Society for Worldwide Interbank Financial Telecommunication

9 November 2006
BE_DPC_Executive_Summary

EXECUTIVE SUMMARY OF SWIFT'S RESPONSE TO THE BELGIAN PRIVACY COMMISSION'S ADVISORY OPINION 37/2006 OF 27 SEPTEMBER 2006

SWIFT has submitted a detailed answer of more than 60 pages to the Belgian Privacy Commission in response to the findings set forth in its advisory opinion of 27 September 2006. As the executive summary below of SWIFT's response makes clear, SWIFT continues to believe that it acted in full compliance with applicable laws when it complied with lawful and mandatory subpoenas served on its US branch by the US authorities for a sub-set of message data transiting through its network as part of its SWIFTNet FIN service.

The principal defect in the Commission's analysis is that it considered SWIFT as a data controller within the meaning of the Belgian data privacy law, including in relation to the UST's processing of the subpoenaed data. SWIFT's detailed answer demonstrates why SWIFT is a data processor only. *It therefore follows that SWIFT has not violated the Belgian data privacy law in connection with the actions imposed upon its US branch by the US authorities in respect of data held by it in the US. SWIFT's detailed answer also demonstrates the extent to which SWIFT obtained from the US authorities significant and unique protections for the data subpoenaed. In many instances, these protections are responsive to the data protection principles applicable in Europe, notwithstanding the fact that the provisions of the Belgian (and other European) data privacy laws were not applicable to the delivery of data in response to the US subpoenas. Finally, the detailed answer demonstrates that the Commission's judgment that SWIFT would have committed a "serious error of judgment" is unfounded and inappropriate.*

S.W.I.F.T. ***SCRL***

Avenue Adèle 1 - B-1310 La Hulpe - Belgium
Tel.:+32 2 655 31 11 - Fax: +32 2 655 32 26 - SWHQ BE BB - www.swift.com
VAT: BE 413.330.856 - RPM Nivelles

[1-6] **1. A brief restatement of the facts. –** SWIFT offers as its principal service, to its members and other financial institutions, a highly secure, automated and standardized financial messaging service, known as "SWIFTNet FIN", which is used by financial institutions to perform international payment and other transactions on behalf of their clients. SWIFT only has contractual relations with financial institutions, and not with the clients of those institutions.

The SWIFTNet FIN service is critical for the financial industry worldwide. As a result, the SWIFT architecture and infrastructure meets various requirements, to ensure full resilience of the SWIFT network and the confidentiality and integrity of the messages carried through the network. This has dictated since the inception of SWIFT that it store messages in two operating centers located in Europe and in the US, operating in real time as a mirror to one another. This architecture, known to the SWIFT users, is one of the critical components of the SWIFT messaging service which is overseen by the G10 Central Banks.

In the aftermath of September 11, 2001, SWIFT's US branch was subpoenaed by the US Treasury for a sub-set of message data transiting through its network as part of its SWIFTNet FIN service and located in the US. SWIFT had no option under US law but to comply with the valid and mandatory subpoenas served upon its US branch. SWIFT nevertheless obtained from the US authorities significant protections that ensured that only the data relevant to a terrorism investigation was accessible, that the data remained confidential and secure and that the US authorities' actions be monitored in real time. A written agreement documents these procedures.

[7 - 11] 2**. The Commission's reasoning. –** The Commission[1] ultimately found that SWIFT should have informed European Privacy Authorities and the European Commission in due course of the US Treasury decision to subpoena a sub-set of message data from SWIFT's US branch. This information, according to the Commission, would have enabled these authorities to develop a common European solution (much in the same way as was done in relation to passengers' name records (PNR) data) for the communication of personal data to the relevant US authorities.

Having no jurisdiction with respect to the US authorities' actions themselves, the Commission chose to qualify SWIFT as a data *controller* within the meaning of the Act[2], thus rendering SWIFT responsible for complying with the Act in the context of its SWIFTNet FIN service and of the UST's processing of the subpoenaed data.

---

[1] The Belgian Privacy Commission

[2] The Belgian law of December 8, 1992 on the protection of privacy with regard to the processing of personal data, as amended.

Through this erroneous qualification, the Commission determined that the Act is applicable to, and that it thereby had jurisdiction over, a disclosure imposed by US authorities on SWIFT's US branch which takes place entirely on US soil. The Commission referred to precedents such as the PNR and the SOX (Sarbanes-Oxley) cases, despite a dispositive distinction. Unlike the facts in these precedents, no data is being transferred by SWIFT from the EU to the US Treasury.

By thus wrongly giving the Act an – overreaching - extraterritorial effect, the Commission was able to criticize - through SWIFT - the US authorities' actions on their own territory in the context of the fight against terrorism. Yet, if such purpose of the processing – the fight against terrorism – were to be determined by a EU Member State's authority, it would fall outside the scope of Directive 95/46/EC and the jurisdiction of EU Member States' national Data Protection Authorities since it relates to the EU's second pillar[3]. In matters of public security and fight against terrorism, there currently exists in Europe a legal void with respect to data protection rules.
The Commission's findings not only entail absurd consequences for international data transmission providers such as SWIFT, but are also inconsistent with the Act and general data protection principles.

[12 - 15] **3. The Act's material and territorial scope (art. 3 and 3bis of the Act). –** To establish its jurisdiction under the Act, it would have been sufficient for the Commission to establish that Belgian financial institutions - as data *controllers* - used the services of SWIFT – as data *processor*. This would have resulted in the Act being applicable to the processing of personal data collected by Belgian financial institutions in the context of their international payment or other activities through use of the SWIFTNet FIN service.

The Commission however found the Act applicable for the sole reason that SWIFT's registered office was located in Belgium, thereby necessarily implying that SWIFT was a *controller* under the Act. SWIFT does not challenge the fact that some of the provisions of the Act apply to its processing activities in the context of its SWIFTNet FIN service, but only as *processor* on behalf of the Belgian financial institutions, and not as a data *controller*.

With respect to the processing under the Commission's scrutiny, i.e. the access of data by the US Treasury, the Commission failed to analyze SWIFT's role and simply applied the erroneous qualification of SWIFT as a data *controller* in the SWIFTNet FIN-context to the separate UST processing-context. A proper analysis of SWIFT's role in this latter respect should have concluded instead that such processing, i.e. the transmission of data to public authorities for purpose of public security, is distinct from the initial processing in the context of the SWIFTNet FIN

[3] Matters of public security fall within the EU's second pillar, for which no harmonized Community data protection rules exist.

service and does not fall within the territorial scope of the Act. The Commission therefore failed to justify the applicability of the Act to the UST processing.

Neither of the two territorial applicability criteria set forth in Article 3bis of the Act is met with regard to the processing by the UST (i.e. link to the activities of an establishment of the data controller in the country or use of equipment located in the country). Therefore, the Act is not applicable to the UST processing and the Commission should have concluded accordingly.

[16 - 23] **4. SWIFT is a carrier of messages, a "data *processor*" within the meaning of art.1, §5, of the Act. –** SWIFT, in the context of its SWIFTNet FIN service, carries out the secure transmission of financial messages between financial institutions, in accordance with the financial institutions' instructions and on their behalf. The financial institutions collect the personal data directly from their clients. Likewise, the financial institutions determine the means of processing by deciding whether to use SWIFT's services, rather than the available alternative transmission services offered by competing service providers to SWIFT, such as virtual private networks, banks' proprietary networks, internet, etc. Finally, the financial institutions determine the purpose of the processing – e.g. the execution of international payment orders. For the purposes of the Act, only the (Belgian) financial institutions are data *controllers*, since they determine both "the purposes and the means of the processing of the personal data". SWIFT, by contrast, is the *processor* of the data within the meaning of the Act, i.e. "it processes personal data on behalf of the controller".

The Commission distinguished between (i) the processing of the personal data in the context of the financial institutions' international payment services, which the Commission rightly held to be under the institutions' sole control, and (ii) the mere processing of personal data allegedly taking place in the context of the SWIFTNet FIN service, which would be carried out under SWIFT's and the financial institutions' joint control.

The Commission's finding in that respect is ill-founded, because SWIFT's role is limited to a mere financial messaging provider. Indeed, contrary to the two examples provided by the Commission (i.e. the Terminated Merchants Databases in the VISA-MASTERCARD cases and the computer reservation systems in the airline sector), the SWIFTNet FIN service does not include any processing of personal data contained in the financial messages. SWIFT's role is limited solely to the transmission of financial messages on instruction of its customers.

SWIFT does not determine the purposes of the processing and therefore cannot be qualified as data *controller* within the meaning of the Act in the context of its SWIFTNet FIN service. SWIFT's qualification as data *processor* is completely in line with Directive 95/46/EC, with the Act's parliamentary preparatory works, and with the contractual documentation entered into between SWIFT and its customers (which contract the Commission simply ignored, in violation of Article 16 of the

Act, the general principles of Belgian law and the case law of the Belgian Supreme Court).

Interestingly, the first European Privacy Authority that has taken a position on the issue, the German regional privacy authority Schleswig-Holstein Unabhängiges Landeszentrum für Datenschutz, has in its detailed opinion of 23 August 2006, rightly determined that "SWIFT acts as an agent or subcontractor of the data controllers, the members of the SWIFT group" (i.e. the financial institutions). Such finding[4] is based on the same factual background as the one in Belgium and is rendered under similar legislation, both countries having implemented Directive 95/46/EC. There is thus every reason for this holding that qualifies SWIFT as *processor* to apply equally in Belgium under the Act. SWIFT calls upon the Article 29 Data Protection Working Party for a harmonized application of the definitions of "*controller*" and "*processor*" as set forth in such Directive, consistent with the German regional privacy authority qualification.

[24 - 27] **5. SWIFT does not exceed the role of a data *processor* in the context of its SWIFTNet FIN service. –** The Commission found that since SWIFT managed a "strongly centralized international cooperative network", and made decisions reaching beyond the normal margin of maneuver of a processor, SWIFT exceeded the role of a mere data *processor* under the Act. In other words, the engineering by SWIFT of an overall complex offering of secure messaging services would, in the Commission's opinion, command SWIFT's qualification as data *controller* under the Act.

Should the Commission's reasoning that a processor may not determine the technical standards of its service, be deemed correct, then no data transmission provider may ever be qualified as data *processor* under European data protection laws. However, Directive 95/46/EC expressly states otherwise.

In addition, the Act does not require the *controller* to determine the *processor*'s service architecture, as designed and established for the subcontracted processing. SWIFT, as *processor*, may decide on the technical architecture and specifications of its network and services. On the other hand, the financial institutions, by selecting SWIFT as processor and by verifying that its service architecture meets the relevant confidentiality and security requirements for the contemplated data processing, determine the "means" of the processing under the Act.

The technical standards and the architecture of SWIFT's services are moreover exclusively designed in order to meet the financial institutions' specific requirements regarding the security, stability and resilience of a critical network for the global financial system. In this regard, SWIFT has fully complied with its

[4] SWIFT refers to the authority's finding with respect to SWIFT's qualification as *processor*, and not to other findings of such authority, which SWIFT contests.

obligation as data processor to have the technical security and organizational measures in place to protect the data.

[28 – 29] **6. SWIFT does not exceed the role of a data *processor* in the context of the UST processing. -** The Commission found that SWIFT's decision to comply with the UST's subpoenas resulted in SWIFT becoming a data *controller* in the context of the UST processing, because such "decision" is incompatible with a data processor's role under the Act.

The Commission however ignored the fact that SWIFT had no choice but to comply with compulsory subpoenas lawfully issued by the UST to its US branch. Indeed, SWIFT was forced to grant access to data stored in the US, and at no time did it determine the purposes of the UST's processing (the fight against terrorism) nor did it determine its means (the search tool has been developed, is controlled and is operated by the UST). SWIFT held no decision power over the processing and, as a result, cannot be qualified as the data *controller* of a processing imposed upon it by US laws and US authorities.

It is in this context surprising that the Commission criticizes SWIFT for having obtained from the UST extensive data protections and assurances, restrictive access conditions and independent supervision. The financial institutions are aware – through the SWIFT Data Retrieval Policy – that SWIFT may be forced to retrieve, use or disclose message data in order to comply with a bona fide subpoena or other lawful process by a court or other competent authority. In such a case, SWIFT is required to continue fulfilling its contractual obligations as *processor*, i.e. protect the data security and confidentiality. SWIFT did so successfully by obtaining from the UST extensive security measures covering the required disclosure. It is thus startling that SWIFT is criticized by the Commission for having obtained the protections of personal data that the Act aims to implement, for having endeavored to limit the UST access to what was strictly necessary to the purpose of fighting terrorism financing and for having put 'oversight' controls in place to ensure the above, in circumstances where the Act nevertheless did not apply.

[30 - 39] **7. SWIFT did not infringe the Act in the context of its SWIFTNet FIN service. –** Because SWIFT is a data *processor* under the Act, no infringement of a data *controller*'s obligations of information and declaration may be imputed to SWIFT (art. 9 and 17 of the Act). Only the financial institutions have direct and contractual relationships with data subjects and are in a position to ensure the effectiveness of the data subjects' rights under the Act.

The Commission's assertion that these obligations rest with SWIFT entails absurd consequences: for instance, in order to comply with the data subjects' information obligation, SWIFT would be required to open all financial messages transiting through its network in order to attempt to identify data subjects (the financial institutions' clients) in more than 200 countries. This would be in violation of both the proportionality and confidentiality principles and would be an absurd and

impossible task, considering that more than 11 million messages transit daily through the SWIFT network.

With respect to SWIFT's alleged infringement of the rules under the Act (art. 21) prohibiting transfer of data to the USA - a jurisdiction deemed not to afford an adequate level of protection to the data transferred - the Commission's findings are unfounded.

The SWIFT messaging services involve operating centers on different continents. These are operated by SWIFT branches. Because SWIFT's US branch does not constitute a legal entity separate from SWIFT (a Belgian company), SWIFT *itself* remains legally responsible for the data processing in its relationship with the data controllers and therefore, the data transferred to the US operating center remain entirely subject to the Act. Contrary to the Commission's assertion, the protection of the data concerned is thus in no way undermined: the applicable level of protection necessarily remains in the present circumstances adequate *because* it is the level of protection prescribed by the Act, which remains applicable to SWIFT to the extent of its obligations as data processor.

Moreover, even if it were held that no adequate level of protection applies as a result of the data processed in the US, the Act contains various exceptions that are applicable in the circumstances (art. 22 of the Act):

a. The Act provides that important public interest grounds can justify cross-border transfers to a country not ensuring an adequate level of protection. This exception is met in the current circumstances given the requirement of resilience of the SWIFT network and infrastructure that is critical to the Belgian, European and global financial system and overseen as such by the G10 Central Banks. Such requirement dictates the location of an operating centre in the US, much for the same reasons that several European national banks are keeping their gold reserves in the US. The Commission did not address the application of this exception, except by simply noting that the US are not deemed to offer an adequate level of protection, but this is precisely why the identified exception exists in the first place.

b. Since the cross-border transfer of personal data is an integral part of the purpose of the processing – e.g. the execution of an international payment order- and is necessary for meeting the financial institutions' specific needs for a highly secure and resilient network, such transfer is necessary for the performance of the contract between the data subjects and the financial institutions as *controllers*, but also for the performance of the contract between SWIFT as *processor* and the financial institutions as *controllers*, in the data subjects' interest.

Finally, the Commission points to certain "solutions" (binding corporate rules, standard contractual clauses, Safe Harbour) that SWIFT should have considered to validate the export of the data to the US. These "solutions" were not legally available to SWIFT in the current circumstances. Contractual solutions (standard

clauses) and Binding Corporate Rules were unavailable, because SWIFT's US branch does not have a separate legal personality, and because SWIFT is not a data *controller*. Since SWIFT's US branch does not qualify as a "US Organization", the Safe Harbour solution was equally unavailable.

Moreover, even if these “solutions” could have been applied, they would not have prevented the UST from accessing message data, by way of compulsory subpoenas issued under US law in respect of data located in the US.

[40 – 50] **8. SWIFT did not infringe the Act in the context of the UST processing. -** The Act, as already demonstrated, is not applicable to the UST processing imposed upon SWIFT’s US branch by US authorities on US soil. The Commission also expressly admitted the validity and compulsory character of the UST subpoenas, SWIFT’s legitimate interest within the meaning of the Act in complying with these subpoenas and the existence of a conflict of laws.

The Commission, however, artificially differentiated between the processing by the UST of subpoenaed data and the data processing operated by SWIFT *as part of the UST processing.* It held SWIFT responsible for the data processing operated *as part of the UST processing*, notwithstanding the fact that SWIFT had no decision power or influence over the various elements of such processing (including as to data quantity, data holding period, confidentiality of the processing, independent supervisory authority and transparency).

The Commission's reasoning, which led it to consider that SWIFT had infringed the Act, and in particular the proportionality principle and the obligations of information and transparency, is conceptually flawed, and its conclusions without basis under the Act.

Concerning SWIFT’s alleged infringement of the ***proportionality*** principle (art. 4 of the Act), SWIFT notes that if it had challenged the UST’s subpoenas in court (which SWIFT determined was highly unlikely to conclude the subpoena was invalid under US law – based upon advice received from specialized outside counsel), such challenge would almost certainly have led to the UST accessing the data *without* the very restrictive access conditions SWIFT was able to obtain from the UST.

The Commission found that SWIFT “limited itself” to complying with US law and should have considered alternatives. None of the so-called "alternative schemes" identified by the Commission were in any way available to SWIFT. This is particularly true for the various official procedures and treaties that the Commission argues were available to SWIFT: (i) The Financial Action Task Force (“FATF”) is certainly no forum SWIFT could have consulted in the context of the lawful and compulsory subpoenas that its US branch received. FATF issues recommendations to its member States while SWIFT is a private entity, and the FATF is certainly not an international forum to deal with valid measures issued

against private persons by its member States. (ii) SWIFT is not a "Financial Intelligence Unit" ("FIU"), and may thus not address itself to the Egmont Group, an informal information exchange forum between States' FIUs. (iii) Finally, the Agreement on Mutual Legal Assistance between the EU and the US of 25 June 2003 did not exist at the time the UST subpoenas were issued - and is still currently not in force - and will in any case become only binding upon States*;* equally relevant, it applies only to data located in the contracting member state, and not like in the present case in the state of the requesting party; finally, under the terms of this Agreement on Mutual Legal Assistance, data protection principles cannot as a rule constitute an obstacle to cooperation by the requested State.

The obligations of ***information*** *and* ***transparency*** (art. 4 of the Act and art. 8 of the European Convention of Human Rights) were not applicable to SWIFT given its role under the Act as a *processor*. Nevertheless, SWIFT did inform its overseers (the G10 central banks) of the UST subpoenas. Moreover, the financial institutions were already aware – through SWIFT's Data Retrieval Policy – of the fact that SWIFT may be forced to retrieve, use or disclose message data in order to comply with a bona fide subpoena or other lawful process by a court or other competent authority.

SWIFT also obtained monitoring of the UST's access in real time by SWIFT, as well as auditing by an external audit company, a quite remarkable achievement with respect to a government's actions with respect to public security.
Finally, since the subpoenaed subset of data already were on US soil, at no point did any crossborder data transfer exist. No infringement of the Act in this respect may thus exist.

9. Conclusions. – SWIFT strongly objects to the Commission's findings and to the judgment it expressed that SWIFT would have committed a "serious error of judgment", whereas SWIFT obtained unique and effective data protection guarantees from the UST, in circumstances where the Act was not applicable.

SWIFT is caught in a political debate over the proper balance that must be struck between the need for data privacy protections and the need for personal security. SWIFT strongly believes that it did its utmost to achieve the right balance in the difficult circumstances that it was confronted with and in light of the limited options available to it, in full compliance with its duties as data *processor* under the Act. SWIFT welcomes the ongoing reflections on the need for a clear and stable EU-US legal framework for these issues in order to avoid that in the future, SWIFT and other private companies be placed in similar circumstances.

* * *