

## RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

### SWIFT

Robert, Romain; Gayrel, Claire

*Published in:*  
E-finance & Payments Law & Policy

*Publication date:*  
2011

*Document Version*  
Publisher's PDF, also known as Version of record

[Link to publication](#)

*Citation for pulished version (HARVARD):*  
Robert, R & Gayrel, C 2011, 'SWIFT: first joint review, first observations', *E-finance & Payments Law & Policy*, vol. 5, no. 7, pp. 1-4.

#### General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

#### Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

## **Publication of the first joint review of the Agreement between the EU and the US on the processing and transfer of Financial Messaging data from the EU to the US for the purposes of the TFTP**

Claire Gayrel, Researcher at the CRIDS, University of Namur, [claire.gayrel@fundp.ac.be](mailto:claire.gayrel@fundp.ac.be)  
Romain Robert, Attorney and researcher at the CRIDS, [romain.robert@dewolf-law.be](mailto:romain.robert@dewolf-law.be)

*In accordance with its Article 13, the first review of the Agreement between the EU and the US on the processing and transfer of Financial Messaging data from the EU to the US for the purposes of the Terrorist Finance Tracking Program (TFTP) took place six months after the entry into force of the Agreement on the 1<sup>st</sup> August 2010.*

### **The TFTP story**

The TFTP Agreement was concluded after a long story which started in 2006 with the New York Times revealing that SWIFT (Society for Worldwide International Financial Telecommunication), an organization established in Belgium, was transferring financial messaging data to the US Treasury Department despite of the European restrictions regarding the transfer of personal data from the EU. These transfers were carried out by virtue of administrative subpoenas issued by the US Treasury's Office of Foreign Asset ("OFAC") operating on the basis of powers under the TFTP and requiring SWIFT in the US to transfer personal data held on its US server to OFAC for counter terrorism purposes.

The TFTP was criticised within the EU, notably by several data protection authorities and the European Parliament, considering that the transfers of data under the TFTP breached the provisions of Directive 95/45/CE. In spite of these European protests and having seen to the sensitivity of the context of the 9/11 terrorist attacks and the transatlantic alliance in the war against terrorism, the EU and the US agreed on subsequent interim agreements providing for a temporary framework for the transfers of financial messaging data from SWIFT to the US Treasury before the conclusion of a long-term agreement in this matter.

In order to ensure the continuity of the TFTP under the conditions of a new messaging architecture of SWIFT, a new agreement was considered necessary. The European Parliament rejected the first proposal of the new EU-US Agreement concerning the transfer of financial messaging data for the purposes of TFTP, arguing that the proposal did not afford substantive personal data protection. An improved version of the Agreement was negotiated and approved on 13 July 2010 and entered into force on 1<sup>st</sup> August 2010.

### **The different reports**

Besides the EU Joint Review Team Report of 30 March 2001, published in accordance with Article 13 of the Agreement, two other reports were made available. The first one was published by Europol Joint Supervisory Body ("JSB") on 1<sup>st</sup> March 2011. The JSB has the task of reviewing Europol's activities in order to ensure that the rights of the individuals are not violated by the storage, processing and use of data held by Europol. The JSB mandated an inspection group to check Europol's implementation of the TFTP Agreement. This inspection took place in November 2010, that is to say only a few months after the entry into force of the Agreement.

A later report was published by Europol as an Information Note to the European Parliament on 8<sup>th</sup> April 2011 about its activities in relation to the TFTP Agreement. This Report was therefore published after the EU review team report. According to Article 13 of the Agreement, five main parameters were to be taken into account for the review: (i) the number of financial payment messages accessed, (ii) the number of occasions on which leads have been shared with Member States, third countries, and Europol and Eurojust, (iii) the implementation and effectiveness of the Agreement, including the suitability of the mechanism for the transfer of information, (iv) cases in which information has been used for the prevention, investigation, detection, or prosecution of terrorism or its financing, and (v) compliance with the data protection obligations specified in the Agreement. The reading of the three reports surely raises some questions regarding these elements, since one can note that the effectiveness of the TFTP is barely addressed and the data requests appear to be so difficult to assess that a conclusion on the respect of the conditions laid down in the Agreement seems almost impossible to reach.

### **Confidentiality issues**

Europol does not have access to the financial data sent to the US Treasury by SWIFT, and is therefore not aware of the overall volume of financial data transferred. The same is true for the Joint Review Team that has not been allowed to access this information, since US authorities stated that making an overall figure public would be “*detrimental to the effectiveness of the program*”.

However, we share the opinion of the EU joint review team that considers that the overall volume of data transferred is a necessary element to assess the effectiveness TFTP Agreement, its implications on civil liberties and *in fine* its proportionality. Since no independent supervision is provided to control the volume of data transferred under the TFTP Agreement, it is made difficult to control the proportionality requirement (including the necessity test) provided by article 8 of the European Convention of Human Rights.

As a consequence, the EU join team recommended that more statistical information on the overall volumes of data provided under the Agreement and the data accessed be provided in the course of future reviews. One can understand the necessity to protect the confidentiality of some information to protect the effectiveness of the program, but we are of the opinion that a valuable and reliable review cannot be carried out without some basic data in order to assess the TFTP.

### **Assessment of the requests**

US requests to obtain the transfers of financial messaging data from the designated providers (at that time only SWIFT has been recognized) are addressed to Europol, in charge of the verification that the requests comply with the Agreement. The verification will in particular concern the conditions laid down in its Article 4, providing among other requirements that these have to be “*tailored as narrowly as possible in order to minimise the amount of data requested.*” In this respect, one can read in the Europol Joint Supervisory Body's report that the requests for SWIFT data were “*almost identical in nature and [requesting] – in abstract terms – broad types of data*”, adding that “*due to their abstract nature, proper verification of whether the request are in line with the conditions of article 4 (2) of the TFTP Agreement – on the basis of the available documentation – [was] impossible.*”

One should notice that, if Europol happened to request further information regarding several US requests, it nevertheless approved all of them. One could conclude that there could be serious doubts as to whether Europol is properly empowered, under the current conditions of the Agreement, to control the compliance of the US requests with the data protection requirements.

In practice, justifications has also been provided by the US Treasury to certain Europol staff through confidential oral briefings, during which Europol staff was not able to make written notes. Since the information provided during these oral briefings were of importance in Europol's decisions, the Europol JSB underlines the necessity that justifications be exclusively provided in writing in order for supervisory bodies to properly audit the verification process. The EU joint review team also considered that *"there seems to be scope to provide more detailed and targeted justifications for the requests to the designated provider in writing in order to enable Europol to perform its functions even more effectively."* This would also allow for more effective independent review of the decision adopted by Europol by giving more transparency.

### **Safeguards and oversights on the searches**

Other important guarantee concerning the processing of financial messaging data transferred by SWIFT is -besides the proportionality principle- the purpose limitation principle, providing that processing shall only be carried out by the US Treasury Department *"for the exclusive purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing"* (Article 6 of the Agreement).

Concerning the respect these principles, several guarantees has been put in place. First, searches are designed technically to allow only narrowly tailored searches justified by a clear nexus to terrorism. Second, independent overseers, among whom are an EU appointed overseer and one designated by SWIFT, verify (in real time or retro-actively) all the searches made in the database. Third, when the search led to results that confirm their interests to a terrorist investigation, dissemination of the TFTP derived information is subject to a previous review by the independent overseer.

The join team concluded that the system of independent oversight over the implementation of these safeguards incorporated in the Agreement was very valuable. The overseers have actually used their powers to investigate on the searches and to block any dissemination that was potentially in breach of Article 5 of the TFTP Agreement.

### **The effectiveness of the TFTP**

While the first report of the joint review team makes clear that it would be premature to address the issue of the effectiveness of the program, it nevertheless provides interesting elements to comment here. The EU joint review team reasserts the *"operational value"* for the FBI, but also insists on the *"unique value"* of the program, which is described as *"the most important Agreement the US has in place in this area"*.

In addition, the report notices that *"in many cases the value of the TFTP is not recognised as such even by the recipients of TFTP derived information, either in the US or abroad."* Further, the review team reports the *"general difficulty of assigning a concrete value to*

*information derived from the TFTP since it is normally only one piece of the puzzle of an investigation.*” However, the ability to assess whether this one piece of the puzzle was decisive or not is of great importance at the time of assessing the effectiveness of bulk personal data transfers to the US.

According to the EU joint review team report, another indication of the value of the program could be found in the increasing number of requests from the FBI that would demonstrate that the information derived from the TFTP “*was perceived as offering added value to ongoing terrorism investigations*”.

The caution with which the drafters of the report are evoking the effectiveness of the program can appear surprising for the outsider commentator. While previous reports (notably those delivered by the French anti-terrorist Judge Jean Louis Bruguière) strongly insisted on the effectiveness of the program and therefore its value for the European Union, one could remain circumspect about the conclusions of the review team, which seems satisfied with “*indirect indications*” of the added value of the TFTP derived information to counter-terrorism investigations”. If *effectiveness* does not substitute *necessity*, in the sense of article 8 of the ECHR, it however constitutes one of the underlying conditions of the proportionality principle for the assessment of any invasion into citizens' privacy.

Having considered the above, no wonder that the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament, raised serious concerns. Member of the Parliament questioned Europol's credibility, and considered this a bad precedent for further agreements in this area. We will soon discover how the Parliament will react when it will be confronted to the proposal of the Commission of a legal and technical framework for the extraction of data on EU territory. Indeed, according to the Decision 2010/421/UE of the Council, the Commission is invited to submit such a framework to the European Parliament and the Council, no later than one year from the date of entry into force of the Agreement.