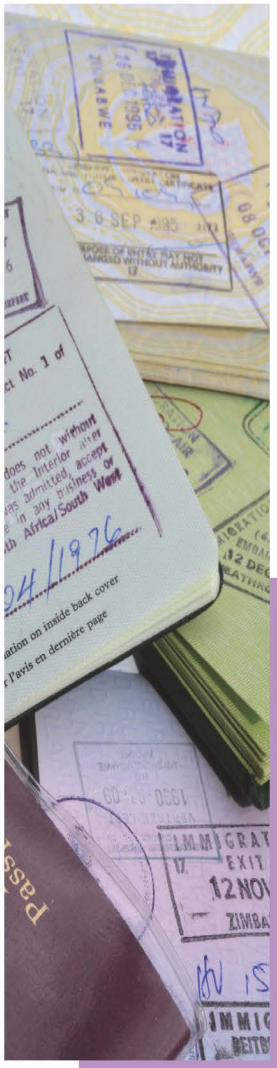
EUROPEAN PARLIAMENT

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS



Constitutional Affairs

Justice, Freedom and Security

Gender Equality

Legal and Parliamentary Affairs

Petitions

Evaluation of EU measures to combat terrorism financing

In-depth analysis for the LIBE Committee

EN

2014

EUROPEAN PARLIAMENT

DIRECTORATE GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C: CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS

Evaluation of EU measures to combat terrorist financing

IN-DEPTH ANALYSIS

Abstract

Upon request by the LIBE Committee, this note evaluates the EU's measures to combat terrorist financing and their societal and political impact. In response to the renewed politicization of the EU-US Terrorist Finance Tracking Programme (TFTP) and taking into account that the European Commission has announced in November 2013 its intention not to present at this stage a proposal for a European Terrorist Finance Tracking System (EU TFTS), and in the light of the development of a 4th Directive on anti-money laundering and combatting terrorist financing (AML/CFT Directive), the note proposes a set of recommendations concerning possible measures to combat terrorist financing.

PE509.978 EN

DOCUMENT REQUESTED BY THE
COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS (LIBE)

AUTHORS

Dr. Mara WESSELING
(Centre de Sociologie des Organisations, Sciences-Po Paris/CNRS)

Foreword by: Prof. Dr. Marieke DE GOEDE
(Universiteit van Amsterdam)

RESPONSIBLE ADMINISTRATOR

Mr Alessandro DAVOLI
Policy Department Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
E-mail: poldep-citizens@ep.europa.eu

LINGUISTIC VERSIONS

Original: EN

ABOUT THE EDITOR

Policy Departments provide in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact the Policy Department or to subscribe to its monthly newsletter please write to:
poldep-citizens@ep.europa.eu

European Parliament, manuscript completed in April 2014.

This document is available on the Internet at:
http://www.europarl.europa.eu/studies

DISCLAIMER

CONTENTS

LIST OF TABLES

EXECUTIVE SUMMARY

This note provides the LIBE Committee with background information and a set of recommendations concerning the EU measures to combat terrorist financing. The analysis in particular considers the Third Directive on anti-money laundering and combatting terrorist financing (**Third AML/CFT Directive**), the EU-US Terrorist Finance Tracking Programme (**TFTP**) and the European Terrorist Finance Tracking System (**EU TFTS**).

The note emphasizes that **more critical scrutiny** is **needed** regarding the fight against terrorism financing. It is time to recognise that the pursuit of terrorism financing has side effects with profound implications and that the preventative effects of this fight are not clearly proven.

The **first section** presents an **overview of the EU's main instruments for combating terrorism financing**, placing the Third AML/CFT Directive and the TFTP in a broader framework to combat terrorism financing. This part of the briefing also brings back into memory the specific policy contexts in which these measures were created and how they evolved. The note shows that the risk-based practices of the Third Directive have a far-reaching scope touching on the daily financial transactions of virtually all European citizens (1.2). The historical study of the TFTP recalls the multiple controversies surrounding the programme before and after the adoption of the EU-US TFTP. It also draws attention to a number of fundamental questions that have not been thoroughly discussed so far (1.3). The last part of this section discusses the EU TFTS and recalls the key arguments for developing this initiative (1.4).

The **second section** provides **an analysis of the Third AML/CFT Directive, the TFTP and the EU TFTS and identifies a number of weaknesses of these instruments**. It shows that, despite increased reporting, the effectiveness of both the Third Directive and the TFTP in the fight against terrorism financing is insufficiently proven and even appears controversial. Moreover, the implications of the methods of data analysis and their consequences are insufficiently known. Yet, this briefing argues that

- the searches made within the TFTP are not targeted but potentially exponential;
- they might lead to wrongful criminalisation by association;
- maintaining the 'status quo' instead of developing an EU TFTS is not a satisfying response.

Finally, in the **third section** some possible **initiatives and recommendations** are developed in order to contribute to future debates and to improve future EU initiatives.

FOREWORD

Since 2001, and in direct relation to the attacks of 9/11, the pursuit of terrorist and suspect money has gained momentum in regulatory systems and policing practices across the globe. It has become a commonplace to assert that 'money trails don't lie' and that financial data offer unprecedented access to suspects' networks, locations and activities. Though not entirely free from political controversy, the pursuit of terrorism financing has largely remained, as this report points out, the 'war the no-one sees.'

Yet it is time to hold the fight against terrorism financing up to more critical scrutiny. Important questions concerning this seemingly technical way of pursuing potential suspects remain unanswered. These questions include not just our understanding of financial privacy, but also practical questions concerning effectiveness, foreseeability of regulatory impact, and accountability of security interventions enabled through this agenda.

A key concern is that of financial privacy. If perhaps account information and financial transaction records offer unprecedented insight into a person's movements and networks, it also contains sensitive information on an individual's daily life. Important life events such as weddings, funerals or moving house are often accompanied by significant financial transactions. As the use of debit card payments is becoming more commonplace – instead of bulk cash withdrawals – financial transaction information entails ever more minute insight into an account holder's preferences and patterns. If click-stream data build a record of one's interests, financial data show what one actually spends money on. This does not go unrecognised by banks themselves: Dutch bank ING has recently launched a plan to share financial transaction data with commercial parties for a fee. ING's plan caused quite some debate in The Netherlands, and illustrates the necessity for a European-wide discussion on the nature of financial privacy. Unlike with (many) social media, citizens cannot choose to disengage from the financial system. One simply cannot opt out of having a bank account in modern life. This special position of the banking system in citizens' daily lives has to translate into special responsibilities when it comes to safeguarding clients' privacy. This is not just a matter of individual privacy, but also of fostering the conditions of a democratic society.

Furthermore, as discussed in this report, the effectiveness of measures to combat terrorism financing remains disputed. A commonplace complaint from the banking industry is that their substantial investments into compliance departments is not matched by government feedback on the usefulness of their reports in actual criminal investigations. Similarly, though the recent EU-US review report on the Terrorism Financing Tracking Programme (TFTP) describes a number of important case examples, too little is publicly know concerning the way the TFTP has actually worked to help arrest suspects and bring them to justice. As this report shows, the use of financial data within this programme is not fully targeted but potentially exponential.

Other questions relate to the transparency, accountability and foreseeability concerning the identification of suspicious transactions and the freezing of funds. Under the risk-based approach, banks have come to play an important independent role in the work of security. Not all banks implements the requirements in the same way, which raises questions of forseeability for banking clients.

It is time to recognise that the pursuit of terrorism financing does have side effects. It is not at all clear that it has the preventative effects that form the basis of its rationale. In the case of charitable money flows and remittance-dependent families, a financial lifeline can be a matter of life-and-death. Current discussions in the UK concerning Barclay's intention to cease working with a leading Somali financial network underscore the importance of remittances to war-torn areas. Decisions to close accounts or freeze financial flows should be made with the utmost responsibility and accountability. This report contributes to generating debate on the side effects of financial warfare, and to reopening questions on fundamental rights in relation to this important security domain.

Prof. dr. Marieke de Goede,
University of Amsterdam

INTRODUCTION

Background

This note provides the LIBE Committee with an evaluation of the EU measures to combat terrorist financing and looks at possible measures and initiatives to combat terrorism financing, including but not limited to a "European Terrorist Finance Tracking System" (EU TFTS), while also considering the impact on fundamental rights.

Two separate sets of developments concerning the EU's two main instruments to combat terrorism financing inform the request for this evaluation. First, a renewed phase of politicization of the Terrorist Finance Tracking Programme (TFTP) took place due to the revelations from 5 June 2013 onwards in media outlets worldwide on numerous NSA spying programs. These revelations led to the adoption of the **European Parliament's resolution of 4 July 2013** which suggested the possible suspension of the PNR and TFTP agreements with the US in order to obtain full information on ongoing surveillance programmes and the suspension or revision of any laws and surveillance programmes that might be violating the fundamental right of EU citizens to privacy and data protection, the sovereignty and jurisdiction of the EU and its Member States, and the Convention on Cybercrime.[1]

A second and firmer call for the suspension of the TFTP agreement was voiced by several MEPs from 9 September 2013 onwards, when amongst others the Brasilian channel *Globo TV*, *Der Spiegel* and the *Washington Post* revealed that the NSA was also involved in the surveillance of SWIFT.[2] A written exchange between Cecilia Malmström, European Commissioner for Home Affairs and David Cohen, Under-Secretary of the US Department of the Treasury for Terrorism and Financial Intelligence, followed between 12 and 18 September and led to the start of consultations and an inquiry by the European Commission into this matter. On 24 September, Malmstrom stated before the EP's LIBE committee that if the press reports are true, then it could 'constitute a breach of the agreement and a breach of the agreement can certainly lead to a suspension"'[3]. Yet, in following declarations the European Commissioner expressed her belief that the NSA has not had access to the SWIFT data. Deeming the new revelations a breach of the EU-US TFTP agreement, the European Parliament called for its suspension in its **resolution of 23 October 2013**.

The recommendation for suspending the EU-US TFTP was reiterated in the EP report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (known as **the Moraes report**) published on 21 February 2014 and in a resolution taken by the European Parliament on 12 March 2014.

Moreover, on 27 November 2013, the European Commission published Joint Reviews on the processing and transfer of Passenger Name Records, on the value of TFTP provided data, on the functioning of Safe Harbour, and a **communication on the European Terrorist Finance Tracking System (EU TFTS)**. The notable conclusion of this communication was

[1] EP resolution of 4 July 2013, P7_TA(2013)0322.
[2] See for instance: '*MEPs call for suspension of EU-US finance tracking deal*', EU-Observer, 10 September 2013, http://euobserver.com/justice/121373.
[3] EP Press Release 24 September 2013, MEPs raise suspension of EU-US bank data deal.

that 'the case to present at this stage a proposal for an EU TFTS is not clearly demonstrated'.[4]

A second set of developments concerns the adoption of a **Fourth AML/CFT Directive**. For this purpose the European Commission has prepared a proposal published on 5 February 2013. At the time of writing this briefing note, the proposal has been adopted with amendments by European Parliament on 11 March 2014 and is currently under review of the Council.

Terrorism financing as a 'core component' in the war on terror

This briefing provides background information on the EU framework for combating terrorism financing and especially evaluates the two main instruments in this domain, the EU's Third AML/CFT Directive and the TFTP. However, before going into detail, it is important to place the current CFT instruments within a broader discussion on the fight against terrorism and to recall the origins, design and purposes of the financial measures adopted in the European fight against terrorism financing.

The interest for pursuing terrorist money did not arise from the events of 9/11. From the mid-1980s, the conception of terrorism was progressively and actively reframed and became understood as a crime rather than a political struggle through violent means. Although still considered as a relatively marginal issue, the fight against terrorism financing was given substance in the 1990s via UN economic sanctions against, first, a number of countries suspected of sponsoring terrorism followed by designated entities and individuals. The 1999 UN Convention for the suppression of terrorism financing led to a broadening of the definition and a criminalisation of terrorism financing. In the same period, combating terrorism financing became also part of the follow-the-money strategies against drug traffickers and organised crime. **Current CFT measures still embody these dual origins of freezing assets on one hand and monitoring and tracing money trails on the other**.

What changed after 9/11 was, first, the political urgency and importance given to measures to combat terrorism financing. Considerations that were more important prior to 9/11 – the deregulation of financial markets, respect for civil liberties, on-going discussions over the insignificance of the amounts of money involved in terrorism and the (in)effectiveness of international sanctions, combined with the absence of major terrorist attacks – were suddenly overshadowed. Second, given the political momentum and the technical possibilities, the adoption of financial surveillance measures based on massive amounts of financial data from the modern banking and credit industries, 'smart' software, public-private cooperation and the promise of prevention, became acceptable.

Immediately after 9/11 combating terrorism financing became a 'core component'[5] of the international and European efforts to combat terrorism and its financing. The first public reactions of EU representatives immediately stated that both terrorists *and their financiers* must be targeted to make an end to terrorism. The investigation of financial flows and banking data is believed to be a powerful tool for tracking mobile suspects, providing

[4] European Commission, Communication from the Commission to the European Parliament and the Council, A European terrorist finance tracking system (EU TFTS), COM(2013) 842, 27 November 2013.
[5] See for instance: webpage of the European Commission, available at: http://ec.europa.eu/home-affairs/policies/terrorism/terrorism_financing_en.htm, last accessed on 23 March 2014.

reliable information compared to other forms of intelligence, uncovering identities and locations, providing insights in networks before terrorist acts are committed.

It is intriguing to note that, despite its centrality in and unlike the military operations carried out in name of the War on Terror, the tracing of terrorist monies can be described as **"a war that no one saw"**[6], fought through financial data and computer systems. Yet, academic research and media reporting have shown that although largely unseen, the measures for combating terrorism financing have **profound political and societal implications and made real victims**.

Structure and scope

The fight against terrorism financing has been a rather uncontroversial aspect of the international fight against terrorism. Although the EU-US TFTP has led to years of heated debates and the successive AML/CFT Directives were adopted only after thorough legal discussions, the effectiveness of the 'follow the money' logic for combating terrorism has often been assumed as proven.

This note aims to evaluate the EU's measures against terrorism financing with regard to their effectiveness and their impact on citizen's fundamental rights but also considers its broader political and societal implications. It will first give a short overview of the EU's legal framework and in particular the current state of play regarding the Third AML/CFT Directive, the TFTP and connected to this the EU TFTS. The second section will provide an analysis of these measures and identifies a number of their weaknesses. It especially focusses on the consequences inherent to the methodologies on which these measures are based, i.e. risk-based analysis and social network or link analysis. Finally the last section will provide a set of possible initiatives and recommendations for the European Parliament.

[6] Qualification used by The Washington Post (2011), *Profile: Stuart A. Levey*, Who Runs Government Website, http://www.washingtonpost.com/politics/stuart-a-levey/gIQAeUm69O_topic.html, last accessed 29 March 2014.

1. OVERVIEW OF THE EU'S MAIN INSTRUMENTS FOR COMBATING TERRORISM FINANCING

KEY FINDINGS

- Compared to the TFTP, the 3rd AML/CFT Directive has proved to be a less controversial instrument for financial surveillance. Yet it has a **discrete but far-reaching scope**, touching on the daily financial transactions of virtually all European citizens.
- Despite their high political saliency, the discussions on the TFTP held between 2006 and 2010 in the EU became quickly narrowed down to two main issues: privacy and data protection. **The NSA spying revelations bring a number of fundamental but seemingly forgotten questions with regard to the TFTP back into the debate.**
- The **key arguments for a developing an EU TFTS were to avoid the transfer of European financial data in bulk to the US**, to enhance control over European security decisions and the analytical and filtering processes of the programme and the guarantee of data protection and privacy guarantees in full accordance with EU legislation.

1.1. The European framework to combat terrorism financing

The current European CFT measures are mainly based on the nine special recommendations of the Financial Action Task Force (FATF), an informal platform consisting of a group of OECD states (see table 1.1). These recommendations require states worldwide to regulate all sorts of financial transactions in order 'to detect, prevent and suppress the financing of terrorism and terrorist acts'.[7] The guidelines are comprehensive in the sense that they incorporate all relevant UN Conventions and resolutions and involve a wide scope of professionals in the efforts to inhibit terrorism financing.

Table 1: FATF Special Recommendations

I.	Ratification and implementation of UN instruments
II.	Criminalising the financing of terrorism and associated money laundering
III.	Freezing and confiscating terrorist assets
IV.	Reporting suspicious transactions related to terrorism
V.	International co-operation
VI.	Alternative remittance
VII.	Wire transfers
VIII.	Non-profit organisations
IX.	Cash couriers

Source: www.fatf-gafi.org

[7] FATF (2001), *FATF Pledges to Combat the Financing of Terrorists*.

The EU has transposed the FATF's Special Recommendations into EU law by adopting a number of Directives and Regulations (see table 1.2). In the weeks following 9/11, the freezing and seizing of funds and financial assets on the basis of UN Security Council Resolutions (UNSCR) 1267 (1999) and 1373 (2001) were most prominent actions. These resolutions required the blacklisting of individuals and groups suspected of terrorism, in particular Osama Bin Laden, the Al Qaeda network and the Taliban. The purpose of these economic sanctions was to reduce the flow of funds to terrorists and to disrupt their activities. Moreover, according to the Council of the European Union, the listing procedures give an important political sign and have a deterrent psychological impact.[8] However, the practices of blacklisting have also raised controversy, as they were at first not compatible with certain fundamental rights, such as the lack of democratic and judicial oversight by the European Parliament and the European Court of Justice and the presumption of innocence.[9]

Table 2: Overview of the EU's legal framework and the corresponding FATF Special Recommendations

EU CFT Legislation	FATF Special Recommendations to combat terrorism financing
Regulation (EC) 2580/2001 freezing funds of suspected terrorists Common Position 2001/931/CFSP	SR I: Ratification and implementation of UN instruments SR III: Freezing and confiscating terrorist assets
Regulation (EC) 881/2002 implementing UN Al Qaeda and Taliban sanctions	SR I: Ratification and implementation of UN instruments SR III: Freezing and confiscating terrorist assets
Third Directive on the prevention of the use of the financial system against money laundering and combating the financing of terrorism (2005/60/EC)	SR I: Ratification and implementation of UN instruments SR II: Criminalising the financing of terrorism SR III: Freezing and confiscating terrorist assets SR IV: Reporting suspicious transactions related to terrorism SR V: International co-operation SR VI: Alternative remittance SR VII: Wire Transfers
Regulation Controlling Cash Entering or Leaving the Community (EC) No 1889/2005	SR IX: Cash couriers
Regulation (EC) No 1781/2006 on information on the Payer Accompanying Transfers of Funds	SR VII: Wire transfers
Directive 2007/64/EC on payment services in the internal market, *i.e.* 'Payment Services Directive'.	SR VI: Alternative remittance.

Source: Wesseling, 2013

Surrounded by far less media attention than the economic sanctions, the other FATF guidelines required more negotiation and were transposed in the years after 9/11. These measures attempt to regulate the financial sector and track financial transactions. Seven of

[8] Council of the European Union (2004), *The Fight against Terrorist Financing*, Doc. 16089/04, 14 December 2004, p.3.
[9] See for instance: Amicelle & Favarel-Garrigues, (2009); Bulterman, (2005); de Goede (2012), Guild (2008), (2010); Tappeiner, (2005); Vlcek, (2005), Wesseling (2013), (full details in references section).

the nine Special Recommendations are addressed in the Directive on the Prevention of the Use of the Financial System against Money Laundering and Combating the Financing of Terrorism (2005/60/EC). Special Recommendations VII and IX have been transposed separately into EU law in the form of the Regulation Controlling Cash Entering or Leaving the Community (EC) No 1889/2005 and Regulation (EC) No 1781/2006 on information on the Payer Accompanying Transfers of Funds. Additional action with regard to alternative remittance services (FATF SR VI) was taken through the adoption of Directive 2007/64/EC, the so-called 'Payment Services Directive'.

In 2004, the European Union has designed a specific Strategy on Terrorist Financing which was revised in 2008 and 2011. The EU's 2004 Strategy on Terrorism Financing explains that the two approaches for combating terrorism financing (freezing financial assets on the one hand and tracking transactions on the other) 'are not mutually exclusive'.[10] Depending on the specific situation, governments may consider it more useful not to publicly designate a terrorist (group) but silently to track their financial transactions in order to obtain more insights in their activities. After an initial wave of designations in the wake of 9/11, the emphasis of the European efforts against terrorism financing has shifted increasingly to tracking terrorist transactions. The two most important elements in this context are the Third Directive on the prevention of the use of the financial system against money laundering, and combating the financing of terrorism, adopted in 2005, and the Terrorism Finance Tracking Programme (TFTP).

The Third Directive is the most comprehensive EU measure to fight terrorism financing with a broad impact on daily financial lives of citizens and mundane transactions. It obliges professionals of regulated entities to increase surveillance on their clients and the accounts they may hold. Through enhanced 'Know Your Customer' (KYC) and due diligence requirements, regulated professions have to establish the identity of their client, to record and analyse their financial transactions and to report any suspicious transaction to a national Financial Intelligence Unit (FIU). The Third Directive is a salient example of large-scale public-private security cooperation and an important but rather discrete example of the data- or intelligence-led fight against terrorism.

The Terrorist Finance Tracking Program (TFTP) was initially a secret American intelligence programme and was not designed as a European instrument for combating terrorism financing. Created shortly after 9/11, the programme consisted of gathering and analysing financial transaction data from the SWIFT financial messaging system in order to detect terrorist plots and trace potential terrorists and terrorism financiers. Although the EU was not involved in the development of the TFTP, the EU has worked towards the conclusion of a long-term agreement on the transfer since the revelation of the programme. In fact, the EU Member States are said to be greatly benefitting from TFTP information that is spontaneously send by U.S. authorities and with the adoption of the 2010 EU-US TFTP Agreement the EU Member States are entitled to submit their research requests to the U.S. authorities. Therefore, the programme – described as a 'powerful tool' for both American and EU law-enforcement authorities[11] - must today be considered as an integral part of the EU framework for combating the financing of terrorism. In addition, one of the conditions of the European Parliament to consent with the 2010 EU-US TFTP Agreement was the development of a European equivalent of the programme (article 11), baptised European Terrorism Financing Tracking System (TFTS).

[10] Council of the European Union (2004), see note 8, p. 3
[11] http://ec.europa.eu/home-affairs/policies/terrorism/terrorism_tftp_en.htm, last accessed on 24 February 2013.

The following three sections will provide a short overview highlighting the main features of the Third AML/CFT Directive, the TFTP and the TFTS.

1.2. The Third AML/CFT Directive

In 2005 the European Union adopted the Third Directive on the prevention of the Use of the Financial System for the Purpose of Money Laundering and Combating Terrorism Financing (2005/60/EEC) (henceforth the Third Directive) as a response to the Special Recommendations on terrorism financing compiled by the FATF shortly after 9/11 and revised in 2003.

The Third Directive is a **'preventive effort'** to combat terrorism via the financial system and has three proclaimed objectives with regard to combating terrorism financing. Posing monitoring and control duties on a range of regulated entities[12] should lead to:

- the identification of clients and the monitoring of their transaction data in order to detect terrorists and their associates before they strike,
- the disruption of terrorist plots by denying (alleged) terrorists access to their funding and thereby limiting their access to money,
- enhancing the stability and the reputation of, and the confidence in the financial system by repressing the transfer of legally or illegally obtained money for terrorist purposes through the financial system.[13]

Compared to the two previous AML Directives (91/308/EEC and 02001/97/EC), the Third Directive represents a qualitative shift in purpose in that it **explicitly includes the fight against terrorism financing** and it **introduces a risk-based approach** to replace the existing rule-based approach.

The extension of the Directive to include terrorism financing was seen as a logical step after 9/11 as terrorism financing often involves international transactions, cash transactions, criminal or clean money, and may also concern service providers outside the financial sector. Its inclusion in the EU's AML framework evidences the importance of anti-money laundering legislation as a key component in the international efforts to combat terrorism financing.

The shift from a rule-based approach to a **risk-based approach** was another significant change. It implies that instead of the application of a set of fixed norms to every transaction as required in the First and Second AML Directive, a risk-based approach is more flexible. It aims to differentiate between high and low risk customers and transactions allocating resources more efficiently to the most risky categories. Moreover, risks are evaluated according to changing terrorism financing trends and profiles which has the advantage that criminals cannot adapt their behaviour to avoid attracting attentions to their transactions. Finally, through risk-based software transactions are monitored continuously and therefore unusual or suspicious transactions are flagged almost instantly.

[12] These are: credit institutions, financial institutions, insurance companies, auditors, real estate agents, notaries and independent legal professionals (under certain conditions), dealers in high value goods or legal persons trading in goods worth EUR 15.000, casinos, trust or company service providers.
[13] EU (2005), Third Directive on the prevention of the Use of the Financial System for the Purpose of Money Laundering and Combating Terrorism Financing (2005/60/EEC), p.15.

In practice, the Third Directive requires regulated entities (mainly the banking and financial services sectors) to store and monitor their clients' data and to make risk-assessments to detect suspicious transactions. This means that designated entities are required to identify the identity and **monitor all transactions of all their clients**, in a risk-based manner. Compared to the TFTP, which mainly deals with international money transfers, it must therefore be highlighted that the Third Directive implies a much wider scope of transactions and involves virtually all Europeans.

Similar to the Second and Third Directive, the proposal for a Fourth AML/CFT Directive, is justified as a response to 'the changing nature of money laundering and terrorist financing threats, facilitated by a constant evolution of technology and of the means at the disposal of criminals'. It proposes a broadening of the group of regulated entities by including gambling services and dealers in goods with a threshold of EUR 7500 (instead of EUR 15.000), a clarification of the notion beneficial ownership and changes in the provisions on sanctions. More fundamentally it maintains and further elaborates the risk-based approach to combating terrorism financing. The second part of this note proposes a set of reflections on the CFT aspects of the Third Directive.

1.3. The EU-US Terrorist Finance Tracking Programme

On 23 June 2006 the *New York Times*, followed by media world-wide disclosed the Terrorist Finance Tracking Programme (TFTP), a secret programme initiated by the CIA rapidly after the 9/11 terrorist attacks and overseen by the US Treasury Department's Office of Foreign Asset Control (OFAC). This programme involved the analysis of millions of banking transactions worldwide through access to the financial records stored in the database of a Belgian cooperative called Society for Worldwide Interbank Financial Telecommunication (SWIFT). A large part of the transferred SWIFT data concerned transactions from or to bank accounts in one of the EU member states.

The revelation of the TFTP provoked a yearlong controversy between the EU and the US and within the EU, in which all EU institutions were greatly involved. The European Parliament took a major and persisting interest in the TFTP. Between its revelation in June 2006 and the conclusion of a EU US TFTP in the summer of 2010, heated debates have taken place in the European Parliament, and successive (interim) agreements and solutions to continue the programme have been prepared by the European Commission and the Council.

An analysis of the debates of the European Parliament in the weeks after the disclosure of the TFTP shows that a variety of aspects related to the programme raised concern. These include important questions on the legality of the programme and the compatibility of the TFTP with European privacy and data protection legislation, which have been extensively discussed in the years following the disclosure of the programme. Yet, MEPs were also worried about issues that rapidly seemed to be forgotten. These included the **value of the transatlantic partnership** and **the US record on respecting international agreements** under the Bush administration. They highlighted the conflict between the initially secret programme and the **aim of transparency towards citizens**. They wanted **proof of the effectiveness** of the programme in combating terrorism and of its limitation to terrorism investigations. In addition they feared the possibility of the use of SWIFT data for **industrial spying**. More generally, they called for a need to have a thorough discussion on the **nature of the War on Terror** and the **desirability of Orwellian practices** – referring to the collection and analysis of massive amounts of personal data – as one of its

main weapons. It is important to bring back these political questions into the debate. Some recent reports and debates show already a renewed interest for these insufficiently debated but important political and societal questions in response to the revelations on the NSA spying programme.[14]

At the request of the European Parliament, civil rights groups and on their own initiative, **Data Protection Agencies opened investigations** to check if any European or national privacy and data protection laws had been violated through the allegedly illegal transfer of financial data from SWIFT to the US Treasury. The Belgian Privacy Commission (CBPL/CPVP) was assigned to lead the investigations while other (EU member) states did parallel investigations. Furthermore, the Article 29 Working Party and the European Data Protection Supervisor (EDPS) also issued opinions. In short, the Belgian Privacy Commission expressed great concern about the lack of transparency surrounding the arrangements SWIFT had made with the US Treasury. They confirmed the non-compliance of SWIFT with European privacy and data protection law and qualified the subpoenas of the US Treasury as 'non-individualised mass requests'. In addition, they highlighted that there was still no proof of the vital interest of the transfer of the massive amounts of financial data and suggested alternatives to the TFTP by drawing attention to existing procedures for exchanging financial data. The Article 29 Working Party added to this analysis that the EC directive 95/46 on data protection was applicable to the transfer of data from the SWIFT database and also established a responsibility of financial institutions in respecting this directive. Finally the EDPS found that the European Central Bank, as an overseer of SWIFT, a user of SWIFT's financial messaging system and as a central policy maker, should have shown commitment to respecting European privacy and data protection law.

Despite these assessments and their clear conclusions, it was quickly decided that the EU and the U.S. should negotiate about a clear legal framework in which the transfer of SWIFT data could continue. Between 2007 and 2008 three ad hoc solutions were advanced in order to render the TFTP more acceptable for the EU. All of them received substantial criticism. In April 2007, SWIFT decided to adopt the **Safe Harbour privacy principles** to facilitate the transfer of personal data from the European Community to the U.S., ensuring an adequate level of data protection according to European privacy and data protection laws. This was criticized because SWIFT is a European company with branches in the U.S.. Having its headquarters near Brussels, SWIFT should in the first place comply with Belgian laws on privacy and data protection which provide a higher standard of protection than the Safe Harbour Principles.[15] On 28 June 2007, following a negotiation of the European Commission, the Council Presidency and the U.S. authorities, a set of unilateral commitments, the so-called **'representations'**, of the US Treasury was made public. This document aimed to reassure Europeans about the programme, yet, it must be emphasized that its content reflected to a large extent the controls and safeguards that had already been negotiated by SWIFT. Finally, as part of the representations, an **'eminent European person'** was designated to review the procedures governing the handling, use and dissemination of the SWIFT data subpoenaed by the US Treasury. On 7 March 2008, the European Commission appointed the French counter-terrorism judge Jean Louis Bruguière for this function. He issued a first classified report in December 2008 and a second one in January 2010. However, both the appointment and the reports proved controversial. The neutrality of Bruguière was questioned because of his 30-year career in prosecuting terrorists, his very close relations with the American law-enforcement community and the

[14] For a more detailed discussion see: Wesseling (2013), *The European Fight against Terrorism Financing, Professional Fields and New Governing Practices*, Boxpress.
[15] Fuster, G., de Hert, P., Gutwirth, S. (2008), *SWIFT and the Vulnerability of Transatlantic Data Transfers,* International Review of Law, Computers & Technology, 22(1-2): 191-202.

absence of proof of his affinity with defending privacy and data protection rights. Moreover, his reports were considered unconvincing as they contain almost no empirical evidence and too much politically motivated instead of based on objective facts.

In response to the disclosure of the TFTP and to improve its commercial appeal in some jurisdictions, SWIFT decided to implement a new messaging architecture in which European and American data would be stored under different data privacy arrangements in separate regional databases. This change would imply that from December 2009 European data would cease to be automatically available in bulk to the US. In order to ensure the continuity of the TFTP after this organisational change, the conclusion of a **new EU-US agreement was considered necessary**. This led to a new period of politicization of the TFTP. When the European Parliament learned about the negotiations concerning an agreement, many MEPs strongly mobilized themselves on this issue. They were very disappointed and angry when an interim agreement was concluded just one day before the Lisbon Treaty was to enter into force and ultimately rejected the agreement on the basis of an extensive list of privacy and data protection shortcomings and inter-institutional power struggles. A new version of the EU-US Agreement was voted and accepted by the EP on 7 July 2010 and entered into force in August 2010.

The final EU-US TFTP Agreement introduces a number of important new elements to the TFTP. As defined in the Agreement, **Europol** has become responsible for receiving a copy of data requests along with any supplemental documentation and verifying that these U.S. requests for data comply with certain conditions (specified in article 4.2), including that they must be as narrowly tailored as possible in order to minimise the volume of data requested. Once Europol confirms that the request complies with the stated conditions, SWIFT is authorised and required to provide the data to the US Treasury. It explicitly mentions the possibility of the establishment of an **equivalent European TFTP System** (article 11, see next section for more detail). The Agreement also introduced an independent European **overseer** with the authority to review in real time and retrospectively all searches made of the provided data, the authority to query such searches and as appropriate to request additional justification of the terrorism nexus and block any or all searches in case of breaches of the safeguards on data processing (article 12). Furthermore, the Agreement states that regular **joint reviews** should be undertaken and specifies the elements that should be included in the reviews (article 13). In accordance with the Agreement three such joint reviews have been published so far (February 2011, October 2012, and November 2013). Finally, the Agreement also explicitly established a number of rights for European citizens. These include **transparent information** on the TFTP on the US Treasury offering a possibility for citizens to ask questions and information on the procedures available for the exercise of **the right of access** (article 15) and **the right to rectification**, erasure or blocking (article 16) including the availability of **administrative and judicial redress** (article 18).

Despite the introduction of these improvements, **many MEPs continued to feel dissatisfied with the Agreement**. Their main objection – the transfer of personal data in bulk from the SWIFT database to the US authorities – remained unresolved in the new text. Other concerns included: the retention period and deletion of the data (article 6), the conditions for sharing information with third countries (article 7) and public control and oversight (article 12). In addition, **reports and parliamentary debates have also continued to stir the debate and pointed to serious shortcomings in the implementation of the Agreement**. In 2010, parliamentary questions were raised regarding the fact that the identity of the interim and permanent overseer of the TFTP, a EU public official was held confidential for security, privacy and integrity reasons. In 2011,

it became known that Europol had difficulties guaranteeing the data protection rules set out in the agreement. A few months later it became clear that Europol has never rejected a request to the US Treasury, transferred bulk data on daily basis and did not know how much data was actually transferred.[16] The public statement made by the Europol Joint Supervisory Body declared that 'this could indicate that it is not possible to fulfill all intended safeguards of Article 4'.[17] This was followed by a court ruling in 2012 with respect to the disclosure of secret documents concerning the TFTP.[18] That same year, it became public that there was a potential conflict of interest amongst the members of the EU review team. This team is composed of three members from the DG Home of the European Commission and also included two individuals that are on a joint-supervisory body (JSB) linked to Europol. This means that these two persons – a data protection expert from the Netherlands and one from Belgium – are reviewing themselves.[19] In addition, in September 2013, the revelations from Snowden stated that the NSA has secretly tapped into the SWIFT database. While these claims have been denied by the US authorities and the European Commission does not see a need for further inquiries, part of the European Parliament is not fully convinced by the provided evidence that the US authorities did not breach the EU-US TFTP Agreement.

1.4. The EU Terrorist Finance Tracking System

If one is to reconstruct the debates concerning the TFTP that have taken place in the European Parliament between 2006 and 2010, and taking into account the persisting opposition of a part of the EP to the content of the EU-US TFTP agreement, the demand for a European equivalent in the form of a EU Terrorist Finance Tracking System (EU TFTS) might have seemed paradoxical to observers from outside.

Yet several reasons have been expressed in favour of the creation of a European equivalent TFTP system. The key arguments for the development of a European system would be (1) avoiding the systematic transfer of European financial data in bulk to the U.S., (2) an enhanced control over European security decisions and (3) the analytical and filtering process and (4) a better protection of personal data and a stronger guarantee for the respect for fundamental rights in accordance with EU legislation. In practice this would mean that 'searches into the SWIFT data would be carried out by European intelligence officers and more targeted data would be provided to the US authorities'. In addition, some Member States saw an added value in developing an independent European system for tracking terrorist finance in the longer term. Furthermore, it could increase their capacities to access relevant data and could strengthen their analytical capacities to track and identify terrorists through financial transactions".[20]

When the EU signed the EU-US TFTP agreement, it engaged itself to study the development of a durable, legally sound European solution to the issue of the extraction of financial

[16] Pop, V. (2011) *EU Police Report Shows Holes in US Data Deal*, EU Observer, 9 March 2011, and *MEPs Decry 'Breach of Trust' in EU-US Data Deal*, EU Observer, 16 March 2011, Nielsen, N. (2012) *EU hands personal data to US Authorities on Daily Basis*, EU Observer, 22 June 2012.
[17] Europol JSB (2012), *Europol JSB Inspects for the Second Year the Implementation of the TFTP Agreement*, 14 March 2012.
[18] In t Veld, S. (2012), *Uitspraak Europees Hof van Justitie over SWIFT*. Available at: http://site.d66.nl/europa/agenda/20120504/uitspraak_europees_hof_van, last accessed: 29 March 2014.
[19] Nielsen, N. (2012), *Terrorist data oversight tainted by potential conflict of interest*, EU Observer, 20 December 2012.
[20] European Commission (2013) *Communication From the Commission to the European Parliament and the Council, A European Terrorist Finance Tracking System (EU TFTS)*, COM(2013) 842 final, 27 November 2013 Brussels, p. 2.

messaging data within the EU. Practically this meant that the Commission was invited to submit "a legal and technical framework for the extraction of data on EU territory" before 1 August 2011 and a progress report on the development of an equivalent system before 1 August 2013.[21]

The Commission delivered a first **Communication detailing five different available options** and designed a roadmap for establishing an EU TFTS.[22] Two of the options advanced by the Commission – situated at the extreme ends of the spectrum ranging from a purely centralised approach on the European level and a purely national approach within each Member State - were rapidly excluded from further analysis as they were considered undesirable from a political, legal and operational viewpoint. The three other options were hybrid options and consisted of an option for:

(1) a coordination and analytical service via an EU central TFTS unit and with most tasks and functions being carried out on EU level,

(2) a EU TFTS extraction service involving the establishment of an EU central TFTS unit dealing with raw data but without analytical capabilities,

(3) an upgraded Financial Intelligence Unit (FIU) Platform made up of all the FIUs of the Member States and an ad hoc EU level authority responsible for issuing requests for raw data to the Designated Provider(s).

The **roadmap** published by DG Home specified amongst others the scope of a future TFTS – which could include financial service providers in addition to SWIFT and cooperation with third countries – and the estimated costs of establishing a EU TFTS. Depending on the option chosen, these costs would range between 33 to 47 million Euro to set up a centralised European or a hybrid system and an estimated annual cost of 7-11 million Euro to run the programme. The costs for a purely national system were esteemed to be significantly higher, respectively 390 million set-up costs and 37 million Euro running costs.[23]

Subsequently, these three hybrid models and an additional option of a retention and extraction regime were further developed into different sub-options for a future TFTS.

On 27 November 2013, the Commission published **a Second Communication on the EU TFTS and an Impact Assessment**, building on a number of core principles and identified options. The Communication highlights an explicit distinction between **a framework for extraction of data** on EU territory and allowing searches on the data that is currently provided by the EU to the U.S., to be conducted on EU soil, and **an equivalent EU system** which implies an independent system for tracking terrorist finance though access to, searches on and analysis of the data of Designated Provider(s) requiring a modification of the EU-US TFTP Agreement. It stresses **four principles** that need to be taken into account in the reflection on the various options for an EU TFTS: **fundamental rights, most notably right to privacy and personal data protection, necessity, proportionality and cost-effectiveness**. On the basis of these principles the Commission has conducted an impact assessment that shows that each of the feasible options has advantages and

[21] EU US TFTP Agreement, OJ L 195, 27 July 2010, p. 5.
[22] European Commission (2011), *A European terrorist finance tracking system: available options*, COM(2011)429 final and European Commission (2011), *Roadmap on the legislative proposal establishing a legal and technical framework for a European Terrorist Financing System* (EU TFTS), July 2011.
[23] European Commission (2011), Roadmap (…) see note 22.

disadvantages and concludes that 'the case to present at this stage a proposal for an EU TFTS is not clearly demonstrated'.[24]

The second part of this briefing note proposes an analysis and certain shortcomings on the three described CFT instruments.

[24] European Commission (2013) 842 and European Commission (2013) Commission Staff Working Document, *Impact Assessment Accompanying the document Communication from the European Commission to the European Parliament and the Council on a European Terrorist Financing Tracking System (TFTS)*, SWD(2013) 488 final, 27 November 2013, Brussels.

2. EUROPEAN CFT MEASURES: EFFECTIVENESS AND POLITICAL AND SOCIETAL IMPLICATIONS

KEY FINDINGS

- The 3rd Directive has raised **concerns with** regard to certain legal notions and issues, **privacy rights**, transparency, accountability. Moreover the **effectiveness** of the Third Directive in combating terrorism financing has been **insufficiently proven.**
- **Fundamental questions** on the suitability of an AML framework to combat terrorism financing, the shortcomings of a risk-based approach and the implication of charging private actors with national security tasks **must be thoroughly (re)considered**.
- While the Joint Reviews provide more insight into the TFTP, **some of the provided evidence appears controversial**. Furthermore more information must be made public regarding the **implications of the methods of data analysis** underpinning the TFTP.
- Some safeguards of the EU-US TFTP Agreement prove to be difficult/impossible to exercise in practice.
- The European Commission's 2013 **Communication on the EU TFTS does not offer a satisfying response** to the concerns on the transfer of financial data of European citizens in bulk to the US which remains insufficiently addressed in the EU-US TFTP Agreement and was for many MEPs a precondition to their consent.

This section proposes an analysis of the Third AML/CFT Directive, the EU-US TFTP and the EU TFTS. The scope of this note does not allow for giving an exhaustive overview of all aspects of these three measures. The aim is here to address the effectiveness of the measures, to draw attention to the methods underpinning financial surveillance measures, and to discuss some of their political and societal implications.

2.1. Analysis of the Third AML/CFT Directive

Previous studies by academics, consultancy firms and public bodies on the Third Directive have highlighted **a number of pitfalls**. These include **legal issues**, such as the question whether the EC/EU has the legal competence to adopt global standards in this field, the compatibility of the Directive with the protection of civil liberties and certain fundamental rights, in particular the confidentiality of the lawyer-client relationships as lawyers are also object of the Third Directive's reporting duties and the discrepancy between the FATF recommendations and the text of the Third Directive.[25] Equally, the definition and

[25] Mitsilegas, V. and Gilmore, B. (2007), *The EU legislative Framework against Money Laundering and Terrorist Finance: a Critical Analysis in the Light of Evolving Global Standards*, International Comparative Law Quarterly, 56:119-141, Van den Broek (2011), *Gelijkwaardigheid in het Antiwitwasbeleid: de FATF en de EU*, SEW, 10:422-428, Deloitte (2011), *Final Study on the Application of the Anti-Money Laundering Directive*, European Commission DG Internal Market and Services-Budget.

implementation of certain notions, such as Politically Exposed Person (PEP) and Ultimate Beneficial Owner (UBO) have spurred intense debates in political arenas and amongst the concerned professions.

Another major point that has been raised in a number of impact assessment reports of consultancy firms and national auditing agencies on the Third Directive and seems to be shared among many stakeholders, concerns the **thin results yielded by the Directive's requirements** with regard to combating terrorism financing. Reports prepared for the European Commission show that compliance with the Directive is sufficient but that the effectiveness of the Directive is difficult to measure because of a 'lack of quantitative and limited qualitative information.[26] Moreover, they argue that it is difficult to measure success because the preventive effect of the recommendations can hardly be measured at all.[27] The Dutch National Audit Office stated that the results of the AML/CFT legislation have been disappointing. It 'insufficiently prevents against terrorism financing' and, 'the chances of terrorism financing being discovered and punished are small'.[28] The proposal for a Fourth AML Directive explicitly takes into account the need to increase the effectiveness of the AML framework.

In the light of these findings it seems important to provide an analysis of the kind of processes that are set in motion by the Third Directive and of the assumptions underpinning the rationale of the Directive.

A first **fundamental question concerns the suitability of the AML framework for combating the financing of terrorism**. As mentioned above, quite rapidly after the 9/11 attacks the fight against terrorism financing became grafted on the already existing anti-money laundering legislation. This choice was understandable in the political context just after the attacks during which political leaders wanted to undertake swift action and there was a perceived need of urgency. Yet, the choice for this existing framework has a number of downsides since the logics of anti-money laundering measures are not necessarily applicable to combating terrorism financing. Although terrorism financing and money laundering are sometimes connected, their differences can be summarized as follows. Money laundering is driven by profits and the process takes place after illegal funds have been obtained. Terrorism financing, however, takes place before the crime and becomes criminal money after the transfer to an individual or group associated with terrorism. This is also called reverse money laundering or money dirtying. Contrary to money laundering, political goals are the main driver of terrorism financing. It usually involves small amounts of money and this money is not necessarily illegally derived. Moreover, including terrorism financing in the AML framework also assumes that terrorists use the formal financial sector to the same extent as money launderers. These characteristics of terrorism financing contribute to the difficulty to detect terrorism-related transactions with the AML instruments.

Second, the requirements of the Third Directive entail **a shift of responsibility and authority from the public sector to the private sector in the field of national security**. It implies that a range of private professionals (developers of detection software, compliance officers within banks, legal experts…) are responsible for the filtering and pre-selection of the risky profiles and transactions through an accumulation of individual and

[26] Deloitte (2011), see note 25, p. 293.
[27] John Howell & Co. (2007), *The EU's Efforts in the Fight against Terrorism Financing in the Context of the Financial Action Task Force's Nine Special Recommendations and the EU Counter Terrorist Strategy*, Independent Scrutiny for the European Commission, p. 26.
[28] Algemene Rekenkamer (2008), *Bestrijding Witwassen en Terrorisme Financiering*, p. 15

fragmented decisions. Subsequently these decisions structure the investigations led by FIUs and eventually the prosecution of terrorism financiers. Hence by charging private entities with the responsibility to combat terrorism financing, a shift has taken place as these entities are now involved in national security questions and are even the first to make certain security decisions.

Third, aside the advantages for regulated entities of reducing the administrative burden, being more cost-effective and an expectation of better quality reporting, **the risk-based approach to combating the financing of terrorism poses a number of challenges**. The risk-based approach allows for a prioritization of certain risks regarding customers, products, services or geographical areas. As a consequence monitoring practices and identification requirements vary according to the risk scores assigned to the profile of the customer, the specific financial product or the services and countries involved in a transaction. High-risk customers and transactions become subject to enhanced due diligence procedures while low-risk customers and transactions can be dealt with through simplified due diligence procedures. The norms are not only differentiated according to the kind and level of risk, but they are also flexible in order to be able to respond quickly to new trends of terrorism financing. However, the down-side of this differentiation and flexibility are the **lack of legal certainty, transparency and accountability** with regard to how decisions are taken. Moreover, it must be stressed that the **risk-based approach is not a neutral or objective** mathematic approach. For instance, the algorithms, risk categories and scenarios on which the risk-based analysis in banks is based, are an approximate aggregate of assumptions on how terrorism is financed, the available data elements and the technical possibilities to exploit the data. When a customer's profile is flagged or a transaction provokes a hit in the bank's monitoring software, humans must assess the significance of the results produced by the software and decide on their procedural follow-up. It can lead to arbitrariness and even discrimination as decisions are supposed to be partly made on the basis of intuition, self-regulation, and personal expertise. **This may have implications for clients with certain profiles** (one might think of those with Islamic names) **or behaviour** (such as making transfers to foreign countries, the use of certain products, the logic of a transaction in relation to other transactions).

Fourth, under the Third Directive regulated entities have to monitor all transactions of their clients along a set of specific criteria. Prior to the adoption of the Third Directive **privacy concerns** with regard to the requested practices were only briefly discussed in the European Parliament and were especially voiced by specific groups of experts. They included the concerns of some legal professionals (notably notaries and lawyers) that the obligation to report suspicious transactions would be in conflict with the confidential nature of the **lawyer-client relationship** and the right to a fair trial, and the respect for private life. Meanwhile a court case brought to the European Court of Justice established that albeit with exceptions the right to fair trial is not violated by the Third Directive. Another case considered by the European Court on Human Rights ruled that privacy violations had taken place in that particular case and this judgement enhances the respect for professional secrecy and confirms the limits of the authorities' power to interfere in the lawyer-client relationship. A second issue consists of the identification and the verification of the **ultimate beneficial owners** which some stakeholders consider as being privacy intruding. Moreover, the fact that the Third Directive gives maximum powers to Financial Intelligence Units to access directly or indirectly, on a timely basis, the financial, administrative and law enforcement information that it requires to properly fulfil its tasks, can conflict with data

protection obligations causing privacy issues for the reporting entities involved.[29] Thirdly, the matching of identification data of clients against various **public blacklists** as part of due diligence procedures has been considered a breach to the right to privacy. In fact, these lists contain names of suspected – and not only convicted – individuals and entities, potentially resulting in unjustified financial and reputational damage.

Fifth, the responsibility of the private sector to detect suspicious clients and transactions, and the diffused decision-making procedures across multiple departments within institutions, **lead to an almost complete lack of transparency and accountability**. In the words of a representative of the British Banking Association: 'there is a risk to the risk-based approach itself in that it does mean that banks have to make judgements, people have to take responsibility (…)'.[30] So far it is unclear to outsiders when decisions are taken and on the basis of what information. As the monitoring and reporting process are and must be entirely hidden to clients, it is impossible for them to control, complain or appeal against a bank's decision. Yet, the fact that defensive reporting of fictive suspicious transactions takes place and may lead to erroneous inclusion in police databases, makes the case for accountability all the more urgent.

Finally, despite the efforts undertaken by regulated entities, **the Third Directive sets in motion an apparatus of compliance, in which compliance itself has become the main objective**.[31] In fact, it is not indifferent whether the public or the private sector is responsible for combating terrorism. Although the argument that the private sector can combat terrorism financing more efficiently and more cheaply on the grounds that it already possesses financial data has some legitimacy, it needs to be emphasized that a bank's primary mission is not combating terrorism financing. While banks claim to feel a social and moral commitment with respect to combating terrorism financing, their first reflex is to not act as unpaid criminal investigators. In practice, this leads to a discrepancy between the Directive's objective of combating terrorism financing and the banks' objective of being compliant with CFT measures, and calls the effectiveness of involvement of the private sector into question.

2.2. Analysis of the TFTP

The TFTP is an important illustration of the philosophy of the War on Terror started by the US Bush administration. The aim of this and similar programmes is to prevent terrorism by exploiting massive amounts of personal data through technological tools. It implies proactive and even pre-emptive action to prevent harmful events from happening.[32] In this respect, the SWIFT database is particularly attractive as it constitutes the information hub of a very large part of the formal financial sector. From the perspective of intelligence services, the SWIFT database brings together very detailed information on financial transactions worldwide. While it is impossible to control all individual payment orders from any ordering customer to his or her bank somewhere on the globe, an important part of this information can be collected in the form of standardized and encrypted SWIFT messages sent through the SWIFTNet FIN service. By analysing massive amounts of international bank transactions available in the SWIFT database, it becomes possible to

[29] Deloitte (2011), see note 25, p. 69 and 291.
[30] House of Lords (2009) *Minutes of Evidence Taken Before The Select Committee on the European Union (Sub-Committee F) on Money Laundering and the Financing of Terrorism*, 4 March 2009, p. 25
[31] For a full description of this argument see: Wesseling 2013, see note 14.
[32] See for instance: Amoore, L. & de Goede, M. (2008), de Goede (2012), Wesseling et al (2012) (full details can be found in the references).

trace suspected terrorists at an early stage and without issuing separate information requests to individual banks. The data contained in the SWIFT database also permit intelligence services to establish large networks of potential terrorism suspects by mapping the transactions between individuals. Moreover, the relative anonymity of SWIFT outside the financial sector was – prior to the revelation of the TFTP – considered an advantage for using its financial data as a preventive tool in the War on Terror.

However, until now **little is known about the precise workings of the TFTP** and for many years communication proving the effectiveness of the TFTP has been minimal. To make a sound evaluation of the TFTP possible, the aim of this section is to reconstruct what kind of analysis could be made in the context of the TFTP and what might be the implications of this methodology. It also discusses to what extent the provided information on practical cases constitutes sound evidence for the effectiveness of the programme?

Although formal communication on the analytical instruments used for the TFTP is limited, it is possible to **propose a serious description of how the programme could work and identify its weaknesses** on the basis of an extensive analysis of official documents from national and European government authorities, publications by Data Protection Agencies, academic literature and work by investigative journalists.

The financial messages contained in the 'SWIFTNet FIN' database contain information such as the name, address, and location of the sender and the receiver as well as the amounts of money involved. As stated in article 5.3 of the EU-US TFTP Agreement, the use of this information for the TFTP **does not and shall not involve data mining or any other type of algorithmic or automated profiling or computer filtering**. According to US government officials this article is respected because the data retrieved from the SWIFT database were used for **link analysis or social network analysis**. Link analysis uses large collections of data to find links between a subject—a suspect, an address, or other piece of relevant information—and other people, places, or things. Instead of predictive algorithms, link- or social network analysis consists of subject- or pattern-based queries. In the case of the SWIFT data, the connections with terrorism investigations may be established on the basis of real names, addresses, phone numbers, and bank accounts. The data of interest are usually presented in the form of nodes in a network connected by links. By combining and linking the pieces of data with other sources, layers can be added to improve the understanding of the behaviour that the data represent.[33] Subsequently characteristics of the nodes and connections between them, can be analysed, for instance, the centrality of a person or entity, its closeness to others and the thickness of the connections between the nodes.[34]

The data elements on which searches are done **must have an established nexus to terrorism or its financing**. In a first stage, it can be assumed that, searches included the names of the 9/11 hijackers, the blacklisted entities and individuals suspected of terrorism and probably also all charities that have been publicly linked by the US as having possible terrorist ties, such as the Holy Land Foundation, Al Haramain, and the Global Relief Foundation. In addition, it is very probable that broader watch lists have been matched against the system. Like other intelligence services, the CIA has access to the Terrorist Identities Datamart Environment (TIDE) containing data on known, suspected or potential international terrorists. According to the US National Counterterrorism Centre, this

[33] US Department of Treasury (2006), *Feasibility of a Cross-border Electronic Funds Transfer Reporting System Under the Bank Secrecy Act*, October 2006, p. 10.
[34] More comprehensive descriptions and illustrations on the use of link analysis in the context of the TFTP can be found in: de Goede 2012, Wesseling et al. 2012, Wesseling, 2013 (see references).

database of terrorism suspects contains as of 2008 more than 500.000 names corresponding to approximately 400.000 individuals.[35] More recent reports indicate that in 2013, the database contains 875.000 names.[36] The TIDE records also include separate entries with aliases, (fake) passport numbers and (fake) birth dates. The vast majority of the listed persons (95%) are not U.S. citizen or residents.

The understanding of the TFTP as a programme based on link analysis provides a better understanding of the distinction that is made between **TFTP 'reports' and 'TFTP leads'**.[37] According to the 2013 Joint Commission report, 'a TFTP lead refers to the summary of a particular financial transaction identified in response to a TFTP search that is relevant to a counter terrorism investigation. Each TFTP report may contain many TFTP leads'.[38] (European Commission, 2012, 2013). For example, the 2013 Joint Report states that Spain has issued 11 requests which generated 93 investigative leads. It also stated that two requests Spain had issued with regard to Hezbollah generated as many as 27 leads and another request related to the PKK led to 19 leads. More generally the report notes that since the inception of the TFTP, it has produced tens of thousands of leads and over 3000 reports. However, **what remains unclear is how these leads are generated and what exactly must be understood by a lead or 'valuable lead information'? Up to how many links removed from the initial subject or data element the TFTP establishes its link-analysis?**

Despite the obligation that the requests from the US Treasury must be 'tailored as narrowly as possible', the data retrieved from the SWIFT data base may involve enormous amounts of data. Moreover the lists with terrorism suspects contain thousands of names and each subject is related to multiple other contacts. Therefore, **link-analysis is not 'extremely targeted' but potentially exponential**. Moreover, not all established links are necessarily related to terrorism as suspected terrorists will not only make terrorism related expenses. Clarification is thus needed how decisions are made on 'widening investigations, drawing in new suspects and identifying associates and potential future terrorists' while **avoiding criminalization by association and collateral damage of falsely identified suspects**.[39] More information is also needed regarding the information that is send to EU authorities. **What is the status of lead information?** Are these raw data of all possible links established by the software or have TFTP investigators already made an assessment of the relevance of the generated leads?

Furthermore, the data obtained from the TFTP is often praised for their accuracy and their rapid availability in comparison with other sources of intelligence and more conventional means of investigation. 'It may provide investigators with account numbers, bank identification codes, names, addresses, transaction amounts, dates, email addresses and phone numbers'.[40] Although these claims are not necessarily wrong, it must be stressed

[35] US National Counterterrorist Centre, *Terrorist Identities Datamart Environment* (TIDE), available at http://online.wsj.com/public/resources/documents/watchlist082108c.pdf.
[36] Reuters (2013), *Number of Names on U.S. Counter-Terrorism Database Jumps*, 2 May 2013.
[37] European Commission (2011), *Report on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program,* 17-18 February 2011, SEC(2011)438, (2012), *Report on the second joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program*, October 2012, SWD(2012)454, (2013), *Joint Report from the Commission and the U.S. Treasury Department regarding the value of TFTP Provided Data pursuant to Article 6 (6) of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program*, 27 November 2012, COM(2013)843.
[38] European Commission, (2013) (2012), see note 37.
[39] De Goede (2012), *Speculative Security, the Politics od Pursuing Terrorist Monies*, Minnesota University Press, p.63.
[40] European Commission (2013) see note 37.

that financial data from the SWIFT database **does not provide the specific context of a transaction**. TFTP data can establish links between individuals but the exact meaning of the relation between them remains speculative. The first newspaper articles on the TFTP reveal for example that there have been many false positives and investigations into useless links.[41] Moreover, it implies that TFTP investigators have to (re)construct or imagine, a posteriori, the context and relevance of a financial transaction in order to define whether the connection between the dots is actionable and constitutes a hit.[42]

Over the years, the **request for detailed, publicly available evidence proving the effectiveness of the TFTP** became louder, especially due to the mobilisation of MEPs regarding this issue. While this information was sparse during the first years after the disclosure of the TFTP, considerably more information has been provided since 2010 in particular in through the Joint Review procedures provided for in article 13 of the Agreement. The following paragraphs analyse the available information on the effectiveness of the TFTP.

Initially, the *New York Times* article revealing the TFTP in 2006 only mentioned one high profile case. In 2003, a financial transaction helped to locate Riduan Isamuddin, alias Hambali, the Indonesian leader of Jemaah Islamiyah (JI), a terrorist organisation linked to Al Qaeda and alleged mastermind of the 2002 bombing of a Bali Nightclub and of the 2003 attacks on the Jakarta Marriot hotel. Soon, two other cases in which SWIFT data are said to have played a role became public. These were the case Uzair Paracha and the case of the so-called 'liquid bombers'. Paracha was convicted and given a thirty-year prison sentence in the US in 2005 for receiving $ 200.000 in exchange for assisting a Pakistani Al Qaeda operative planning to commit a terrorist attack in the US. With regard to the disrupted plot to detonate liquid explosives on 10 flights from the UK to the US and Canada, 25 British individuals were arrested of which eight were prosecuted and three of them were found guilty of conspiracy to murder involving liquid bombs. However, how exactly data from the SWIFT database has contributed to the investigation and the indictments did not become clear. Regarding the first two cases, **it is important to highlight that the analysis of these cases shows the clear link between the TFTP and the detention and possibly torture in secret prisons and Guantanamo Bay**. Human rights associations have denounced that following his arrest in Thailand, Hambali was brought to a secret prison and later he was transferred to Guantanamo Bay, where he is currently being held without charge.[43] Similarly, in the case of Uzair Paracha, his father Saifullah Paracha who was suspected of the same offences as his son was arrested in Bangkok in July 2003 and subsequently detained in the CIA prison in Bagram, Afghanistan, and since September 2004 he has been held as an enemy combatant at Guantanamo Bay without any official charges against him.[44]

New figures became public when initial EU-US TFTP agreement was signed on 30 November 2009, before the vote of the European Parliament at the beginning of February 2010 and before its final vote on 8 July that same year. After the EU-US TFTP Agreement entered into force, and in line with articles 6 and 13, regular and public reports have been published specifying the number of occasions on which leads have been shared with Member States, third countries, Europol and Eurojust as well as providing cases in which the information has been used for the prevention, investigation, detection or prosecution of terrorism or its financing.

[41] Wesseling, M. (2013), see note 14.
[42] De Goede, (2012), see note 39, Wesseling et al. (2012), *Data Wars Beyond Surveillance, Opening the Black Box of Swift*, Journal of Cultural Economy, 5(1):45-62.
[43] Human Rights Watch (2004), *In Name of Security*, 24 May 2004, available at: http://www.hrw.org/sites/default/files/reports/malaysia0504.pdf.
[44] Amnesty International (2007), Act Now for Saifullah Paracha, available at: http://www.amnesty.org/fr/library/asset/AMR51/179/2007/ar/4046933e-34eb-45df-a9f4-b94760cc5539/amr511792007eng.pdf.

With regard to the quantitative evaluation, a distinction can be made between TFTP **information spontaneously provided** by the US Treasury (referred to in article 9 of the Agreement) and information transfer following a **EU request** for TFTP searches (article 10) (see table 3). Distracting the TFTP reports based on requests, these numbers show that roughly between 100 and 150 TFTP spontaneous reports are shared each year with EU Member States. The provided numbers do not allow for an interpretation which countries benefitted from the TFTP information, whether the information was useful and for what purposes – prevention, investigation, detection, prosecution – it was used.

Table 3: Overview of TFTP reports to the EU

Year	Cumulative total number of reports to European authorities since 2001 (total for that year)	Cumulative total of EU TFTP requests
End 2009	1450 (100)	-
January 2010	1550	-
January 2011	1700	15*
July 2011	1800	-
October 2012	More than 2000	94
November 2013	2100	194

Sources: A compilation of data from Bruguière 2010; Cohen 2010; De Volkskrant 2009; European Commission 2011, 2012 2013, Het Parool 2010; US Treasury 2011.
* This number is based on the period between August 2010 and January 2011.

In addition, concrete examples in which SWIFT data are said to have played a role are given in the 2010 Bruguière report, via the US Treasury website and in the Joint Review Reports of the TFTP of 2012 and 2013. According to the 2013 Joint Review report, TFTP data has provided added value in 16 high profile cases of which 11 have taken place prior to the conclusion of the Agreement. The report also gives a number of other examples in its explanation on how the TFTP is used.

A quick analysis of these concrete examples shows that in **a majority of the cases data from the TFTP does not allow for preventive action avoiding a terrorist attack from happening but contributes to investigations after an attack has taken place**. In this context it is important to recall that one of the arguments that made the analysis of vast amounts of banking data under the TFTP acceptable was the promise of prevention and its alleged unprecedented capacity to reveal identities and locations of suspected terrorists and their networks before terrorists strike. Yet, in most of the provided examples the added value concerns post-attack information gathering.

Moreover, in an – still ongoing – attempt for improving our understanding of how SWIFT data has been used so far, one of the provided added value examples has been investigated in more detail. According to the Bruguière report 'TFTP information revealed that Mohammed Bouyeri, the attacker of the Van Gogh murder investigation had connections to individuals with global terrorism connections' and that TFTP information provided added value in the Van Gogh investigation. However, reports drafted on basis of intelligence from the Dutch intelligence service AIVD and the court ruling in Bouyeri's case explicitly state that they did not find any indications of alleged international contacts. This finding suggests that both the intelligence services and the court did not possess the information from the TFTP, or they did not consider this information trustworthy or sufficiently significant. Furthermore, it suggests that the claim made in the Bruguière report is disputable, and calls into question what the added value of the TFTP information was if it did not play a role in preventing the murder of Van Gogh nor in the prosecution of Bouyeri. In short, **in this case, the provided information on the effectiveness of the TFTP is contradicted by information from other sources.**

Despite the claims that the TFTP has saved lives and that its effectiveness is proven, the above analysis shows that more information is needed on the practices and results of the TFTP, in addition to addressing issues such as the retention periods, the deletion of non-extracted data, oversight by Europol and independent overseers.

2.3. Reflections on an EU TFTS

The 2013 Impact Assessment (IA) offers a detailed overview of ten policy options concerning the possible setting up of an EU TFTS. Four of these options have been discarded because they were considered as impracticable from a legal or technical view. These include – the status quo plus option, the termination of the present EU-US TFTP agreement, a fully centralised system at EU level and a fully decentralised system at Member State level. In the assessment of the **remaining six policy options** four criteria have been used: effectiveness, impact (economic, social and political), practicability and feasibility. Special attention was being paid to the principles of privacy and data protection, proportionality, necessity and cost-effectiveness. Analysing the IA against the background information provided in section 1.4, the following considerations can be offered.

First, it is important to highlight that despite the arguments provided by the Communication of 2013 to justify the absence of a proposal for an EU TFTS, the Communication of 2011 clearly indicated that sticking with the status quo 'would not reply to the call from the Council and the Parliament to come forward with a proposal to submit "a legal and technical framework for extraction of data on EU territory"'. The **status quo option does not provide a solution** as it 'would not contribute to limiting the amount of personal data transferred to third countries and it would not provide for the processing of data on EU territory, subject to EU data protection principles and legislation'.[45] Bringing this aspect back into memory is important because for many MEPs the promise of data analysis capacities on European soil through an EU TFTS was one of the preconditions for approving the EU-US TFTP Agreement in 2010.

Second, an element that is very present in the IA concerns **costs**. In the assessment of each of the policy options it is stressed that there could be resistance against expenditures due to financial and budgetary constraints in the current economic crises. However, the direct financial costs of the policy options that were considered feasible do not appear extreme in the context of a European security programme. However, a more fundamental issue that needs to be discussed concerns whether financial arguments should outbalance the more fundamental concerns of respect for human and fundamental rights and enhanced control over European security decisions. Likewise, it needs further debate how costs compare with estimated benefits in terms of effectiveness. There are no estimations how many requests Member States would make in case of an EU TFTS. On the basis of current information, it can be argued if the conclusion that a TFTS have 'overall some positive impact on the prevention of terrorism and enhancing security'.

Thirdly, **the IA addresses four problem drivers**. One of the concern is that the current mechanism in place to analyse financial messaging data is led by a third country thus not fully representing EU's specific interests (driver 1). This 'implies that the TFTP has mainly been used by the US for the purpose of investigating terrorist activity linked to the threat as perceived by the US and less on forms that pose a threat to the EU'. However, the difference in perception of the threat should not be the only aspect considered with regard

[45] European Commission, COM(2011)429 final, p. 8, see note 22.

to this driver. The current handling of the TFTP by the US also implies that the EU has less control over data and searches. Another problem that was highlighted concerns the protection of personal data of European citizens (driver 3). Although a number of improvements have been made and applied with the implementation of the EU-US TFTP, standards are still not fully equivalent to EU legislation as the issue of bulk transfers remains and shortcomings with regard to judicial and administrative redress have not been resolved. Furthermore, it is claimed that there is insufficient technical and legal capability within the EU and in Member States to establish financial linkages to trace and map terrorist networks (driver 4). Yet, if reciprocity between the parties and cooperation, assistance and advice of the US to contribute to the effective establishment of an EU TFTS (article 11.2) has real substance, it should be possible to overcome these obstacles. Finally, the Impact Assessment does propose options for broadening the scope of information that could be analysed in a future EU TFTS by adding additional financial messaging providers and additional message types (driver 2). It does not sufficiently emphasize other options in which not all elements of the US TFTP are copied into a future EU TFTS and in which the EU system would take into consideration the specificity of the EU legal and administrative framework including the respect of applicable fundamental rights[46].

[46] COM(2011) 429 final, p. 4, see note 22.

3. POSSIBLE INITIATIVES AND RECOMMENDATIONS

KEY FINDINGS

Following from the preceding overview and the analysis, the suggested initiatives and recommendations can be divided in four parts, concerning the need to: (1) increase publicly available evidence on effectiveness and methods, (2) discuss the centrality and desirability of financial surveillance measures in the light of the difficulties to trace terrorist monies and its unintended side-effects, (3) strengthen the accountability, transparency and citizen's rights of the TFTP Agreement, and (4) re-launch reflections to realise an EU TFTS.

This note aims to provide background information on possible measures to combat terrorist financing, including but not limited to an EU TFTS, and a set of recommendations for improving existing initiatives in this field.

3.1. Increasing publicly available evidence on effectiveness

Recommendation: more evidence is needed to establish the effectiveness of the EU measures for combating the financing of terrorism.

The evaluation of the EU's main instruments to combat terrorism financing shows that it has been difficult to obtain evidence on the effectiveness of financial measures to combat terrorism, due to methodological limitations or secrecy. Yet, qualitative analysis has shown that both the practices of risk-based analysis of the Third (and maintained in the Fourth) Directive, and of link-analysis for the TFTP, have a number of important shortcomings while evidence on the effectiveness in combating terrorism financing remains limited in quantity and quality.

Recommendation: insight into the added value of the TFTP could be further enhanced by providing statistics specifying which of the reports or leads were used for respectively prevention, investigation, detection, or prosecution.

Compared to the earlier absence of public reports providing evidence and examples of the added value of the TFTP, the Joint Briefings have contributed to improving knowledge about the TFTP. However, the numbers provided in these reports do not provide much insight in the purpose and their contribution for ongoing terrorism investigations.

Recommendation: more information is needed on the actual workings and implications of risk- and link-based security initiatives for combating the financing of terrorism.

This briefing provided a brief overview of how two financial surveillance programmes work and of their implications for European citizens. From the analysis it became evident that the implications of risk-based and link-based security methods are potentially serious for citizens but remain largely unnoticed because of a lack of limited possibilities to independently investigate their practices and their alleged success stories.

3.2. (Re-)opening fundamental discussions

Recommendation: (re)opening fundamental discussion on the nature and centrality of the current fight against terrorism financing and the desirability of financial surveillance instruments in the light of limited and debatable evidence on its effectiveness.

In the wake of the revelations of what came to be called in June 2006 the 'Swift affair', the European Parliament has held extensive debates about the implications of these revelations. Although the TFTP remained an important issue on the European agenda until the adoption of an US-EU TFTP Agreement in the summer of 2010, and regularly re-emerged as a source of concern, the focus of the questions surrounding the debates on the TFTP has steadily been narrowed down. Taking into account the point made above on the very limited and debatable evidence of success cases and the recent stream of revelations on American surveillance initiatives, it seems necessary to re-open debates regarding the desirability of the TFTP in case its preventative qualities appear limited. An important contribution in this sense has recently been made in the Moraes report.

Furthermore, discussion is needed about the centrality of combating terrorism financing in the fight against terrorism, given the well-established facts that terrorism is relatively cheap and meaningful terrorist scenarios are very difficult to design.

3.3. Improving accountability, transparency and assuring citizen's rights

Recommendation: increased transparency is needed with regard to the volumes of data transferred to the US Treasury, the Overseer and the Joint Reviews.

One focus of the transatlantic discussion on practices of classification in the case of the TFTP has become the question of numbers. We do not know, to date, the volumes of data transferred from the SWIFTNet FIN service to the US Treasury in the context of the TFTP. These numbers are not public, yet deemed important in the context of the Agreement which stipulates that data requests have to be 'tailored as narrowly as possible' (Article 4.2.c.).[47] More transparency is also needed with regard to the identity of the EU Overseer. Despite the reasons given to justify the secrecy surrounding the identity of the Overseer (see section 1.3), it seems remarkable to keep hidden the face of the individuals in Washington who are supposed to produce European accountability in relation to the TFTP. Would the integrity of the Overseer and the treaty arrangements not be *enhanced* by his public appearance?[48]

In order to limit the chance of conflicts of interest in the Joint Review team and increase democratic oversight, it could be considered that future Joint Review teams include MEPs (for instance members of the LIBE committee) who have security clearance.

The methodology of the review procedure could further be strengthened by the possibility to watch the databases being operated in real-time with results shown and explained on

[47] De Goede, M. & Wesseling, M (forthcoming) *Clashing Cultures of Secrecy: Tracking Terrorism Financing and the Paradox of Publicity*, Special Issue 'Security and its Publics', Cultural Politics.
[48] De Goede, M. &Wesseling, M (forthcoming) see note 47.

screen by a senior analyst, as has been the case within the Joint Review of the PNR Agreement.[49]

Recommendation: making the right to access, rectification, erasure, blocking and administrative and judicial redress a reality.

With regard to the TFTP, the European Parliament has successfully negotiated the access of European citizens to US Courts to appeal against abuse or wrongful decisions following from the TFTP. However, as stated in the Second Joint Review of the TFTP the rights of access, and rights to rectification, erasure, blocking and redress cannot be exercised in practice. Because the Treasury is only allowed to access the database if a nexus with terrorism is clearly established, that also means that there is no possibility for the Treasury to search the database for information of individuals which was not accessed before.[50] Another possibility for redress is to start a procedure under the Freedom of Information Act (FOIA). However, a study of the two court cases brought before the American Court of Justice by American citizens for potential privacy breaches by the TFTP (*Walker Kruse v. SWIFT SCRL* and *Amidax Trading Group v. SWIFT SCRL et al.*) have shown that these cases were unsuccessful as the plaintiffs could not provide evidence that their personal data were directly targeted by the TFTP. The difficulty for plaintiffs to provide plausible evidence that their financial data have been used in a security programme which functioning continues to be top secret, combined with the observed threat to shut down lawsuits concerning the TFTP on national security grounds and the immunity of SWIFT with regard to the transfer of financial data to the US Treasury, also temper expectations on successful legal action of European citizens against the TFTP.

Recommendation: further clarifications are needed regarding possible access of the NSA into the SWIFT database.

In the light of the declarations of the US authorities, the European Commission and SWIFT that the TFTP Agreement has not been violated through the secret access to the SWIFTNet FIN Service by the NSA, further information must be collected whether this means that, contrary to what was suggested in the media reporting, the SWIFT database has not been accessed at all by the NSA or whether there is a loophole in the agreement by which secret access of the NSA might not be considered as a breach of the TFTP Agreement.

3.4. Continuing efforts to develop an EU TFTS

Recommendation: continuing efforts to develop an EU TFTS

The Impact Assessment (IA) has indicated that each of the six policy options that it discussed has advantages and disadvantages. Yet, if an EU TFTS was to be established, the comparison of the different options led to believe that option B.3.1, establishing a central EU TFTS unit but in which Member States are free to undertake their own searches, is considered to be able to contribute most to the achievement of the policy objectives described in the IA. As the transfer of bulk data is not adequately dealt with under the TFTP, shortcomings concerning the practicability of certain rights and the control over searches remain. This note concludes that maintaining the status quo is not a desirable policy outcome and further efforts must be made to address these issues.

[49] European Commission (2013) Joint Review of the Implementation of the Agreement between the European Union and the United States of America on the Processing and Transfer of Passenger Name Records to the United States Department of Homeland Security, SEC(2013)630.
[50] European Commission, (2011), p. 16-17, see note 37.

REFERENCES

- Amicelle, A. & Favarel Garrigues, G. (2009), *La lutte contre l'argent sale au prisme des libertés fondamentales: quelles mobilisations?* Cultures & Conflits, 76:39-66.
- Bigo, D., Carrera, S., Hayes, B., Hernanz, N., Jeandesboz, J. (2012), Justice and Home Affairs Databases and a Smart Borders System at EU External Borders: An Evaluation of Current and Forthcoming Proposals, CEPS Study, No. 52/December 2012.
- Bulterman, M. (2005), *Oh, baby, baby, it's a wild world, over terrorisme financiering, financiële transacties en rechtsbescherming*, NJCM Bulletin, 30(8): 1069-1084.
- Council of the EU (2004), *The Fight against Terrorist Financing,* Doc. 16089/04.
- De Goede, M. (2012), *The SWIFT Affair and the Global Politics of European Security*, Journal of Common Market Studies, 50(2): 214-230.
- De Goede, M. (2012) *Speculative Security, The Politics of Pursuing Terrorist Monies*, Minesota University Press.
- De Goede, M. & Wesseling, M. (forthcoming) *Clashing Cultures of Secrecy: Tracing Terrorism Financing and the Paradox of Publicity*, Cultural Politics.
- European Commission (2011), *Report on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program*, 17-18 February 2011, SEC(2011)438.
- European Commission (2012), Report on the second joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, October 2012, SWD(2012)454.
- European Commission (2013), *Joint Report from the Commission and the U.S. Treasury Department regarding the value of TFTP Provided Data pursuant to Article 6 (6) of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program*, 27 November 2012, COM(2013)843.
- European Commission (2011), Roadmap on the legislative proposal establishing a legal and technical framework for a European Terrorist Financing System (EU TFTS).
- European Commission (2013), Proposal for a Directive on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, 5 February 2013.
- European Parliament (2013), *resolution of 4 July 2013 on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' privacy*.
- European Parliament (2013), *resolution of 23 October 2013 on the suspension of the TFTP agreement as a result of US National Security Agency surveillance.*

- European Parliament (2014), *Report on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and their Impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs*, 21 February 2014.

- European Parliament (2014), Legislative resolution of 11 March 2014 on the proposal for a directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (COM(2013)0045) – C7-0032/2013 – 2013/0025(COD).

- Europol Joint Supervisory Body (2012), *Europol JSB Inspects for the Second Year the Implementation of the TFTP Agreement*, Public Statement, 14 March 2012.

- FATF (2001), *FATF Pledges to Combat the Financing of Terrorists*, Press release, Doc. PAC/COM/NEWS(2001)90, 30 October 2001.

- Fuster, G., de Hert, P., Gutwirth, S. (2008), *SWIFT and the Vulnerability of Transatlantic Data Transfers,* International Review of Law, Computers & Technology, 22(1-2): 191-202

- Guild, E. (2008), The Uses and Abuses of Counter-Terrorism Policies in Europe: The Case of the 'Terrorist Lists', Journal of Common Market Studies, 46(1):173-193.

- Guild, E. (2010), *EU Counter-Terrorism Action: A Fault Line Between Law and Politics?*, CEPS, April 2010.

- Mitsilegas, V. & Gilmore, B. (2007) *The EU legislative Framework against Money Laundering and Terrorist Finance: a Critical Analysis in the Light of Evolving Global Standards*, International Comparative Law Quarterly, 56:119-141.

- Tappeiner, I. (2005), *The Fight against Terrorism. The Lists and the Gaps*, Utrecht Law Review, 1(1): 97-125.

- Van den Broek, M. (2011), *Gelijkwaardigheid in het Antiwitwasbeleid: de FATF en de EU*, SEW, 10:422-428.

- Vlcek, W. (2005), *European Measures to Combat Terrorist Financing and the Tension between Liberty and Security*, Challenge Working Paper, September 2005.

- Wesseling, M., de Goede, M., Amoore, L. (2012), *Data Wars Beyond Surveillance, Opening the Black Box of Swift*, Journal of Cultural Economy, 5(1):45-62.

- Wesseling, M. (2013), *The European Fight against Terrorism Financing, Professional Fields and New Governing Practices*, Boxpress.

EUROPEAN PARLIAMENT

CATALOGUE QA-01-14-397-EN-C

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

Role

Policy departments are research units that provide specialised advice to committees, inter-parliamentary delegations and other parliamentary bodies.

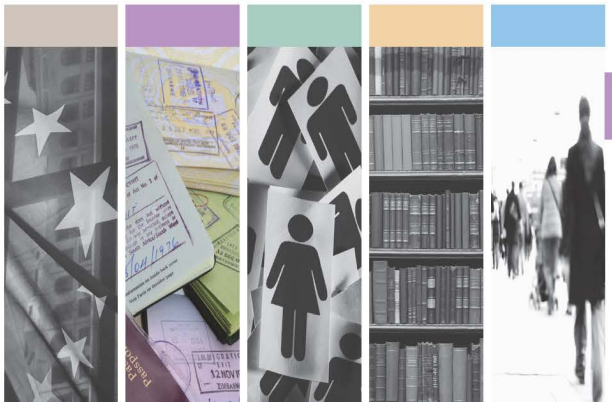
Policy Areas

- Constitutional Affairs
- Justice, Freedom and Security
- Gender Equality
- Legal and Parliamentary Affairs
- Petitions

Documents

Visit the European Parliament website: **http://www.europarl.europa.eu/studies**

PHOTO CREDIT: iStock International Inc.



ISBN: 978-92-823-5713-2
DOI: 10.2861/62586

Publications Office