help monitor the financial activities of suspected international terrorists or networks.

The US Treasury Department issues subpoenas to the Society for Worldwide Interbank Financial Communications (SWIFT) for "limited subsets of data". SWIFT handles international transactions between financial institutions in over 200 countries, including in Europe. Until 2009, it kept all its data on US soil and therefore within US legal jurisdiction.

The programme had been kept secret from European governments, until it was exposed in 2006 by several media sources. In addition to the political fall-out from the revelations that European data had been accessed and used, Belgium, which hosts SWIFT's main European operations, concluded that the actions breached both Belgian and EU data protection rules. A transatlantic dialogue was established to set up certain safeguards following concerns expressed by, inter alia, the European Parliament (EP).

The US has argued that, whilst providing invaluable counter-terrorism information, the TFTP conforms to both federal and international law.[1] This view was supported by

Author: Nic Copeland
Contact: nicholas.copeland@europarl.europa.eu ✆ 32695

the Commission in the first of two reports by its appointed expert.

In 2009, SWIFT initiated its "dual-zone" programme, moving European transaction data off US territory, and therefore outside the jurisdiction of a US subpoena, and into the EU. This was primarily done to alleviate client privacy concerns but it had the effect of forcing the US to negotiate with European countries. The dual-zone was to take full effect from 1 January 2010.

In order to continue accessing SWIFT data from that date, the US required an agreement with the EU. This centred on the need to find an acceptable balance between two competing objectives: providing sufficient international security and counter-intelligence capability on one side and ensuring adequate data protection and privacy safeguards.

Both the Commission and the MS, who emphasised the contribution to transatlantic cooperation and the potential value to EU counter-terrorism investigations, appeared satisfied by US assurances on the latter element. The European Parliament on the other hand remained less convinced.

Towards an EU-US agreement

In September 2009, the EP adopted a resolution setting out a minimum set of requirements for any agreement. It insisted that data should only be used for the purpose of fighting terrorism and that it must satisfy EU rules on data protection, procedural rights, proportionality and reciprocity. The EP expressed particular objection to the transferring of data in bulk rather than being restricted to specific subjects.

With the EP's powers scheduled to increase significantly from 1 December 2009 with the coming into force of the Lisbon Treaty, the Council proposed an 'interim' agreement that would allow the US to continue to access SWIFT data whilst a new longer term agreement was negotiated. Although many of the EP's substantive concerns remained, the Council concluded the interim agreement on 30 November 2009, the day before Lisbon entered into force.

The agreement was only sent to the EP for its consent a week before it was due to enter into force on 1 February. A rapidly prepared report for the LIBE committee recommended the rejection of the text, citing many of the issues raised in the EP's earlier resolution. Despite a personal request from US Secretary of State Hillary Clinton to EP President Buzek, dire predictions for the future of counter-terrorism from some US officials[2] and a warning from the Commission that it could be replaced by bilateral agreements with weaker safeguards, the EP withheld its consent to the agreement in February 2010.

Opinion is divided on the strongest reason for the rejection. Some suggest that it was symbolic - the flexing of the EP's post-Lisbon muscles - evidenced by its flat rejection of the agreement, in preference to delaying the vote whilst it sought further information. Others considered it to be a principled stance reflecting a concern for necessity and proportionality in the use of personal data for cross-border law-enforcement purposes.

According to Buzek, "the majority view is that the correct balance between security, on the one hand, and the protection of civil liberties and fundamental rights, on the other, has not been achieved".

As part of its resolution rejecting the text, the EP requested the Commission to submit recommendations to the Council for a long-term agreement with the US.

The "SWIFT II" agreement

Following Council authorisation, the Commission opened negotiations with the US on the Financial Messaging Data Agreement (FMDA) in May 2010.

In a resolution adopted some days earlier, the EP indicated several areas where it believed improvements should take place. It called for a two-track approach with stricter safeguards being implemented than in the existing

agreement, whilst in the longer term it called for a "European solution" to the extraction on its soil of requested data.

In addition, it proposed a judicial public authority be designated by the EU to receive requests from the US Treasury, that it should provide for reviews at set times and that the specific rights of both US and EU citizens should be established on a non-discriminatory basis. The new agreement was agreed by the Council at the end of June 2010 and approved by the EP at the beginning of July. It is valid for five years and, unless either party objects, will be renewed annually thereafter.

The agreement contains a number of key provisions, representing advances – from an EP perspective – on both the previous arrangements and the rejected interim agreement. The FMDA:

- assigns a group of independent experts, including a European official appointed by the Commission, to supervise the use of data by US officials on US territory;
- entrusts Europol with verifying whether US requests for information meet specified requirements;[3]
- requires US law to provide a right of redress to individual citizens regardless of nationality;
- requires the US Treasury to delete any unrequested financial data that may be transmitted; and
- proposes the development of an EU data extraction system equivalent to TFTP. (The Council Decision concluding the Agreement required the Commission to submit a legislative proposal by 1 August 2011.)

Whilst the EP considered the new agreement an "improvement", it nevertheless highlighted that some modalities required clarification. In particular it pointed out that Europol was not the "judicial authority" it had envisaged and expressed the need for independent oversight.

The agreement in action

Article 13 of the FMDA required a joint review at the latest six months after it entered into force.[4] The review would assess the safeguards, controls and reciprocity provisions. A Commission report on the joint review was published in March.

It argued that it was too early to assess the FMDA's effectiveness, and the report therefore focused on its implementation and whether its mechanisms were now properly in place.

The report concluded that all the relevant parts of the FMDA had been implemented and that the measures taken by the US authorities to ensure this are convincing, in some cases going beyond what is required. It also found indications of added value to both US and EU authorities in combating terrorism and its financing.

Despite the Commission's generally positive tone, concerns have been expressed. The EU review team recognised the "justified concerns" of the US which feared that disclosure of certain information could jeopardise the effectiveness of the programme. However, the report pointed to the clear interest in the provision of statistical information in order to understand the scope of the programme and the implications for civil liberties.[5] The review team called for more statistics to be provided for future reviews, as well as for ways to be found to provide more regular information. It also stated that, where possible, information should be made public.

The role of Europol

This concern has focused attention on the role of Europol which, under Article 4, is responsible for verifying US data requests. Europol is required to substantiate the necessity of the data and, once established, to ensure that each request is "tailored as narrowly as possible".

The EU review team was also made aware of a separate report[6] on Europol's role in implementing the TFTP agreement, by the Joint Supervisory Board (JSB). The JSB is an

independent entity set up to ensure individual data protection rights are respected in Europol's activities.[7] It found that certain data protection requirements were not being met.

The report cites four data transfer requests made to Europol at the time of inspection, all of which were granted. It contends that their "abstract" nature prevented proper verification by Europol. It also highlighted the provision of oral rather than written information by the US Treasury as making effective data protection supervision impossible.

Although using more nuanced language, the Commission report also considered there to be scope for more detailed and targeted justifications in writing, even where information is classified.

A number of MEPs have expressed serious concerns about the FMDA in the light of the JSB report. EP rapporteur Alexander Alvaro has suggested the report "raises serious concerns" for data protection as Europol appears to be merely "rubberstamping" US requests for the transfer of bulk data without scrutiny. Other MEPs have argued that it reinforces the need for an "EU TFTP".

Europol's Director has, however, strongly defended its actions. In an Information Note prepared for the EP, he argues that the task of verifying a request is done on the basis of an "operational judgment" of its validity. This would take into account both knowledge and experience in combating terrorism and in observing the principle of proportionality in processing personal data. In six of the eight requests Europol had received to 1 April, it had failed to meet the 48-hour time period allocated for verification, on one occasion taking 16 days. This, he argued, reflected "the care and diligence Europol has applied in discharging its duties under Article 4".

Main references

J Monar, The Rejection of the EU-US SWIFT Interim Agreement by the European Parliament: A Historic Vote and its Implications, *European Foreign Affairs Review* 15; 143-151, 2010

E Dretzka and S Mildner, Anything but SWIFT: Why Data Sharing is still a Problem for the EU, *American Institute for Contemporary German Studies*, May 2010

Disclaimer and Copyright

Endnotes

[1] The US argues that the TFTP conforms to both the International Emergency Economic Powers Act (IEEPA) and the United Nations Participation Act (UNPA).

[2] Clinton calls Parliament chief over bank data deal, *EU Observer*, 4 February 2010.

[3] The FMDA requires that data be 'pushed' not 'pulled' i.e. sent by Europe, not gathered by the US.

[4] Article 13 does not set out time limits for future reviews but states that they would be carried out regularly. The Commission has indicated that another review would take place during 2012.

[5] In particular it cited the overall volume of financial payment messages provided to US authorities and the number of searches performed on this data as two areas where tension exists.

[6] The findings of the inspection and the evaluation are contained in the annex to the report. This annex is classified "EU Secret" and is not publicly available.

[7] The JSB provides an external review of Europol's storage, processing and use of personal data. That role is performed internally by the Data Protection Officer.

Author: Nic Copeland
Contact: nicholas.copeland@europarl.europa.eu ✆ 32695