



Journal of Internet Banking and Commerce

An open access Internet journal (<http://www.arraydev.com/commerce/jibc/>)

Journal of Internet Banking and Commerce, April 2007, vol. 12, no.1
(<http://www.arraydev.com/commerce/jibc/>)

SWIFT Privacy: Data Processor Becomes Data Controller

Author's Name: **Edwin Jacobs**

Author's Title/Affiliation: **Lawyer at Monard-D'Hulst (Brussels) and affiliated researcher at the Interdisciplinary Centre for Law and Information Technology (ICRI), IBBT, University of Leuven, Belgium**

Postal Address: **Tervurenlaan 270, 1150 Brussels, Belgium**

Author's Personal/Organizational Website: www.monard-dhulst.be

Email: **[Edwin.Jacobs \(at\) monard-dhulst.be](mailto:Edwin.Jacobs@monard-dhulst.be)**

Brief Biographic Description: Edwin Jacobs is the former head of the legal department of ISABEL, a leading service provider in e-banking, e-business en e-government, a certification service provider involved in e-Banking, e-Business (i.a. electronic invoicing) and e-Government. Currently he is a lawyer heading the TMT-IP (Technology, Media, Telecom - Intellectual Property) department of the independent law firm Monard-D'Hulst in Brussels. His areas of interest are legal management of ICT-projects, privacy, e-business, electronic contracting, outsourcing and service level agreements, intellectual property, security, electronic invoicing, copyright, trade marks, etc. He is also an affiliated researcher at the Interdisciplinary Centre for Law and Information Technology (ICRI) at the University of Leuven.

Abstract

Last month, SWIFT emphasised the urgent need for a solution to compliance with US Treasury subpoenas that provides legal certainty for the financial industry as well as for SWIFT. SWIFT will continue its activities to adhere to the Safe Harbor framework of the European data privacy legislation. Safe Harbor is a framework negotiated by the EU and US in 2000 to provide a way for companies in Europe, with operations in the US, to conform to EU data privacy regulations. This seems to conclude a complex privacy case, widely covered by the US and European media. A fundamental question in this case was who is a data controller and who is a mere data processor. Both the Belgian and the European privacy authorities

considered SWIFT, jointly with the banks, as a data controller whereas SWIFT had considered itself as a mere data processor that processed financial data for banks. The difference between controller and processor has far reaching consequences.

Keywords: privacy; data protection; SWIFT; data processor; data controller; electronic banking

© Edwin Jacobs, 2007

Introduction

In an effort to combat terrorism, and more particularly its funding, the US authorities set up a secret programme in 2001 to trace financial transactions of people suspected of having terrorist ties. This programme involved the cooperation of SWIFT, a Belgian-based company with an operation centre in the US that electronically transfers financial data. SWIFT has data centers in both countries. SWIFT provided the US Treasury Department with access to financial data coming from financial institutions worldwide.

The US Treasury Department addressed several administrative subpoenas to SWIFT's operation centre order to gain access to SWIFT's database. SWIFT didn't challenge the subpoenas in court but instead negotiated with the US Treasury Department about the scope and the extent of the subpoenas, in order to obtain certain guaranteed levels of privacy and confidentiality. The result was that SWIFT allowed indirect access to its database through a "black box", a system with financial data provided by SWIFT, but operated by and located at the US Treasury Department. The scope of the searches in the black box was limited to terrorism, but the definition of terrorism was very large. It required insight in the search criteria and audits by an independent auditor and specific SWIFT employees.

SWIFT didn't notify the existence nor conditions of this collaboration with the US to its members (financial institutions) or data subjects, nor to the privacy authorities. It is estimated that several billion financial messages were searched by the US Treasury Department every year since 2001. Exact figures are not available.

Reactions of governments, central banks, European Parliament

The existence of the collaboration between SWIFT and the US Treasury Department was revealed in the American press in June 2006. European governments and the Belgian administration denied all knowledge. Belgian and European central banks (1) rejected any responsibility to act, based on their confidentiality duty and the scope of their oversight mission (2). The European Parliament organised a public hearing and issued a resolution that expressed serious concerns as to the purpose of the data transfers (3).

Reports of the Belgian and European Privacy Authorities

In September 2006, the Belgian Privacy Commission issued a public advice about the transfer of financial transaction data by SWIFT to the US Treasury Department (4). The so called "Working Party 29", the EU's advisory body on data protection and privacy, published its report on 23 November 2006 (5).

While the Belgian Privacy Commission considers SWIFT to be the data controller (instead of a mere processor) determining the purposes and means of the data processing as part of its services, it still holds a moderate view, recognising that SWIFT finds itself in a conflict situation between American (subpoenas) and European law (privacy). The Privacy Commission considered that SWIFT, being a data controller instead of a data processor, was in breach of Belgian data protection legislation, in particular the rules on proportionality, transparency towards data subjects, notification of the processing to the Privacy Commission and transfer of the data to non-EU countries (in this case the USA) which do not offer an adequate level of protection of personal data (6).

The Working Party 29 however goes even further and firmly states that Belgian and European privacy legislation had been seriously infringed because "the hidden, systematic, massive and long-term transfer of personal data by SWIFT to the UST in a confidential, non-transparent and systematic manner for years constitutes a violation of the fundamental European principles as regards data protection". The report suggests that the mere fact of having an operating center in the USA constitutes a breach of European data protection principles because, a company having such an operating center, places itself in the foreseeable situation of being impacted by US subpoenas.

Impact of the reports. Data processor versus data controller

Both reports refer to arguments already previously used in previous data protection infringement case, such as the transfer of airline passenger data. Very remarkable in this particular case is that the Belgian and the EU reports consider both SWIFT and its members (the financial institutions) to be data *controllers* in the meaning of EU data protection legislation, whereas SWIFT had very sound arguments that it was a data processor and not a data controller. As a result, all parties are jointly, although not equally, held responsible for the data protection infringements. This is remarkable because most banks had no knowledge of the US subpoenas and data transfers to the US authorities.

Although no penalties have been imposed, this has far reaching consequences, because of the legal obligations of a data controller as opposed to a mere data processor. In this case SWIFT was held to be a data controller determining the purposes and means of the data processing as part of its highly specialised services.

Safe Harbor Arrangement

Last month, SWIFT announced (7) that it will continue its activities to adhere to the Safe

Harbor framework of the European data privacy legislation. Safe Harbor (8) is a framework negotiated by the EU and US in 2000 to provide a way for companies in Europe, with operations in the US, to conform to EU data privacy regulations. The question is whether the European data protection authorities will be satisfied with this solution (9).

Conclusion

While, on one hand, it should be welcomed that an important matter such as data protection receives a lot of attention, I hope that the data protection authorities will apply the legislation in a correct but pragmatic way, taking into account the fact that the difference between a data controller and a data processor, at least when applying the classical criteria set forth by the privacy legislation, is not always that obvious (e.g. in an international context with highly specialized outsourcers) and can sometimes be subject to debate.

References

- (1) Trichet, Jean-Claude, Statement by the President of the ECB at the public hearing at the European Parliament on the interception of bank transfer data from the SWIFT system by the US secret services, 4 October 2006, <http://www.ecb.int/press/key/date/2006/html/sp061004.en.html>
- (2) Hustinx, Peter, European Data Protection Supervisor (EDPS) opinion on the role of the European Central Bank in the SWIFT case, 1 February 2007, http://www.europarl.europa.eu/hearings/20070326/libe/edps_opinion_swift_en.pdf
- (3) European Parliament, Public Hearing, "The Interception Of Bank Transfer Data From The Swift System By The Us Secret Services" 4 October 2006, http://www.europarl.europa.eu/hearings/20061004/libe/programme_en.pdf
- (4) Summary of the opinion on the transfer of personal data by SCRL SWIFT following the UST (OFAC) subpoenas, http://www.privacycommission.be/communiqu%E9s/summary_opinion_Swift_%2028_09_2006.pdf. The original full version of 27 February 2007 (in Dutch) can be found here: <http://www.privacycommission.be/persberichten/AD37-2006.pdf>
- (5) Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), 22 November 2006, http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2006_en.htm
- (6) 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, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT>
- (7) Press Release SWIFT, March 29, 2007, http://www.swift.com/index.cfm?item_id=61490
- (8) Safe Harbor privacy principles issued by the U.S. Department of Commerce on 21 July 2000, http://www.internet-observatory.be/internet_observatory/pdf/legislation/law_int_2000-07-21.pdf
- (9) European Parliament (Committee on Civil Liberties, Justice and Home Affairs),

Programme - Public Seminar: "PNR/SWIFT/Safe Harbour: Are transatlantic data protected?"
26 March 2007,
http://www.europarl.europa.eu/meetdocs/2004_2009/documents/oj/658/658892/658892en.pdf