



Summary of the opinion on the transfer of personal data by

SCRL SWIFT following the UST (OFAC) subpoenas

Upon request of the "Collège du renseignement et de la sécurité" (College for Intelligence and Security), the Privacy Commission has issued the following opinion on 27th September 2006. This is amongst others based on the Belgian Privacy Law, public information about SWIFT, documentation requested from SWIFT and elements obtained following repeated requests.

The Privacy Commission consulted with the EU group for the protection of individuals with regard to the processing of personal data, which was set up on the basis of Article 29 of Directive 95/46/EC (hereafter referred to as "Working Party 29" or "WP 29"). WP 29 has already declared to be setting a priority on defending European data protection rights and pointed out the lack of transparency in the negotiations with the US Department of the Treasury (UST), and more precisely with the Office of Foreign Assets Control (OFAC).

A. INTRODUCTION

The Commission's investigation focused on the processing of personal data via the SWIFTNet FIN service and on SWIFT's role in the transfer of personal data to the UST..This investigation does not focus on processing in the framework of a company's normal administration (for which SWIFT made the required declarations to the Commission).

B. FACTS

SWIFT provides her clients (approx. 7,800 financial institutions) with automated services consisting essentially in the transmission of financial messages between financial institutions worldwide. SWIFT itself is not a financial institution. SWIFT has two operations centres, one in Europe and one in the US, which store transaction messages processed via SWIFT for a period of 124 days. The SWIFTNet FIN service makes it possible to send messages regarding financial transactions between financial institutions.

After the attacks of September 2001, the UST served several subpoenas on SWIFT in the US. The scope of these is very wide from a material, territorial and time scale point of view. It concerns non-individualised and mass requests for information by the UST about (a.o.) European financial transactions. From the Commission's verifications it appears that a distinction between two levels was made in the UST's extraction process: retention in a black box of the data transferred following the subpoenas on the one hand, and effective consultation of the messages in the black box by the UST after search tasks were carried out with a view to fight terrorism.

After verification of the subpoenas, SWIFT made decisions on how to comply with them. SWIFT also informed its control committee, among which the National Bank of Belgium (NBB), who considered however not to be competent to rule on the SWIFT compliance with the consecutive subpoenas, since this falls outside its control competence.

C. APPLICABILITY OF THE BELGIAN PRIVACY LAW

The Commission considers that the Belgian privacy law is applicable to the exchange of data via the SWIFTNet FIN service. This regards transactions which may involve private Belgian individuals through the international payment instructions they entrust to their bank. SWIFT also has its headquarters in Belgium (La Hulpe).

D. OPINION ON WHETHER SWIFT AND THE FINANCIAL INSTITUTIONS ARE “DATA CONTROLLERS”

The question is whether SWIFT is merely a processor, for example like a postal service, or a controller in the processing of personal data via its SWIFTNet FIN service.

The Commission considers that

- SWIFT is a controller with regard to the processings of personal data via the SWIFTNet FIN service; the Commission considers a.o. that SWIFT is an international cooperative network with strong central management offering services to several thousands of financial institutions. This situation is not comparable to a simple service concept in which one single professional provider processes personal data on behalf of a single professional or non-professional third party. SWIFT makes decisions which go beyond the normal and legally defined “margin for manoeuvre” within which a normal processor can make decisions; SWIFT is also clearly a controller because it made all the crucial decisions regarding the data transfer to the UST and this without informing its 7,800 clients.
- The financial institutions are controllers because in the inter-bank traffic they co-defined the objective and the means to carry out the payment instructions.

E. INVESTIGATION INTO POSSIBLE VIOLATIONS OF THE BELGIAN PRIVACY LAW

The question whether the (Belgian) financial institutions infringed the Belgian privacy law lies outside the scope of this opinion.

There are fundamental differences between the EU and the US with regard to legislation and principles which regulate the processing of (personal) data; the level of protection in particular is higher in Europe.

In this regard the Commission considers that

- In relation to the normal processing of personal data in the framework of the SWIFTNet FIN service:
SWIFT should have complied with its obligations under the Belgian privacy law, amongst which the notification of the processing, the information, and the obligation to comply with the rules concerning personal data transfer to countries outside the EU .
- With regard to the transfer of personal data to the UST:
SWIFT finds itself in a conflict situation between American and European law. Although SWIFT did make considerable efforts to provide certain guarantees through its negotiations with the UST, SWIFT made some substantial errors of judgement in complying with the American subpoenas. From the beginning, SWIFT should have been aware that the fundamental principles of European law were to be observed, apart from the enforcement of the American law, such as the principle of proportionality, the limited retention period, the principle of transparency, the requirement for independent control and an adequate protection level. The competent authorities (the Commission, its peers and the European Commission) should have been informed from the beginning, which would have made it possible to work out a solution at the European level for the transfer of personal data to the

UST. The Belgian government could also have been approached in order to request an initiative at European level.

The Commission is available to offer further advice on this matter. It invites the government to discuss this case at European level. The European Commission can for example, in light of the European privacy Directive 95/46/EG, work out an acceptable solution providing a suitable balance between the fight against terrorism on the one hand and the protection of privacy on the other hand.