Processing of EU originating Personal Data by United States Treasury Department for Counter Terrorism Purposes — 'SWIFT'

(2007/C 166/09)

Terrorist Finance Tracking Program — Representations of the United States Department of the Treasury

These representations describe the U.S. Department of the Treasury's Terrorist Financing Tracking Program (TFTP) and, in particular, the rigorous controls and safeguards governing the handling, use, and dissemination of data received from SWIFT under compulsion of administrative subpoenas. These controls and safeguards apply to all persons having access to the SWIFT data, unless otherwise noted in specific examples such as those describing the sharing of lead information derived from the SWIFT data with foreign governments.

The TFTP is grounded in law, carefully targeted, powerful and successful, and bounded by privacy safeguards. It represents exactly what citizens expect and hope their governments are doing to protect them from terrorist threats.

The Treasury Department's Terrorist Finance Tracking Program

Shortly after the September 11, 2001 attacks, as part of an effort to employ all available means to track terrorists and their networks, the Treasury Department initiated the TFTP. Under the TFTP, the Treasury Department has issued administrative subpoenas for terrorist-related data to the U.S. operations center of the Society for Worldwide Interbank Financial Telecommunication (SWIFT), a Belgium-based cooperative that operates a worldwide messaging system used to transmit financial transaction information. These subpoenas require SWIFT to provide the Treasury Department with certain financial transaction records — which are maintained by SWIFT's U.S. operations center in the ordinary course of its business — to be used exclusively for counterterrorism purposes as specified in the following sections.

Fundamental Principles Underlying the TFTP

From its inception, the TFTP has been designed and implemented to meet applicable U.S. legal requirements, to contribute meaningfully to combating global terrorism, and to respect and protect the potential commercial sensitivity of and privacy interests in the SWIFT data held in the United States. The TFTP takes into consideration the potential commercial sensitivity and individual privacy interests in the information it encompasses, and the safeguards detailed in these representations apply irrespective of the nationality or place of residence of the individuals involved. The program contains multiple, overlapping layers of governmental and independent controls to ensure that the data, which are limited in nature, are searched only for counterterrorism purposes and that all data are maintained in a secure environment and properly handled.

All actions by the Treasury Department to obtain specified information from SWIFT's U.S. operations center and to use that information exclusively for investigating, detecting, preventing, and/or prosecuting terrorism or its financing or related follow-on investigations and prosecutions are in accordance with U.S. law. Moreover, the data submitted by SWIFT are not searched to collect evidence or detect activity that is not related to terrorism or its financing, even though such activity in itself may be unlawful. The Treasury Department does not perform searches on SWIFT data, nor can the information be used, in connection with general investigations of tax evasion, money laundering, economic espionage, narcotics trafficking or other criminal activity, unless in a particular instance such activity has been connected to terrorism or its financing.

The data received from SWIFT under compulsion of subpoenas consist of copies of completed financial transaction messages, *i.e*, electronic copies of business records maintained at SWIFT's U.S. operations center in the ordinary course of business. Though this data may undergo some processing in the sense of the very restricted counterterrorism search-and-retrieval capacity described herein, there is no alteration, manipulation, addition or deletion of data within individual transaction messages within the searchable database.

The TFTP has proven to be a powerful investigative tool that has contributed significantly to protecting U.S. citizens and other persons around the world and to safeguarding America's and other countries' national security. The program has been instrumental in identifying and capturing terrorists and their financiers, and it has generated many leads that have been disseminated to counterterrorism experts in intelligence and law enforcement agencies around the world.

Concerns Raised Within the European Union

After the public media disclosure of the TFTP in June 2006, concerns were raised in the EU about the TFTP program and, in particular, the possibility that the Treasury Department might have access to personal data relating to an identified or identifiable natural person contained in financial transactions processed by SWIFT. In particular, questions were raised on the TFTP's consistency with obligations under the Data Protection Directive (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), as well as Member State laws implementing that Directive.

Nature of SWIFT Data

The financial transaction records provided by SWIFT under compulsion of subpoena may include identifying information about the originator and/or recipient of the transaction, including name, account number, address, national identification number, and other personal data. It would be highly unusual for SWIFT financial records to include 'sensitive' data as referred to in Article 8 of Directive 95/46/EC (*i.e.*, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning the health or sex life of the individual).

International Counterterrorist Financing Principles

The SWIFT financial data used in the TFTP is extraordinarily valuable in combating global terrorism and its financing, and in carrying out the government's responsibility to defend the public and safeguard national security and to detect, prevent, investigate and prosecute terrorist crimes.

The international community and national authorities recognize that money is the lifeblood of terrorism. This is reflected in the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism and numerous United Nations resolutions relating to the prevention and suppression of the financing of terrorists acts, particularly United Nations Security Council Resolution 1373. In the United States, the Treasury Department and the Congress established the Office of Terrorism and Financial Intelligence in 2004 to marshal the Department's enforcement and intelligence functions with the twin aims of safeguarding the financial system against illicit use and combating, among others, terrorists and other national security threats. The office's various components gather and analyze information from the law enforcement, intelligence, and financial communities as to how terrorists (and other criminals) earn, move, and store money. These activities enable the office to freeze terrorists' assets, to combat terrorism generally, and to develop and promote counterterrorist financing standards in the United States and abroad.

These and other initiatives reflect the everyday reality that terrorists depend on a regular cash flow to pay operatives, arrange for travel, train new members, forge documents, pay bribes, acquire weapons, and stage attacks. In order to send money through the banking system, they often provide information that yields the kinds of concrete leads that can advance a terrorism investigation. This is why counterterrorism officials place a high premium on financial intelligence, including that derived from programs such as the TFTP, which has proved to be of inestimable value in combating global terrorism.

This is also why the financial industry is subject to extensive recordkeeping and reporting requirements that are designed to support governmental counterterrorism efforts. Countries throughout the world have mandated this by law, consistent with the recommendations of the Financial Action Task Force. For example, in the United States, the primary statutory authority is the Bank Secrecy Act. In Europe, similar provisions have been implemented into national law consistent with the Third Money Laundering Directive and, most recently, Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds.

Legal Authority to Obtain and Use SWIFT Data

The subpoenas served on SWIFT are based on longstanding statutory authorities and a related Executive order for combating terrorism and its financing. The International Emergency Economic Powers Act of 1977 (IEEPA) authorizes the President of the United States, during a declared national emergency, to investigate bank transfers and other transactions in which a foreign person has any interest. Similarly, the United Nations Participation Act of 1945 (UNPA) authorizes the President, when implementing United Nations Security Council Resolutions, to investigate economic relations or means of communication between any foreign person and the United States.

On September 23, 2001, the President, relying in part on IEEPA and UNPA and citing United Nations Security Council Resolutions targeting the Taliban and Al Qaida, issued Executive Order 13224. In that Order, the President declared a national emergency to deal with the 9/11 terrorist attacks and the continuing and immediate threat of further attacks, and blocked the property of, and prohibited transactions with, persons who commit, threaten to commit, or support terrorism.

For the purposes of Executive Order 13224, section 3 contains the following definition:

the term 'terrorism' means an activity that —

(i) involves a violent act or an act dangerous to human life, property, or infrastructure; and

(ii) appears to be intended —

(A) to intimidate or coerce a civilian population;

(B) to influence the policy of a government by intimidation or coercion; or

(C) to affect the conduct of a government by mass destruction, assassination, kidnapping, or hostage-taking.

In section 7 of the Order, the President authorized the Secretary of the Treasury Department to employ all powers granted to the President by IEEPA and UNPA as may be necessary to carry out the purposes of the Order. He also authorized the Secretary of the Treasury to redelegate any of these functions to other officers and agencies of the U.S. Government, and directed all agencies of the U.S. Government to take all appropriate measures within their authority to carry out the provisions of the Order. IEEPA and the Order, as implemented through the Global Terrorism Sanctions Regulations, authorize the Director of the Treasury Department's Office of Foreign Assets Control (OFAC) to require any person to furnish financial transaction or other data in connection with an economic sanctions-related investigation. These are the legal authorities under which OFAC issues subpoenas to SWIFT for financial data that are related to terrorism investigations.

Access Control and Computer System Security

The data obtained from SWIFT, consistent with U.S. Government procedures for the handling of information related to the investigation of terrorism and its financing more generally, are subject to strict technical and organizational measures to protect the information against accidental or unlawful destruction, loss, alteration or access. All of the following security measures are subject to independent audit.

The SWIFT data are maintained in a secure physical environment, stored separately from any other data, and the computer systems have high-level intrusion controls and other protections to limit access to the data solely as described herein. No copies of SWIFT data are made, other than for disaster recovery back-up purposes. Access to the data and the computer equipment are limited to persons with appropriate security clearances. Even among such persons, access to the SWIFT data is on a read-only basis and is limited through the TFTP on a strict need-to-know basis to analysts dedicated to the investigation of terrorism and to persons involved in the technical support, management, and oversight of the TFTP.

Extraction and Usage Limited to the Investigation of Terrorism

The TFTP does not involve data mining or any other type of algorithmic or automated profiling or computer-filtering. Multiple layers of strict controls have been built into the TFTP to limit the information collected, to ensure that information is extracted and used only for counterterrorism purposes, and to protect the privacy interests of individuals not connected with terrorism or its financing. These overlapping safeguards continuously narrow and significantly restrict access to and use of the financial data handled by SWIFT in its day-to-day operations

As a threshold matter, the subpoenas served upon SWIFT are carefully and narrowly tailored to limit the amount of data furnished to the Treasury Department. SWIFT is required to provide only data the Treasury Department believes will be necessary in combating terrorist financing, on the basis of past analyses focusing on message types and geography, as well as perceived threats and vulnerabilities. Additionally, searches are narrowly tailored to minimize the extraction of messages that are not relevant to a terrorism investigation. The data provided by SWIFT are searched to extract only information that is related to an identified, preexisting terrorism investigation. This means that every search that is conducted must specifically cite to and record documented evidence supporting the belief that the target is connected with terrorism or its financing. Each and every search of the SWIFT data under the TFTP is also logged contemporaneously, including such affirmative terrorism nexus required to initiate the search.

As a result of the foregoing safeguards, only a minute fraction (*i.e.*, substantially less than one percent) of the subset of the SWIFT messages furnished to the Treasury Department has been actually accessed, and only because those messages have been directly responsive to a targeted, terrorism-related search.

Independent Oversight

In addition to the Treasury Department's ongoing exercise of the controls described herein, the TFTP includes multiple complementary layers of independent oversight: by representatives of SWIFT itself, an independent auditing firm, and other independent U.S. government authorities, including the U.S. Congress.

SWIFT and outside auditors it has retained exercise their independent oversight of the TFTP in several mutually complementary ways. First, certain SWIFT representatives have been granted appropriate security clearances to have 24-hour access to the equipment and data and the ability to monitor, in real time and retrospectively, the use of the data to ensure that they are accessed only for counterterrorism purposes. Additionally, these SWIFT representatives may stop any specific search immediately, and even have the ability to shut down the entire system, if they have any concerns.

With respect to the independent, outside auditors, the maintenance, access to, and use of the SWIFT data are subject to continued, periodic independent audit pursuant to carefully delineated protocols consistent with international auditing standards. These audits cover the access control and computer system security safeguards, as well as the limitation of data usage for the investigation of terrorism, as described above. The independent auditors report their conclusions to the audit and finance committee of SWIFT's Board of Directors.

In addition, consistent with U.S. law, various congressional committees have been repeatedly briefed on the TFTP and its operation, and they continue to be briefed on a regular basis. The TFTP has also been the subject of congressional hearings.

Finally, the Privacy and Civil Liberties Oversight Board, which was established pursuant to the Intelligence Reform and Terrorism Prevention Act of 2004, exercises oversight of the TFTP. The Board's mission is to ensure that concerns with respect to privacy and civil liberties are appropriately considered in the implementation of all U.S. laws, regulations, and executive branch policies related to efforts to protect the United States against terrorism. The Board also is responsible for reviewing the terrorism information-sharing practices of executive branch departments and agencies to determine whether guidelines designed to appropriately protect privacy and civil liberties are being followed.

As described below, this extensive, independent oversight works in tandem with restrictive dissemination controls that operate to further restrict access to information derived from the SWIFT financial records and to further protect privacy interests.

Dissemination and Information Sharing

The international community has recognized the critical importance of sharing terrorism information. For example, UNSCR 1373 calls upon all States to find ways to intensify and accelerate the exchange of operational terrorism information and to exchange information to prevent the commission of terrorist acts. Similarly, section 6 of Executive Order 13224 requires the Secretary of the Treasury (and other officials) to make all relevant efforts to cooperate and coordinate with other countries to achieve the objectives of the Order, including preventing and suppressing acts of terrorism, denying financing and financial services to terrorists, and sharing intelligence about funding activities in support of terrorism. It is against this backdrop that information derived from the SWIFT data is appropriately shared with domestic and international partners. As is true with all other facets of the TFTP, this information-sharing is in accordance with U.S. law and subject to a series of safeguards that are designed to protect the SWIFT data and the privacy interests of the persons to whom it may pertain.

The counterterrorism analysts conducting TFTP searches verify the relevance of any information produced in response to a search before that information is prepared for dissemination through secure channels. The Treasury Department also exercises originator control on any subsequent dissemination of the information, meaning that no recipient is permitted to further disseminate the information without the Treasury Department's express approval. In that regard, as with any unauthorized access to the SWIFT data, any unauthorized disclosure of TFTP-derived information may result in strict disciplinary action or the imposition of civil or criminal penalties.

Information derived from the SWIFT data is shared under strict controls with other U.S. agencies in the intelligence and law enforcement communities to be used exclusively for the purpose of investigating, detecting, preventing, and/or prosecuting terrorism or its financing or related follow-on investigations and prosecutions. This sharing is mandated by the National Security Act, the Intelligence Reform and Terrorism Prevention Act of 2004, and a series of Memoranda of Understanding and related Executive orders. The recipient agencies have the same obligations under U.S. law as the Treasury Department to protect TFTP-derived information. It is also important to note that TFTP-derived information is shared with other U.S. agencies for lead purposes only, which limits its use as affirmative evidence in legal proceedings. Recipient agencies use their own, existing legal authorities to pursue their investigations, including to obtain documentation from other sources that could later be used as evidence in legal proceedings.

These other government agencies also share lead information derived from the SWIFT data with their foreign counterparts for the same purposes, with case-by-case approval from the Treasury Department when justified by national security and law enforcement interests. Many TFTP-derived leads have been shared with foreign authorities, as a general matter without revealing the TFTP as the source.

As for possible public dissemination of SWIFT data, the Treasury Department treats the data as classified, law enforcement sensitive, business confidential information. Accordingly, the Treasury Department does not and would not make the data publicly available unless required to do so by law. In that regard, the Treasury Department will take the position in connection with any administrative or judicial proceeding arising out of a Freedom of Information Act (FOIA) request from third parties for TFTP data, that such records are exempt from disclosure under FOIA.

Redress

The confined nature of the data in an individual SWIFT transaction message, the restricted manner in which certain SWIFT data can be accessed through the TFTP as part of a preexisting investigation of terrorism, and the limits on dissemination as lead information significantly reduce the pertinence of a redress mechanism as part of the TFTP itself. That notwithstanding, appropriate redress for possible misuse by governmental authorities is available under U.S. law.

With regard to an interest of a specific natural person about the use of data and the ability to seek redress for possible misuse, a distinction must be made between the searchable data submitted by SWIFT and messages extracted as part of a targeted terrorism investigation that may serve as the basis for an administrative decision or other governmental action. The data received from SWIFT under compulsion of OFAC subpoenas consist of copies of completed financial transaction messages, *i.e.*, electronic copies of business records maintained at SWIFT's U.S. facility in the ordinary course of business. Though this data may undergo some processing in the sense of the very restricted counterterrorism search-and-retrieval capacity described herein, there is no alteration, manipulation, addition or deletion of data within individual transaction messages within the searchable database.

Additionally, it is again important to emphasize that the vast majority of the transaction messages provided by SWIFT will never be viewed even by counterterrorism analysts, and thus are not known. Consequently, responding to a privacy-related inquiry from a natural person as to whether information about that individual is included in the database would require, in almost all instances, accessing data that would never be accessed in the normal operation of the TFTP. Such access would be inconsistent with the TFTP requirement that every search have a preexisting nexus to terrorism. Finally, because there is no alteration, manipulation, deletion or addition of the data within the searchable database, there exists no basis to 'rectify' any information. Moreover, this would serve to alter the completed business records sought by the OFAC subpoena.

Further processing of the data in an individual transaction message will only occur with respect to the relatively few individual transaction messages directly responsive to a targeted terrorism search that are extracted from the search database. Once extracted and subject to the multiple controls limiting dissemination for counterterrorism purposes, redress for alleged misuse could properly be sought following the appropriate administrative and judicial procedures with respect to the government's acting upon that disseminated information.

The opportunity for redress can be illustrated as follows with respect to an administrative action taken by OFAC to block property under the Global Terrorism Sanctions Regulations that implement Executive Order 13224. A person may seek administrative reconsideration by OFAC of his or her designation as a specially designated global terrorist, whereby that person is given the opportunity to demonstrate that 'the circumstances resulting in the designation no longer apply' and to 'submit arguments or evidence that the person believes establishes that an insufficient basis exists for the designation'. A specially designated global terrorist also may seek judicial review of an agency's decision under relevant provisions of the Administrative Procedure Act. These administrative and judicial avenues to seek redress would apply to any person that is the object of the government decision, regardless of nationality.

Retention Period

The period of time for retention of counterterrorism (and any other) information is a function of numerous, well-established factors, including investigative requirements, applicable statutes of limitation, and regulatory limits for claims or prosecution. The applicability and operation of these and other factors vary from agency to agency, depending on the nature of the agency's specific duties and missions. Accordingly, the retention periods for certain types of terrorism-related information compiled by various agencies depend on the nature of the information and the investigation to which it relates.

Within the U.S. Government, retention and disposition schedules for agency records are approved by the National Archives and Records Administration (NARA) pursuant to various statutes and regulations. All records not deemed to have permanent value must be scheduled for destruction after a specified period of time based on explained administrative, fiscal, and legal values. Factors considered by NARA in approving an agency's record retention periods include applicable statutes of limitation; regulatory limits for claims or prosecution; the potential for fraud; litigation risks and substantive rights; and statutes or regulations granting or limiting a specific legal right.

With regard to a period of time for retention of TFTP-related information, a distinction again must be made between the data subpoenaed from SWIFT and the extracted data that serve as the basis for an administrative decision or other governmental action.

The Treasury Department will endeavour on an ongoing and at least annual basis to identify and delete all non-extracted data that are not necessary for the execution of purposes referred to in these Representations. Subject to the results of the above-mentioned necessity-based analysis, all non-extracted data received by the Treasury Department from SWIFT after the date of publication of these Representations will be deleted by the Treasury Department not later than five years after receipt by the Treasury Department. Subject to the results of the above-mentioned necessity-based analysis, all other non-extracted data will be deleted not later than five years after the date of publication of these Representations.

Extracted data directly responsive to a targeted terrorism search that have been subjected to the multiple dissemination controls described above for counterterrorism purposes, shall be subject to the retention period applicable to the particular government authority with respect to its particular investigative records.

For example, SWIFT data extracted through the TFTP could be used in the investigation of an individual for possible designation under OFAC's Global Terrorism Sanctions Regulations. Under OFAC's NARA-approved record retention schedule, if a final administrative decision is made to designate an individual (which decision would be made public), the information on which the decision was made will be retained permanently as a written record of the evidence supporting the agency's action. The evidentiary file is retained for possible administrative or judicial review in the event a designation is challenged, and also to support further terrorism investigations. Alternatively, if an investigation is closed without a designation, the investigatory files are subject to on-site destruction no later than one year after the investigation is completed.

Finally, consistent with the above-described U.S. legal framework, the retention period for lead information derived from the TFTP that has been disseminated is governed by the regulations and schedules of the recipient agency or government. For example, any derived information that is used in a Justice Department prosecution will be subject to applicable Justice Department retention periods.

Ongoing Counterterrorism Cooperation

The TFTP has been of great value in fighting terrorism globally, including in Europe. The U.S. Government will continue to judiciously assess whether any information obtained through the TFTP may contribute to the investigation, prevention, combating or prosecution of terrorism or its financing in one or more European Union Member States and, in all appropriate cases, will make that information available to the proper authorities in the most expedient manner.

As a sign of our commitment and partnership in combating global terrorism, an eminent European person will be appointed to confirm that the program is implemented consistent with these Representations for the purpose of verifying the protection of EU-originating personal data. In particular, the eminent person will monitor that processes for deletion of non-extracted data have been carried out.

The eminent person will have appropriate experience and security clearances, and will be appointed for a renewable period of two years by the European Commission in consultation with the Treasury Department. The eminent person shall act in complete independence in the performance of his or her duties. The eminent person shall, in the performance of his or her duties, neither seek nor take instructions from anybody. The eminent person shall refrain from any action incompatible with his or her duties under this appointment.

The eminent person will report his or her findings and conclusions annually in writing to the Commission. The Commission in turn will report to the European Parliament and the Council as appropriate.

The Treasury Department will give the eminent person access, information and data necessary for the discharge of his or her duties. The eminent person will at all times act in compliance with secrecy and confidentiality requirements imposed by law. Practical details will be agreed with the Treasury Department.

The Treasury Department also will advise the European Union of any material changes to the safeguards set forth in these representations and of the passage of any U.S. legislation that materially affects the statements made in the Representations.

The Treasury Department will endeavor to have these Representations published in the Federal Register and consents to their publication in the *Official Journal of the European Union*.