SECOND REPORT ON THE PROCESSING OF EU-ORIGINATING PERSONAL DATA BY THE UNITED STATES TREASURY DEPARTMENT FOR COUNTER TERRORISM PURPOSES

TERRORIST FINANCE TRACKING PROGRAMME

JANUARY 2010

Judge Jean-Louis BRUGUIERE

EXECUTIVE SUMMARY

Shortly after the 11 September 2001 terrorist attacks, the United States Department of the Treasury developed the "Terrorist Finance Tracking Programme" ("TFTP") to identify, track and pursue terrorists and their financial supporters. Under the TFTP the U.S. Treasury Department serves administrative orders ("subpoenas") on the U.S. branch of the Belgium-based Society for Worldwide Interbank Financial Telecommunication ("SWIFT"). Pursuant to these administrative orders SWIFT is legally required to provide the U.S. Treasury Department with specified financial record transaction data. Once provided to the U.S. Treasury Department, these data are held on a secure U.S. Government database.

Following disclosure of the previously classified TFTP in mid-2006, the U.S. Treasury Department made a series of unilateral commitments to the European Union concerning the processing of personal data received under the TFTP. These commitments, known as the TFTP Representations, were published in the Official Journal in July 2007, thus for the first time placing in the public domain considerable information about the nature of and safeguards surrounding the TFTP. The Representations make dear, for example, that data received pursuant to the TFTP cannot be processed for any purpose other than the fight against terrorism, that such data must be deleted after a specified period of time and that no searches of data may take place except in cases where there is reason to believe that there is a nexus between the subject of the search and terrorism or terrorist financing. Significantly, the majority of the TFTP privacy safeguards were previously reflected in arrangements between the US. Treasury Department and SWIFT.

The TFTP Representations state that the European Commission could designate an "eminent European person" to verify that the TFTP is implemented consistently with the Representations. In spring of 2008 the French counter terrorism Judge, Mr. Jean-Louis Bruguière, was appointed to carry out this role. Judge Bruguière produced a first Report in December 2008 concluding that the U.S. Treasury Department complies with the strict use limitation and stringent privacy safeguards set out in the TFTP Representations and that the TFTP has demonstrated significant value for the fight against terrorism, in particular in the EU.

The second Report highlights a number of additional mechanisms put in place by the Treasury Department during the intervening period which enhance the existing privacy safeguards surrounding the TFTP. The second Report also confirms the continuing high value of the TFTP for Europe and that U.S. authorities have continued to share TFTP-derived information with their EU counterparts - more than 100 TFTP reports were given to EU Member State authorities in 2009. The second Report includes a number of recent concrete cases where TFTP leads have proved highly valuable in investigating terrorist activity. The second Report concludes that with the level of threat from Al-Qaida inspired terrorism, highlighted by the 2009 Christmas Day incident, as well as domestic terrorism such as the Basque ETA group, it remains crucial that Member state authorities can continue to take advantage of TFTP-derived lead information

which is an important and legitimate source of reliable counter-terrorism Intelligence.

BACKGROUND

In December 2008 Judge Jean-Louis Bruguière[1] produced his first Report on the implementation by the United States Department of the Treasury of the Terrorist Finance Tracking Programme ("TFTP").[2] The purpose of that Report, as set out in the Treasury Department's "Representations" of June 2007[3], was to verify whether the Treasury Department's commitments concerning the protection of EU-originating personal data were duly respected. This necessitated an assessment of the safeguards and mechanisms designed to ensure respect for the protection of personal data. In addition and in order to be able to assess the proportionality of the TFTP, Judge Bruguière's mandate meant that it was necessary to obtain a clear understanding of the value of TFTP-derived information for the fight against terrorism in the EU and beyond.

The December 2008 Report made two principal findings; first that the Treasury Department has implemented significant and effective controls and safeguards which ensure respect for the protection of personal data consistent with the commitments set out in the Representations. Second, the Report found that the TFTP has generated significant value in particular within the EU where over 1300 TFTP-derived reports concerning documented and specific terrorist threats had been shared with Member State services at the date of the first Report. The first Report included a classified Annex setting out a number of concrete cases where TFTP-derived leads have contributed to prevent terrorist attacks in Europe and have otherwise been used to investigate and prosecute terrorism. Judge Bruguière did not find any systemic or underlying concerns to indicate that the commitments set out in the TFTP Representations were not being complied with. However, Judge Bruguière formulated several recommendations set out in the first Report which are based on areas where he believed that additional steps could be taken to solidify measures already in place.

The European Commission presented the findings of the first Report[4] to a joint meeting of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs and the Committee on Economic and Monetary Affairs on 16 February and 3 September 2009. The European Commission presented the Report to the Justice and Home Affairs Council on 26 February 2009. In addition, the Report was presented to other stakeholders including the European Data Protection Supervisor, the European Central Bank and the Article 29 Working Party[5]. The Report was further presented to a number of national authorities

[1] Judge Bruguière was designated as the "European Eminent Person" by the European Commission in April 2008. See European Commission press release of 7 March 2008 IP/08/400

[2] See European Commission press release of 17 February 2009 IP/09/264

[3] C 166/18 of 20.7.2007

[4] The December 2008 Report is classified EU SECRET. A copy of the Report was distributed to the EU 27 Permanent Representatives in June 2009 with the request that it be treated as a secret document according to appropriate national procedures. The Report was also made available to members of the European Parliament's LIBE and ECON Committees when it was presented to them in February and September 2009.

[5] The Article 29 Working Party was set up by Directive 95/46/EC on the protection of individuals with regard to the processing of personal data. Its members include a representative from the data protection supervisory

including the Belgian Data Protection Supervisory Authority, the Spanish Justice and Interior Ministries, the Spanish National Centre for Counter Terrorism, the UK Treasury, Home Office and Financial Services Authority, the German Interior and Justice Ministries and the German Central Bank. The Report was also discussed with the Chief Executive and General Counsel of SWIFT and with the London Investment Banking Association's Data Protection and Privacy Working Group, Judge Bruguière participated in all the above discussions.

Reminder of the Principal Controls and Safeguards surrounding the TFTP

The TFTP does not involve the collection of large quantities of personal data for data mining. It is designed to seek and search in a database only those leads which have an operational value in connection with existing information concerning identified and specific terrorist activity. The core undertakings set out in the TFTP Representations[6] are that:

- SWIFT data are accessed and processed exclusively for counter-terrorism purposes.[7] Any processing of SWIFT data for purposes other than the investigation, detection, prevention and / or prosecution of terrorism or its financing is strictly prohibited. Accordingly, any use of data, for example, to investigate criminal activity not connected to terrorism is not permitted. Any attempt to search the data for a purpose not connected to terrorism would be blocked by the audit process outlined below.

- The U.S. Treasury Department ensures that requests for data ("subpoenas") are narrowly focused on data necessary for the fight against terrorism. This means that the scope of the request is appropriately updated on the basis of the prevailing terrorism threat. The TFTP has now been operational for just over eight years. During that time the scope of TFTP subpoenas has been substantially reduced. The Treasury Department constantly monitors geographic threats, i.e. countries where the threat is considered particularly high, to determine the appropriate geographic focus of TFTP subpoenas.

- Searches of data held on the TFTP database can only be made where pre-existing information supports a reason to believe that there is a nexus between the subject of the search and terrorist activity or its financing. Significantly, this means that any form of data mining of TFTP data is strictly prohibited.

- Necessary measures are in place to identify and delete data which are no longer necessary for the fight against terrorism. In addition, non-extracted data received after the date of publication in the Official Journal (20 July

---

authorities of each Member State.

[6] On 30 November 2009 the Council of the European Union authorised the EU Presidency to sign on behalf of the EU an EU - US Agreement the purpose of which was to sustain the TFTP up to 31 October 2010. The Agreement contains at least equivalent safeguards to those set out in the Representations. It is notable that the safeguards set out in the Agreement are now legally binding commitments rather than a set of unilateral statements.

[7] The TFTP Representations set out a definition of terrorism which broadly corresponds to the approach set out in the Council Framework Decision on combating terrorism of 13 June 2002 (2002/475/JHA).

2007) are irrevocably deleted no later than five years from receipt.

- Physical and logical systems exist to ensure the security of subpoenaed data. To protect the data, multiple security layers exist which isolate the TFTP from other data, prohibit unauthorised access and monitor all instances of access. Significant controls also exist to ensure that no unauthorised copies of TFTP data can be made except for a set of back-up tapes for disaster recovery purposes.

- Detailed logs are kept of all searches made, including the identity of the analyst, date and time of the search, the search terms used and the justification for the search.

The above controls are subject to **independent audit by external auditors** appointed and remunerated by SWIFT. The external auditors have full access to TFTP systems and relevant personnel and have the appropriate security clearance. The tasks of the external auditors include assessing the effectiveness of the controls in order to gain assurance of the adequacy of the physical, logical and administrative security surrounding subpoenaed data as well as to ensure that the "scrutineers" (see below) have a complete view of all TFTP searches undertaken. To this effect the external auditors produce quarterly reports. These highlight any discrepancy which may impact on the ability to ensure that the data are protected and processed in a manner which takes into account the above conditions. A discrepancy will continue to be highlighted until such time as appropriate measures are taken to remedy the matter.

In addition to external audit of the TFTP, the US Treasury Department has authorised SWIFT to employ **"scrutineers"** who have access to each and every search undertaken by TFTP analysts. The role of the scrutineers, who are SWIFT employees with the appropriate security clearance, is to prevent individual queries of TFTP data from being made unless the search expressly articulates, based on pre-existing information, a reason to believe that the person who is the subject of the search has a nexus to terrorism or its financing. In order to do this, the scrutineer will verify and assess the justification for the terrorism nexus which the analyst must give as a pre-condition of performing a TFTP search. SWIFT scrutineers have round-the-clock and real-time access to the TFTP system. They have the ability to query and block individual searches and may even close down the entire TFTP system. All TFTP searches are reviewed independently by at least two SWIFT scrutineers - the majority in real-time and the remainder within 24 hours of the date of the search. In addition, SWIFT scrutineers carry out systematic random audits of searches to verify that the real-time or near real-time monitoring is effective. SWIFT internal audit reports highlight any issues which have been identified by the scrutineer during the preceding three month period.

Evolution of the TFTP

The first TFTP subpoena was served on SWIFT in October 2001. From the date of the first subpoena, SWIFT held discussions with the Treasury Department with a view to reducing the scope of subpoenas, ensuring that searches were targeted

to extract only data directly responsive to a terrorism investigation and implementing appropriate data security measures. The scope of subpoenas has been substantially reduced between October 2001 and the present day *inter alia* by assessing which message categories or types have been responsive to analysts' searches. Where over a 12 month period, a given message category or type has not been responsive, and subject to a further value assessment, data contained in that message category or type are deleted and will no longer form part of subsequent subpoenas. In 2009 a further reduction in the scope of subpoenas took place resulting in the removal of three message types and one country. Deletion of the corresponding data from the TFTP database will be completed in the course of 2010.

Since spring of 2002 the TFTP has been subject to external audit with particular focus on ensuring that the purpose limitation is strictly adhered to and that the security of the data is assured. Since early 2004 SWIFT scrutineers have been able to verify that all searches demonstrate a reason to believe that the target of the search is engaged in terrorism or its financing. Initially scrutineers were able to perform this role on the basis of paper read-outs. From early 2005 scrutineers were given 24 hour access to the TFTP system in order to monitor searches in real-time.

Since October 2001 the Treasury Department has generally served one subpoena per month on SWIFT. Where urgent or otherwise exceptional circumstances have arisen, additional subpoenas have been served during the course of any one month. In 2009 the Treasury Department served 12 subpoenas on SWIFT.

Scope of the Second Report of the Eminent European Person

The focus of this second Report on US Treasury Department implementation of the TFTP is threefold. First, the Report describes and assesses the measures taken by the Treasury Department in response to Judge Bruguière's recommendations set out in the December 2008 Report. Second, this Report considers whether new events or circumstances have come to light which impact on the protection of personal data processed pursuant to the TFTP or which may otherwise undermine the findings of the first Report that the Treasury Department is in compliance with the data protection commitments set out in the TFTP Representations. Lastly, this Report looks at whether the TFTP has continued to provide a high level of added value to the fight against terrorism, notably in Europe.

Working Methodology for second Report

Since the date of the first report Judge Bruguière has undertaken three missions to Washington in connection with the second Report. A first series of meetings took place in June 2009 with a number of high ranking officials within the new United States government. These meetings confirmed categorically that the TFTP is seen as an essential element of national and wider global security and that

commitment to the TFTP has not changed in any way since the arrival of the new U.S. government. A common theme in these discussions was that the TFTP responds to a mutual security objective which is as relevant to the EU as it is to the United States.

As with the December 2008 Report, an important focus of Judge Bruguière's work for the second Report has been to verify that robust mechanisms exist to monitor respect for the protection of personal data and that the necessary formal audit procedures carried out in respect of these data indicate a satisfactory level of compliance. For this purpose meetings took place in September and December 2009 where Judge Bruguière had discussions with the SWIFT "scrutineers" with the external and internal auditors of SWIFT, with the Privacy Officer of the Office of the Director of National intelligence who has oversight responsibility for the TFTP, with the Inspector General of the Treasury Department which exercises an autonomous oversight role within the Treasury.[8]

In January 2010 Judge Bruguière had a further series of meetings with high ranking government officials. These individuals confirmed once again the high importance attached to the TFTP by the United States government which is seen as representing an important contribution to US domestic and wider global security.

Judge Bruguière has been given access to all reporting of internal and external SWIFT auditors covering the period from December 2008 to January 2010. Judge Bruguière was also given access to detailed logs of TFTP searches made during this period including the information explaining the terrorism nexus for searches on dates randomly chosen by Judge Bruguière. In all cases this revealed pre-existing information demonstrating a reasonable belief that the person in question had a nexus to terrorism or its financing. He was further given access to detailed descriptions of the use made of TFTP-derived information in a large number of cases, some of which are summarised below.

Implementation of Recommendations contained in December 2008 Report

It is important to ensure that due attention has been given to the Recommendations contained in the first Report. Refusal or reluctance to take account of these recommendations could have indicated rigidity in the application of the TFTP Representations or unwillingness to take account of new circumstances. As highlighted below, the Treasury Department has taken necessary steps to implement the Recommendations.

The first Bruguière Report recommended that SWIFT scrutineers should endeavour to increase the volume of real-time monitoring of TFTP searches, i.e. monitoring of searches at the same moment as the search is made. In December 2008 scrutineers carried out real-time monitoring in approximately 30% of cases. As at the date of the second Report, SWIFT scrutineers estimate that they monitor in the region of 55% of all TFTP searches in real-time. The Treasury

[8] The members of the Privacy and Civil Liberties Oversight Board which also exercise oversight of the TFTP were not appointed at the time of Judge Bruguière's missions to Washington.

Department has committed to implement an enhancement to the real-time monitoring display to improve the screen view for scrutineers. This will facilitate further the ability to carry out real-time monitoring.

The December 2008 Report called for a revised version of the TFTP Training Guidelines so that these expressly confirm that no information derived from the TFTP can be disseminated until a scrutineer has verified that the search was correctly based on pre-existing information demonstrating a reason to believe that the subject of the search has a nexus to terrorism or its financing. All TFTP users have been trained to ensure there is no dissemination of TFTP information prior to completion of the scrutiny process or without management approval. Formal revision of the TFTP Training Guidelines to this effect was completed in January 2010.

The December 2008 Report called for additional training on how to make narrowly targeted searches in order to reduce as much as possible the returns from a search. All personnel with access to the TFTP underwent TFTP Guidelines training in December 2008 following release of the first Bruguière Report. Additionally, TFTP Guidelines training was conducted in early December 2009. Training to refine searches has been offered to TFTP users multiple times since the December 2008 Report was issued. Also during the course of 2009, modifications have been made to the TFTP search tool in order to reduce further the possibility of making overly broad searches.

The December 2008 Report recommended that where data are identified as no longer necessary for TFTP purposes, the process for deletion of those data should commence within two months of such identification. The Treasury Department has confirmed that following the annual statistical analysis of TFTP data, the process for deleting any information no longer necessary for the fight against terrorism will begin within two months of that determination.

The December 2008 Report recommended the documentation of appropriate responses to "scrutiny incidents", i.e. a scale of appropriate responses to searches which do not comply with strict scrutineer requirements. This could range from additional training to removing access rights to the TFTP system and disciplinary proceedings. The "Change Notification Process" agreed between the Treasury Department and the External Auditors in September 2009 documents appropriate remedies which would apply in the event of an error in carrying out a TFTP search. Potential remedies include retraining, supplemental management oversight of TFTP queries, access suspension or removal from the TFTP. The Change Notification Process states that the particular remedy is at the discretion of the Treasury Department and will take account of matters such as the user intent and the type of error.

The December 2008 Report called for measures to enhance coordination between external auditors, internal auditors and scrutineers. In 2009 the Treasury Department granted unescorted access rights to the SWIFT personnel responsible for TFTP auditing to buildings to improve interaction between SWIFT and the external auditors. This has helped facilitate SWIFT oversight of the audit process and signalled an interest in ensuring a closer and more open relationship

between the Treasury Department, the external auditors and SWIFT.

Compliance with Data Protection Safeguards set out in the TFTP Representations

On the basis of discussions with SWIFT scrutineers, SWIFT internal and external auditors and review of relevant audit reports, several items were highlighted during the course of 2009. Particular items are set out below.

- A total of 12 unrelated incidents took place in 2009. These generally involved the analyst attempting to perform a search without presenting sufficient justification for the terrorism nexus. In some cases the analyst self-reported the incident on realising a mistake had been made. In other cases the incident was identified by the scrutineers. Significantly none of these cases resulted in the dissemination of any information beyond the analyst. In all cases measures were taken to avoid any recurrence. These included additional training, counselling and, if warranted, suspension of the analyst from the TFTP system.

- The TFTP Guidelines require all TFTP analysts to attend a TFTP training programme prior to authorised access to the TFTP and to attend annual refresher training on the TFTP Guidelines[9]. Attendance at such training must be duly documented. In the first part of 2009 the external auditors requested evidence to show that all TFTP analysts had received mandatory training as well as mandatory refresher training. Access to these data is necessary to verify that in all cases mandatory training requirements have been met. It is also necessary to determine whether any user accounts have been or need to be deactivated due to out of date training. Training records were provided to the external auditors in the second semester of 2009. Comparison of these records with training requirements showed no discrepancies. Moreover, accounts which had been locked where training requirements had not been met in the previous year remained locked.

- In September 2009 the Treasury Department adopted the "Change Notification Process" - a documented set of procedures to notify the external auditors of important changes to the operation of the TFTP including changes in hardware or software used. The purpose of the new process is to avoid any possibility that non-notified changes take place which could impact the ability of the auditors to obtain assurances regarding the security, scope and scrutiny of TFTP data. To avoid any risk that significant changes are not pre-notified to the external auditors due to human error, the auditors have recommended that the above controls are supplemented by additional technology-based detection measures to monitor and log network activity. The Treasury Department has committed to procure such a tool and an appropriate technical solution has been identified.

[9] As explained in the first Bruguiere Report the TFTP Guidelines set out the main components of the TFTP which all TFTP analysts must at all times comply with. They include the need to ensure that all searches of the TFTP database are based upon a reason to believe that relevant persons have a connection to terrorism, the obligation expressly to articulate that belief before carrying out the search and the obligation to maintain a detailed log of any search activity.

- Following queries raised by the external auditors concerning the possibility that persons without authorisation to access the TFTP system might gain access to the TFTP Analysis Room, additional measures were taken to ensure that no access is possible except for program managers, analysts read into the TFTP system and security guards. The list of persons with Badge access to the Analysis Room was audited confirming that only those appropriately authorised to work on the TFTP have access to the Analysis Room.

Value of TFTP-derived Information in the fight against terrorism

On the basis of information provided, Judge Bruguière is able to confirm that during 2009 the TFTP has been a highly valuable tool used by intelligence and law enforcement agencies to help map out terrorist networks, to complete missing links in investigations, to confirm the identity of suspects, to locate the physical whereabouts of suspects and to identify new suspects as well as to disrupt attempted terrorist attacks.

Europol is of the opinion that the agreement provides an excellent opportunity to further enhance the cooperation for counter-terrorism purposes. Based on the preliminary exchange of views with the U.S. Treasury Department's Office of Foreign Assets Control, Europol is confident of being able to fully implement the agreement.

The TFTP has continued to demonstrate its value for US and EU counter-terrorism efforts. In total, more than 1550 TFTP-generated reports have been passed to European governments, over 100 of those TFTP reports have been provided in 2009. Additionally, 800 TFTP reports have been passed to non-European governments since 2001. To protect the original source of the information, the receiving government typically has not known that the information is derived from the TFTP.

Significant Examples of TFTP Information Sharing

TFTP information provided substantial information to European governments during the 2006 investigation into the Al-Qaida-directed plot to attack transatlantic airline flights between the UK and US. TFTP information provided new leads, corroborated identities, and revealed relationships among individuals responsible for this terrorist plot. In mid-September 2009, three individuals were convicted and each was sentenced to at least thirty years in prison.

In summer 2007, the TFTP was used to identify financial activity and additional information on Germany-based Islamic Jihad Union (IJU) members. This information contributed to the investigation of IJU members plotting to attack sites in Germany. The TFTP also provided additional information to Germany following the arrests to support the ongoing investigation. More specifically:

- TFTP information identified financial transactions of an arrested IJU suspect and other bank account information connected to him, including the suspect's accounts in foreign countries—this information was provided to the German government prior to the suspect's arrest. The suspect later confessed to being a member of the IJU.

- TFTP information identified financial transactions that a second arrested suspect had with individuals in foreign countries—this information was provided to the German government prior to the suspect's arrest. The suspect later confessed to being a member of the IJU.

In January 2009, the USG conducted research on a US-based individual for having contact with a known Al- Qaeda member. Further Investigation determined additional US-based individuals were conspiring with the first person to conduct a terrorist attack in the United States. Additionally, the individuals were in contact with a suspected Al-Qaida operative residing in Denmark, TFTP research connected the US-based individuals to multiple overseas subjects, who had connections to terrorist organizations. TFTP research showed the flow of money to and from the three US-based individuals. TFTP data contained important information that provided leads and helped produce new lines of investigation. European partners also used the information to assist in their own investigations.

In October 2008, eight Spain-based individuals were arrested for their suspected involvement with Al-Qaida. The cell provided fundraising, training, and weapons to suspected terrorists. Furthermore, this group sent trained individuals to fight Coalition Forces in Iraq, investigation revealed the subjects may have assisted in the escape of the Madrid Railway bombers who coordinated the March 11, 2004, attack. The subjects also had contact with other Al-Qaida affiliates outside of Iraq. European partners provided information outlining the connection to terrorism for the individuals arrested. The resulting report outlined connections between the targets and other individuals in Spain, Morocco, and the Netherlands. Information was provided to European governments to aid in their own investigations.

Historical TFTP Value Examples

The TFTP has provided useful information on terrorists connected to significant attacks. Generally, TFTP information has provided leads, corroborated information, and revealed relationships of terrorists responsible for these attacks. Some examples include:

November 2008 Mumbai Attack
Following the attack the USG provided information about members of the attack.

January 2008 Barcelona Arrests
TFTP information was used to identify the connections of the Spain-based network with connections to Asia, Africa, and North America.

Summer 2007 German IJU Arrests
The USG surged analysis to investigate this threat and this information contributed to the investigation of the IJU network in Germany.

June 2007 JFK Airport Plot
TFTP information identified the specific financiers of the plot and revealed the scope of the network.

2006 Transatlantic Liquid Bomb Plot
TFTP information provided information which assisted in the investigation and conviction of individuals responsible for this attempted attack.

2005 London "7/7" Bombings
TFTP information provided new leads, corroborated identities, and revealed relationships among individuals responsible for this terrorist plot.

April 2005 Van Gogh Murder Investigation
TFTP information revealed that the attacker had connections to individuals with global terrorism connections.

2004 Madrid Train Bombings
TFTP information was provided to multiple European countries to assist in the investigation that followed this attack.

October 2002 Bali Bombings
TFTP information played an important role in the investigation that followed the 2002 bombings in Bali and this investigation culminated in the capture of Hambali, Jemaah Islamiyya's Operations Chief.

Following the attack in Mumbai, the TFTP identified information about several suspected and/or involved high ranking Lashkar-e-Tayyiba (LeT) members with relationships to individuals and institutions in the US and Europe. The TFTP data contributed to the global investigation into the attacks and the leads associated with this investigation were passed to the appropriate governments.

Searches of TFTP data uncovered financial data on an individual identified as the Indonesian financial conduit for Jemaah Islamtyah's July 17, 2009, Jakarta hotel bombings that killed nine people, revealing direct financial connections to Gulf-based donors. This information was shared with Asian and Middle Eastern governments.

In response to an INTERPOL Security Alert issued on 10 February 2009, TFTP research was conducted on 85 terrorists wanted by the Saudi Arabian government for having links to Al-Qaida in Saudi Arabia, Iraq, and Afghanistan. Reporting uncovered the aliases, name variations, and financial networks of at least nine of those individuals. At least one individual may have financial contacts in multiple European countries; others have contacts in the Middle East and Asia, especially Indonesia.

In early 2009, TFTP was used to identify activity of an individual with links to Al-Qaida who was based in a northern European country and who played a role in planning an attack on aircraft. The information was passed to the governments of European and Middle Eastern nations.

In 2009, TFTP has been used to support an investigation into Lashkar e-Tayyiba (LeT) funding networks in the Middle East, Australia, and South Asia. TFTP lead information was provided to the government of a country where a significant LeT fundraiser was based.

In late 2008, TFTP was used to identify relationships associated with senior members of a South Asian Al-Qaida affiliated terrorist group. The TFTP data was shared with a foreign Government.

As recently as mid-2009, the TFTP has identified information on Basque Fatherland and Liberty (ETA) members. This information was provided to European governments.

TFTP: A Vital Counterterrorism Tool

As recent events have demonstrated, terrorism continues to threaten global peace and security. Attempted terrorist attacks, like the recent failed destruction of an aircraft travelling from the Netherlands to Detroit on Christmas Day 2009, underscores the continued importance and relevance of counterterrorism tools like the TFTP.

CONCLUSIONS

This is the second and final Bruguière Report on the Terrorist Finance Tracking Programme. Over the last 24 months. Judge Bruguière has been given unprecedented access to TFTP systems, search logs, and audit reports. Judge Bruguière has interviewed those responsible for the oversight and management of the TFTP. He has discussed the search mechanics of the TFTP with analysts authorised to access the TFTP database. He has considered the importance and value of the TFTP with political and senior appointees of both the previous and current U.S. Administrations. He has spent considerable time with both SWIFT external and internal auditors who aim to ensure protection and security of subpoenaed data. As a result of this work, Judge Bruguière has arrived at the conclusion that the safeguards and mechanisms surrounding the TFTP and addressing data privacy issues are of an exceptionally high standard. In particular, the full and complete access to the TFTP system which has been granted to SWIFT and its external auditors has been highly effective, Four scrutineers have verified that TFTP searches demonstrate an appropriate nexus to terrorism and are not such as to generate overly broad search results.

Judge Bruguière has been given detailed information on the value which TFTF-derived information has generated for the fight against terrorism in Europe and beyond. As the events of 25 December 2009 clearly demonstrate, the level of threat represented by Al-Qaida inspired terrorist groups remains high including within Europe. This disparate and constantly evolving danger can only be addressed by effective and lawfully derived intelligence. At the same time the challenge faced by counter-terrorism analysts is immense - fragments of often contradictory information which need to be pieced together to identify threats and prevent attacks. In this context the TFTP must be seen as an important and highly valuable source of reliable information which has provided police and other services with significant intelligence for the fight against terrorism. Judge Bruguière is of the view that the continuation of the TFTP, surrounded as it is by significant data protection safeguards, is in the interests of Europe and of European citizens.