Royal United Services Institute
for Defence and Security Studies

Occasional Paper

An EU Terrorist Finance Tracking System

Mara Wesseling

An EU Terrorist Finance Tracking System

Mara Wesseling

Occasional Paper, September 2016

Royal United Services Institute
for Defence and Security Studies

Over 180 years of independent defence and security thinking

The Royal United Services Institute is the UK's leading independent think tank on international defence and security. Its mission is to be an analytical, research-led global forum for informing, influencing and enhancing public debate on a safer and more stable world.

Since its foundation in 1831, RUSI has relied on its members to support its activities, sustaining its political independence for over 180 years.

London | Brussels | Nairobi | Doha | Tokyo | Washington, DC

Published in 2016 by the Royal United Services Institute for Defence and Security Studies.

RUSI Occasional Paper, September 2016. ISSN 2397-0286 (Online).

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org
RUSI is a registered charity (No. 210639)

Contents

Acknowledgements

The author would like to thank the representatives of EU institutions and the authorities in several EU member states, as well as several US-based experts, for the time they have spent in sharing their views and expertise. Gratitude is also extended to Tom Keatinge and Inês Sofia de Oliveira at the Centre for Financial Crime and Security Studies at RUSI for their guidance and feedback throughout the writing process, as well as the editorial team at RUSI. Finally, the author is also grateful for the comments received on an earlier draft of this paper from David Carlisle, an independent consultant, and two reviewers who prefer to remain anonymous.

Foreword

Tom Keatinge

Following the 9/11 attacks on New York and Washington DC, US authorities began a relentless effort to identify and disrupt the financing of terrorism in the belief that funding represented the Achilles heel of those that sought to attack the US and its allies. Hitherto, the gathering of financial intelligence had relied on banks filing reports with the authorities whenever they believed they had identified suspicious activity flowing through their books. This system was (and remains) sub-optimal for building an overall picture of financial activity as it provides just a window, through one bank, into the activity of a particular individual, and often only if the bank itself identifies their account holder as being suspicious.

The US authorities therefore sought a means of gaining a much broader picture of financial activity from a source into which they could discretely tap. That source was SWIFT (Society for Worldwide Interbank Financial Telecommunication), the international financial messaging system used by almost all banks to instruct money transfers around the globe. When news of this arrangement broke in 2006, champions of privacy, particularly those within the EU, were alarmed. But the legal underpinning, and the potential security benefits, of this agreement meant that by 2010 an EU–US Terrorist Financing Tracking Program (TFTP) had been adopted that also allows EU member states to benefit from intelligence gathered via SWIFT.

Today, as the EU comes to terms with the threat and reality of terrorist attacks within its member states, and recognising both the power of the TFTP and the gaps that exist in the monitoring of euro-denominated financial transactions in the EU, the suspicions that greeted the TFTP have been replaced by a broadly held desire to replicate this system for Europe with the proposed creation of an EU Terrorist Finance Tracking System.

It is this journey from suspicion to proposed adoption that this latest paper from RUSI's Centre for Financial Crime and Security Studies reviews at a time when EU leaders and policymakers are searching for more effective ways of gathering information that can assist in strengthening counterterrorism responses.

Tom Keatinge
Director, Centre for Financial Crime and Security Studies, RUSI.

Executive Summary

THE IDEA FOR a European equivalent to the US's Terrorist Finance Tracking Program (TFTP) – an investigative tool for tracing and linking international financial transactions in order to detect terrorist plots and networks – was first proposed by members of the European Parliament and certain EU member states during the 2010 negotiations on the EU–US TFTP Agreement. Under this arrangement, the EU is not allowed direct access to the US system but may submit search requests. Critically, transactions conducted under the auspices of the EU's own pan-European payments initiative, the Single Euro Payments Area (SEPA), which enables bank-to-bank payments within the Eurozone, are excluded from the TFTP, an omission that some refer to as 'the SEPA data gap'. SEPA is the EU-wide single market for payments made in euros that has been progressively established with adoption of the Payment Services Directive (PSD)[1] of 5 December 2007 to facilitate cross-border payments. It refers to both a geographic space[2] and a legal framework, providing a standardised payment format for credit transfers, debits, (credit) card payments and money remittance, as well as mobile and online payments. Financial services providers had to migrate to the SEPA format before 1 February 2014,[3] while non-EU SEPA countries must comply with the SEPA framework by the end of 2016.[4]

Article 11 of the EU–US TFTP Agreement specifies that the possibility of introducing a so-called 'EU Terrorist Finance Tracking System (EU TFTS)' would be investigated and that the US would provide assistance and advice in establishing such a system, should this be the result of the investigation. The first impact assessment, produced in November 2013 and detailing the options towards this end, was not taken forward. Nevertheless, a renewed interest in a European system for tracking terrorist finance emerged after the terrorist attacks on the Paris offices of French satirical magazine *Charlie Hebdo* in January 2015 and further Paris attacks in November of the same year. The latest EU 'Action Plan to Strengthen the Fight Against Terrorist Financing', published on 2 February 2016, demanded that by December 2016[5] the European Commission

1. The objective of the PSD is to make cross-border payments denominated in euros as easy, efficient and secure as 'national' payments within an EU member state and to increase competition by opening up the payments market. A revised Payment Services Directive (PSD2) was adopted in October 2015.
2. As of July 2015, the SEPA covered 35 countries – the 28 EU member states, the four EFTA members (Luxembourg, Liechtenstein, Switzerland and Norway) and Andorra, Monaco and San Marino.
3. European Union 'Regulation (EU) No 260/2012 of the European Parliament and of the Council of 14 March 2012 Establishing Technical and Business Requirements for Credit Transfers and Direct Debits in Euro and Amending Regulation (EC) No 924/2009', 30 March 2012, L94/22.
4. EU Counter-Terrorism Coordinator, 'State of Play on Implementation of the Statement of the Members of the European Council of 12 February 2015, the JHA Council Conclusions of 20 November 2015, and the Conclusions of the European Council of 18 December 2015', doc 6450/16, 1 March 2016, p. 29.
5. European Commission, 'Communication from the Commission to the European Parliament and the Council on an Action Plan for Strengthening the Fight against Terrorist Financing', COM(2016) 50/2, 2 February 2016.

should undertake a new assessment of a possible EU TFTS, which would complement the existing EU–US TFTP Agreement.

This paper is structured around two key issues. First, it studies past debates and negotiations concerning the US TFTP in order to highlight those issues of importance should an EU TFTS be created. Second, it examines previous and current proposals, as well as debates, concerning the creation of an EU TFTS, drawing out the differences between previous iterations and current demands. This paper is concerned with identifying the lessons that can be learned from previous experiences and with the analysis of past and current debates on the creation of an EU TFTS. The last section offers further food for thought regarding the possible creation of an EU TFTS.

The study of three successive phases of the TFTP – between 2001 and 2006, when the existence of the programme was not publicly disclosed; between 2006 and 2010, when the privacy and data protection safeguards of the TFTP were intensely debated in the EU; and the period since 2010, when the EU–US TFTP Agreement was adopted – serves to highlight the importance of the following issues that will need to be addressed in the decision-making process for a potential EU TFTS:

1. The design of the system, including whether it should be centralised or decentralised; which datasets it will use; the private companies that will be designated to provide data; and whether its use should extend beyond combating terrorism.
2. The compatibility of such a system with EU privacy and data protection legislation, in particular the issue of requests for data in bulk.
3. Democratic and judicial oversight, including a degree of transparency, accountability procedures and rectification processes.[6]
4. Relations with the US and other third countries – and specifically whether access of the US and other non-EU countries to the EU TFTS would require the adoption of new agreements or could be handled via amendments to the existing framework.
5. The added value of a new complementary programme to the US TFTP, to which the EU already has indirect access under the 2010 agreement. Considerations in this regard include the costs versus the effectiveness and efficiency of the EU having its own system, the potential improvement of fundamental rights, and the political benefits.
6. Societal desirability and popular support.

A comparison of the different options for an EU TFTS between the structure described in the initial 2013 impact assessment and the renewed demands for such a system that have been articulated since January 2015 shows a shift in conceptualisation, from a system that would *replace* part of the EU–US TFTP Agreement to a *complementary* system that would focus on intra-European SEPA data, which is currently not covered by the agreement.

6. In debates regarding the TFTP it became clear that democratic and judicial oversight were initially not sufficiently organised. For several years, the transparency, accountability and judicial redress procedures in the case of false positives of the programme were unclear, a shortcoming which contributed to the long controversies that emerged after the disclosure of the programme.

Moreover, earlier concerns over full conformity with EU data protection and privacy legislation and the need for sovereignty over security decisions seem to have become less central, as discussions now focus on stepping up the fight against terrorism by closing the SEPA data gap.

Initial conclusions, which might be used to stimulate and frame upcoming debates on a potential EU TFTS, are:

- The purpose(s) of the programme – including preventive intelligence gathering, reactive evidence gathering or gains in procedural efficiency – needs to be clearly established. Would the creation of an EU TFTS be worth the investment if its added value is mainly in post-event analysis rather than the disruption of planned attacks?
- It is difficult to estimate accurately the number of terrorist acts that have been prevented as a result of the TFTP, or to establish clearly the relevance of leads from the TFTP to successful prosecutions for terrorist offences. To assess the added value of a potential EU TFTS, it is necessary to develop a better definition of 'effectiveness' and 'success' in this context, as well as a corresponding methodology to measure the outcomes.
- More reflection is needed to establish whether the connections between an individual and a terrorist organisation that may potentially be identified by an EU TFTS could also be identified by other means. In other words, how crucial is it to have broad access to SEPA payment data?
- Consideration should also be given to whether there are other possibilities for closing the SEPA data gap. For example, instead of creating an EU TFTS that mirrors the US TFTP, existing information exchange tools used by national financial intelligence units (FIUs) in Europe and worldwide might be extended. The EU could also explore the use of the planned centralised bank and payment account registers or consider creating other rapid outreach and information exchange tools between law enforcement agencies and the private sector.
- In 2013, the costs of creating an EU TFTS were considered too high. Yet a combination of the evolving conceptualisation of the EU TFTS as a *complementary* tool, the recent terrorist attacks on European soil, and the persistent threat of new attacks may have increased EU member states' willingness to prioritise the necessary investment in an EU TFTS as part of a broader reassessment of EU counterterrorism measures.
- A complementary EU TFTS focusing on SEPA data would not require a renegotiation of the EU–US TFTP Agreement; however, reciprocity with the US and the possible granting of access to other third countries are likely to be discussed.
- It has not yet been determined whether from a data protection and privacy perspective an EU TFTS is necessary and proportionate, and whether existing technical obstacles could be overcome in order to reduce the volume of the requested data.
- There is no ready-made solution for democratic and judicial oversight of an EU TFTS. There is a range of possible supervision arrangements involving a range of actors, and this area would therefore need further exploration.
- For well-informed decision-making on the EU TFTS, the (side) effects and the implications for personal freedom of link analysis and network mapping (the operational practices

which underpin the TFTP and which may underpin the EU TFTS) need to be more extensively debated.[7]

It is likely that the US would support and help to create an EU TFTS on the understanding that it would not alter the existing EU–US TFTP Agreement, that the US would benefit from the system – by submitting research queries and retrieving information from it – and that the system would operate in a robust and timely manner.

Finally, should an EU TFTS be established, the UK's decision to leave the EU would likely require it to seek a new agreement with the US regarding the TFTP. The transaction data on which the TFTP relies is stored in the database of financial messenger provider SWIFT (Society for Worldwide Interbank Financial Telecommunication), and those concerning the UK would no longer be covered by the existing agreement. Having left the EU, the UK would be in a similar situation to other state participants in SEPA that are not in the EU – specifically, the four European Free Trade Association (EFTA) countries (Iceland, Liechtenstein, Norway and Switzerland) as well as Andorra, Monaco and San Marino. Like these countries, the UK would need to negotiate a separate agreement regarding an EU TFTS.

7. The TFTP uses a process referred to as 'link analysis'. This entails automated sifting through large collections of data supplied in order to make financial transactions, and the mapping of a suspect's network by drawing links between names, addresses and bank account numbers. Unlike data mining, the effects of this methodology for combating terrorism are little discussed. Link analysis does not involve the examination of all data contained in a database and is therefore considered to be more targeted. Yet it is known that in the process of revealing financial relations between suspected terrorists, false positives and useless links are also generated. The potential implications for individuals who have been wrongfully designated as terrorist suspects need to be considered. Further clarification is also needed about the fact that the datasets focus on selected countries and whether this might discriminate against individuals dealing with or residing in these countries.

Introduction

The financing of terrorism has been criminalised in the UK since the 1970s and under international law since 1999 (under the terms of the UN Convention for the Suppression of the Financing of Terrorism).[1] However, pursuing terrorist funding was not a high priority in most law enforcement circles.[2] This changed radically after the terrorist attacks of 11 September 2001. Combating terrorism financing became a central element in the global War on Terror and governments rapidly adopted innovative, data-led tools with the aims of gaining better insights into suspicious money flows and terrorist networks and of preventing future attacks.[3]

In this context, the US government created the Terrorist Finance Tracking Program (TFTP) shortly after the 11 September attacks. This initially secret intelligence programme consists of gathering and analysing financial transaction data from the SWIFT (Society for Worldwide Interbank Financial Telecommunication) global financial messaging system, which facilitates money transfers between financial institutions worldwide, in order to detect terrorist plots and trace potential terrorists and their financiers. As the SWIFT system accounts for a large proportion of all messaging related to international bank transactions, searching (parts of) its database was considered discrete, much faster, more efficient and more effective than the options that had existed in 2001 for gathering financial intelligence.[4]

After the existence of the TFTP was publicly disclosed by the US in 2006, the programme progressively became part of European security architecture, leading to the adoption of the EU–US TFTP Agreement in 2010. Although the EU was not involved in the development of the TFTP, EU member states are said to benefit greatly from TFTP information that is sent spontaneously by US authorities without being specifically requested by the EU.[5] Moreover,

1. The Northern Ireland (Emergency Provisions) Act of 1973 and the Prevention of Terrorism Act of 1974 were expanded and strengthened in the 1980s. New clauses were added concerning the forfeiture and freezing of terrorists' assets, the obligation to report information on money suspected as being related to terrorism, and introducing the concept of criminal liability of those who (help to) fund terrorism.
2. Thomas J Biersteker and Sue E Eckert (eds), *Countering the Financing of Terrorism* (London: Routledge, 2008).
3. Marieke de Goede, *Speculative Security: The Politics of Pursuing Terrorist Monies* (Minneapolis, MN: University of Minnesota Press, 2012).
4. European Commission, '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, p. 13.
5. Its great value to the EU has been emphasised on many occasions, both before and since the conclusion of the EU–US TFTP Agreement in 2010. See, for instance, Jean-Louis Bruguière, 'Second Report on the Processing of EU-Originating Personal Data by the United States Treasury Department for Counter Terrorism Purposes: Terrorist Finance Tracking Programme', January 2010, p. 3; European Commission, 'Commission Staff Working Document'; see also the webpage of the

the agreement also entitles EU member states to submit their own research requests to US authorities, which are increasing.[6] Today, the programme must thus be considered an integral part of the EU framework for combating the financing of terrorism.

This paper studies the possible development of an EU Terrorist Finance Tracking System (EU TFTS), which was announced in the February 2016 EU 'Action Plan to Strengthen the Fight Against Terrorist Financing'.[7] It will first recall the history of the US TFTP and the context in which demand for an equivalent in the EU emerged. It will then discuss the previous proposals as well as current ideas for an EU TFTS. Finally, it will provide concluding thoughts to help drive and shape renewed discussions on the creation of an EU TFTS.

In undertaking this study, the paper draws on interviews with individuals within the national ministries in several EU member states, officials from EU institutions (the European Commission and the Council Secretariat) as well as members of the European Parliament (MEPs) and several US experts on the TFTP. It also makes use of official documents, media reports, academic literature and previous research by the author.

European Commission on the TFTP, <http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/tftp/index_en.htm>, accessed 1 August 2016.

6. The number of (Article 10) information requests originating from EU member states rose from fifteen between 1 August 2010 and 31 January 2011 (a period of six months), to 94 between 1 February 2011 and 30 September (20 months) and 70 between 1 October 2012 and 28 February 2014 (seventeen months). The number of leads generated by the TFTP in response to Article 10 requests has also increased significantly, see European Commission, 'Joint Review Report of the Implementation of the Agreement Between the EU and the US on the Processing and Transfer of Financial Messaging Data from the EU to the US for the Purposes of the Terrorist Finance Tracking Program', /*SWD/2014/0264 final*/, 11 August 2014, <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52014SC0264>, accessed 17 August 2016.
7. European Commission, 'Communication from the Commission to the European Parliament and the Council on an Action Plan for Strengthening the Fight Against Terrorist Financing', COM(2016) 50 final, Februaru 2016.

I. The TFTP: An Overview

This section recounts the history of the TFTP. For analytical purposes, this is examined in three phases: first, the period between 2001 and 2006 when the TFTP remained an undisclosed US security programme; second, the period between 2006 and 2010 which saw a series of heated debates on the issue in the European Parliament; and third, developments following the adoption in 2010 of the EU–US TFTP Agreement. The purpose of this analysis is to identify issues and themes that may prove relevant to the decision-making process concerning an EU TFTS.

Top Secret: Designing and Regulating the TFTP (2001–06)

In the search for a comprehensive and innovative response to the 9/11 attacks, the US Treasury rapidly turned its attention to Belgium-based financial messaging service SWIFT (see Box 1). SWIFT had previously resisted requests by law enforcement agencies for access to its database, arguing that it would be easier to request this data directly from banks as SWIFT did not have the technical ability to undertake targeted searches of its database. After 9/11, however, SWIFT decided to cooperate in what it was initially imagined would be a short-term operation.[1]

The TFTP was set up within a few weeks of the 9/11 attacks, initiated by the CIA and then overseen by the US Treasury Department's Office of Foreign Assets Control (OFAC). The US law enforcement community took the view that the 'war on terrorism finance' should focus on pre-empting and apprehending potential terrorists before they could strike by connecting the dots of financial data.[2] In this context, financial investigators considered the SWIFT database to be the 'Rosetta Stone' of the financial sector.[3] Relatively unknown to the public, SWIFT handled the vast majority of messaging associated with international financial transactions, as well as some national ones. It was believed that these transactions could provide precious insights into global money flows and enable the detection and mapping of terrorist networks through a link analysis of transactions on an international level and across different financial institutions. As such, the TFTP held the promise of tracking down known terrorist suspects – most notably persons and entities related to Al-Qa'ida – and of pre-empting future attacks by uncovering as yet unknown networks and patterns.[4]

---

1. Juan C Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare* (New York, NY: PublicAffairs, 2013), pp. 45–65; Eric Lichtblau, *Bush's Law: The Remaking of American Justice* (New York, NY: Anchor Books, 2009), pp. 232–63.
2. Louise Amoore and Marieke de Goede, 'Governance, Risk and Dataveillance in the War on Terror', *Crime Law and Social Change* (Vol. 43, No. 149), pp. 152–53.
3. Eric Lichtblau and James Risen, 'Bank Data is Sifted by U.S. in Secret to Block Terror', *New York Times*, 31 August 2006.
4. For a more detailed analysis, see Mara Wesseling, Marieke de Goede and Louise Amoore, 'Data Wars Beyond Surveillance', *Journal of Cultural Economy* (Vol. 5, No. 1, 2012), pp. 49–66; Mara Wesseling, *The European Fight against Terrorism Financing: New Governance Practices and Professional Fields* (Oisterwijk: BOXpress, 2013).

Box 1: SWIFT, its Database and US Treasury Information Requests.

SWIFT (Society for Worldwide Interbank Financial Telecommunication) was created in 1973 by a group of 239 banks from fifteen countries to facilitate cross-border payments. It launched its services in 1977 via an automated, standardised messaging service and interface software. Today, the cooperative is the foremost financial messenger service in the world and claims to handle 80% of financial transfers worldwide. In 2001, when the TFTP was established, SWIFT connected 7,457 banks in 196 countries, and has since continued to grow. Today, 209 countries and territories across the world and more than 11,000 institutions are part of the SWIFT community.

More than 6.1 billion messages were transferred via SWIFT's messaging system, SWIFTNet FIN, in 2015. Each message contains information such as the names, addresses and the locations of both the sender and the receiver, as well as the amount of money involved. However, the structure of SWIFT's messenger service means that the data elements of interest to the US Treasury and the CIA cannot be delivered directly in their original form. In fact, the messages transferred through the system consist of 'envelopes' containing information on the sending institution, its Bank Identifier Code (BIC), the identification of the receiving institution, and the date and time of the message. The actual message – or 'the letter' – is encrypted and contains information that is entered, using standardised fields, by the sending institution, such as the transaction amount, the currency, the value, the date and the beneficiary's name.

To access SWIFT's financial payment messages, the US Treasury submits information requests that specify the types of messaging data and geographical areas in which it is interested and provides evidence of the necessity of this data for counterterrorism purposes. After approval by Europol, these datasets are then transferred to the US Treasury where financial investigators match and map data elements from terrorism investigations against the content of the 'letters' from the SWIFT database.

Initially, SWIFT held its data in a data-processing centre in Zoeterwoude in The Netherlands and in a mirror database in Virginia in the US. However, to cope with future capacity increases – and to improve its commercial appeal in some jurisdictions following the public disclosure of the TFTP in 2006 – SWIFT decided to review its global messaging system and to regionalise its data centres in 2007. The new architecture allowed for different data privacy arrangements to reflect regional privacy and data protection laws, and implied that from December 2009 European financial data records would only be held in Europe and would cease to be automatically available in bulk to US authorities. This organisational change meant that a new EU–US agreement was necessary if the continuity of the TFTP was to be assured.

Sources: SWIFT, Interview with Lazaro Campos, CEO of SWIFT, SWIFT Dialogue, Q2 2007, pp. 17–19; Belgian Privacy Commission, 'Opinion on the Transfer of Personal Data by the CSLR SWIFT by Virtue of UST (OFAC) Subpoenas', Advice 37/2006, 27 September 2006; European Union, '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', Official Journal of the European Union *(L 195/5, 27 June 2010).*

In the period prior to the public disclosure of the TFTP in June 2006, three themes had emerged during negotiations as being of significance both to the George W Bush administration and to SWIFT: the legality of the TFTP under US law; the design and limitations of the programme; and questions of oversight.

As cooperation with the US law enforcement agencies posed a reputational risk to its policy of political neutrality and confidentiality, SWIFT's primary concern was to have legal clarity in the US. Although the programme stretched the bounds of the US government's previous handling and use of financial data, US Treasury lawyers nonetheless considered it to be legal.[5] In response to SWIFT's requests, the US Treasury was nevertheless willing to offer a number of legal safeguards, in case the programme became public knowledge.[6] Most importantly, from October 2001 a system based on monthly administrative subpoenas (also known as national security letters) was created. This implied that data transfers had to be validated by the US Treasury and data were sent on a monthly basis. It also meant that the transfer of data was restricted to a set list of countries and that searches should have a proven connection with a terrorism investigation.

Further limitations to the US authorities' access to the database and additional privacy and data protection safeguards were negotiated by SWIFT and came into force from spring 2003. For instance, the access and scope of searches were further restricted by the requirements for additional information to justify requests for financial records held in the dataset. Searches also had to be linked to specific ongoing terrorism investigations.[7]

A third issue concerned the democratic and judicial oversight of the TFTP. The programme did not initially fall within the usual frameworks for oversight in the US, as formal approval of the programme by the US Congress was never requested and congressional oversight was minimal. Moreover, the US Treasury had opted to use administrative subpoenas instead of court-approved warrants based on a judicial review. However, some alternative forms of oversight were progressively created. Internal audits were undertaken by representatives of SWIFT (the so-called 'scrutineers') and the programme was also assessed by an external auditing firm.[8]

Transatlantic Controversy Over Legality, Privacy and Data Protection (2006–10)

On 23 June 2006, reports publicly revealing the existence of the TFTP first appeared in *The New York Times*, *LA Times* and *The Washington Post* and were soon picked up by global media

5. Zarate, *Treasury's War,* p. 52.
6. Wesseling, *The European Fight against Terrorism Financing*, p. 156–58.
7. Belgian Privacy Commission, 'Opinion on the Transfer of Personal Data by the CSLR SWIFT by Virtue of UST (OFAC) Subpoenas'.
8. Since the public disclosure of the TFTP, congressional oversight of the TFTP has taken the form of regular briefings to relevant committees and several hearings and reports. Additional layers of oversight by SWIFT's Board of Directors and the US government's Privacy and Civil Liberties Oversight Board were also added in later years. The review of data requests is now, in principle, undertaken by Europol.

outlets. Political outrage on both sides of the Atlantic followed, both over the programme itself and the act of disclosure. The European Parliament was particularly mobilised and expressed its great concerns, in particular regarding the legality of the programme and the compatibility of the TFTP with European privacy and data protection legislation.[9]

The year-long controversy that followed, which saw the EU in opposition to the US as well as strong disagreement among the EU institutions, led to a number of investigations, reports, (interim) agreements and ad hoc solutions. During the debates, three legal and technical issues emerged as crucial: the question of the programme's legality in Europe; its compliance with EU data protection and privacy law; and the democratic and judicial oversight of the programme.

In autumn 2006, the data protection authorities of both the EU and its individual member states undertook a number of investigations into possible violations of European data protection and privacy law through the allegedly illegal transfer of financial data from the SWIFT database to the US Treasury. The Belgian Privacy Commission, the Article 29 Working Party, and the European Data Protection Supervisor (EDPS) all found serious breaches of EU law as a result of their investigations.[10] They confirmed that SWIFT did not comply with European privacy and data protection law, specifically identifying the subpoenas of the US Treasury as mass requests of personal data that violated European data protection law.

To appease the programme's critics in Europe – which included politicians, data protection agencies and civil rights' movements[11] – the US and SWIFT undertook a number of ad hoc initiatives, such as the adoption by the US Treasury of a set of unilateral commitments that became known as the 'UST representations', and the moves to ensure that SWIFT adhered to the Safe Harbour Privacy Principles.[12] It was also rapidly decided that a clear legal framework, fully in line with European data protection and privacy standards, was needed to assure the

9. The EU adopted a number of directives and framework decisions to harmonise privacy and data protection laws in Europe as part of the Single Market project. These initiatives intend to avoid the disruption of international exchanges due to conflicting data protection rules and to ensure the same levels of protection everywhere in the EU. Data protection rules were negotiated between January 2012 and May 2016 and will enter into force in 2018.
10. Article 29 Data Protection Working Party, 'Opinion 10/2006 on the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)', 22 November 2006; EDPS, 'EDPS Opinion on the Role of the European Central Bank in the SWIFT Case', 1 February 2007.
11. See the complaint filed on 19 July 2006 by Privacy International with data protection regulators in more than 30 countries, avilable at <https://www.privacyinternational.org/node/534>, accessed 31 August 2016. In the US, on 23 June 2006 the American Civil Liberties Union (ACLU) condemned the programme, <https://www.aclu.org/news/aclu-says-government-spying-bank-records-further-abuse-power>, accessed 31 August 2016.
12. The Safe Harbour Privacy Principles were designed to bridge the gap between European and US data protection standards established in 2001. US companies adhering to the principles would receive certification and were allowed to transfer data for business purposes from the EU to the US. On 6 October 2015, the European Court of Justice invalidated the European Commission's Safe Harbour Decision, and in early 2016 the European Commission agreed to replace it with the EU–US Privacy Shield.

continued transfer of SWIFT data to US authorities. For this purpose, a specific legal agreement between the EU and the US had to be negotiated.

In practical terms, from 2007, European oversight over the handling of its citizens' personal data was also progressively incorporated into the programme by the US to satisfy European demands. First, as part of the UST representations, French counterterrorism judge Jean-Louis Bruguière was designated an 'Eminent European Person' by the European Commission and was authorised to review the procedures governing the handling, use and dissemination of the SWIFT data subpoenaed by the US Treasury. He issued two classified reports on the subject, the first in December 2008 and the second in January 2010. Both concluded that the TFTP had made a real contribution to counterterrorism efforts in the EU and offered detailed recommendations for further improvement.[13] Following the adoption of the EU–US TFTP Agreement in 2010, an interim and then a permanent 'overseer' were appointed (under the provisions of Article 12 of the agreement). Further oversight procedures were incorporated by tasking Europol with the review of the data requests (under Article 4.4).

TFTP Agreement: Towards Transparency and Accountability (2010–16)?

The first version of the EU–US TFTP Agreement was rejected by the European Parliament in early 2010. However, an amended version – addressing many of the issues that had been raised by the European Parliament as well as by certain member states, including Germany, Austria, Greece and Hungary[14] – was finally adopted in July and entered into force in August of the same year.[15] Nevertheless, even this revised version failed to address sufficiently some key issues raised by some MEPs. These areas included not only their principal objection – the transfer of personal data in bulk from the SWIFT database to US authorities – but also the length of the retention period and the criteria for deletion of the data (Article 6), the conditions for sharing

13. Jean-Louis Bruguière, 'Summary of the First Annual Report on the Processing of EU Originating Personal Data by the United States Treasury Department for Counter-Terrorism Purposes, Terrorist Finance Tracking Programme', December 2008; Bruguière, 'Second Report on the Processing of EU-Originating Personal Data by the United States Treasury Department for Counter Terrorism Purposes'.
14. Edna Dretzka and Stormy-Annika Mildner, 'Anything But SWIFT: Why Data Sharing is Still a Problem for the EU', American Institute for Contemporary German Studies Issue Brief No. 35, 2 May 2010; Jörg Monar, 'The Rejection of the EU-US SWIFT Interim Agreement by the European Parliament: A Historic Vote and its Implications', *European Foreign Affairs Review* (Vol. 15, 2010), pp. 143–51. The issues now included in the final version of the EU–US TFTP Agreement are: the verification of data requests by Europol (Article 4.2); an independent European overseer (Article 12); regular joint reviews (Article 13); the right to ask for access to personal data (Article 15); and the right to rectification, erasure or blocking (Article 16), including the availability of administrative and judicial redress (Article 18).
15. European Union, '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'.

information with third countries (Article 7), and public control and oversight (Article 12).[16] Debate concerning the transparency and accountability built into the EU–US TFTP Agreement has continued ever since (see Box 2).

In October 2010, only months after the agreement came into force, parliamentary questions were raised regarding the fact that the identity of the interim and permanent overseers of the TFTP – EU public officials – was to remain confidential for reasons of security, privacy and integrity.[17]

The next year, it became known that Europol had experienced difficulties guaranteeing the data protection rules set out in the agreement because US data requests were too general and too abstract to allow proper evaluation of their necessity.[18] A few months later, it became known that Europol had never rejected a request by the US Treasury, had authorised the transfer of bulk data on a daily basis, and did not know how much data had actually been transferred. The public statement made by the Europol Joint Supervisory Body (Europol's independent data protection supervisor) in response declared that 'this could indicate that it is not possible to fulfill all intended safeguards of Article 4'.[19]

In 2012, the European Court of Justice ruled on a demand by Dutch MEP Sophie in 't Veld that classified documents related to the opening of negotiations for the EU–US TFTP Agreement must be partly disclosed. This decision was upheld in 2014 in the subsequent appeal case filed by the Council of the EU.[20] That same year, it became public that there was a potential conflict of interest among the members of the EU review team, which comprised three members from the Directorate-General for Home Affairs of the European Commission and two individuals from the Joint Supervisory Body linked to Europol. This meant that, in effect, these two persons – both data protection experts, one from The Netherlands and the other from Belgium – were reviewing themselves.[21]

16. Mara Wesseling, 'Evaluation of EU Measures to Combat Terrorism Financing', analysis for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, April 2014, p. 17.
17. European Parliament, 'Question for Written Answer to the Commission by Sophia in 't Veld (ALDE), Alexander Alvaro (ALDE), Renate Weber (ALDE), Sonia Alfano (ALDE), Gianni Vattimo (ALDE), Louis Michel (ALDE) and Baroness Sarah Ludford (ALDE)', 15 October 2010, <http://www.europarl.europa.eu/sides/getDoc.do?type=WQ&reference=E-2010-8327&language=BG>, accessed 31 August 2016; see also John Rosenthal, 'Terrorist Finance Tracking Program Re-Starts Under Anonymous European Oversight', *Weekly Standard*, 20 September 2010.
18. Valentina Pop, 'EU Police Report Shows Holes in US Data Deal', *EU Observer*, 9 March 2011.
19. Europol, 'Europol Joint Supervisory Body on the Implementation of the TFTP Agreement: Public Statement', 14 March 2012.
20. Council of the European Union vs. Sophie in 't Veld, C-350/12 P, 'Judgement of the Court (First Chamber)', European Court of Justice, Luxembourg, 3 July 2014.
21. Nikolaj Nielsen, 'Terrorist Data Oversight Tainted by Potential Conflict of Interest', *EU Observer*, 20 December 2012.

Box 2: Subjects of Debate Since the EU–US TFTP Agreement Entered into Force in 2010.

- 2010: Continued secrecy about the identity of the European overseer.
- 2011: Europol allegedly violates the data protection rules of the agreement.
- 2011: Europol accused of rubber-stamping all US Treasury requests.
- 2012: Ruling of the European Court of Justice calls for the partial disclosure of secret TFTP documents.
- 2012: Potential conflict of interest among the members of the EU review team.
- 2013: Suggestion by Edward Snowden that the NSA has secret access to the SWIFT database leads to calls for the suspension of the EU–US TFTP Agreement.
- 2014: European Parliament's Moraes Report repeats calls for its suspension.
- 2015: EU Ombudsman denied access to European documents concerning the TFTP.

Fresh controversy followed in September 2013 when Edward Snowden stated that the National Security Agency (NSA) had secretly tapped into the SWIFT database.[22] While these claims have been denied by the US authorities, and although the European Commission did not see the need for further inquiries as a result of this assertion,[23] some MEPs were not convinced by the evidence provided that the US authorities had not breached the EU–US TFTP Agreement, and as a result, they called for its suspension.[24] Early in 2014, the Moraes Report into the various NSA surveillance programmes, undertaken by Claude Moraes MEP, reiterated the recommendation that the EU–US agreement be suspended.[25] An in-depth investigation by the Belgian and Dutch data protection authorities, however, did not find any proof to support claims that a third party had illegally acquired access to SWIFT's database.[26]

The latest struggle regarding the TFTP involves the refusal by the US, in 2015, to allow the European Parliament access to a document on the implementation of the TFTP written by Europol's own internal data protection committee, the Joint Supervisory Body. The technical modalities of the EU–US TFTP Agreement require Europol to obtain permission from the US

22. *Spiegel Online*, '"Follow the Money": NSA Spies on International Payments', 15 September 2013.
23. European Commission, 'EU-US Agreements: Commission Reports on TFTP and PNR', speech delivered by Cecilia Malmström, EU Commissioner for Home Affairs, 27 November 2013.
24. For instance, in the European Parliament's Resolution of 23 October 2013 on the Suspension of the TFTP Agreement as a Result of US National Security Agency Surveillance, 2013/2831(RSP).
25. European Parliament, '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', Committee on Civil Liberties, Justice and Home Affairs, 2013/2188(INI), 21 February 2014.
26. Belgian Privacy Commission, press release, 8 May 2014, only available in Dutch or French at <https://www.privacycommission.be/fr/news/les-instances-chargees-de-controler-le-respect-de-la-vie-privee-ne-constatent-aucune-infraction>, accessed 31 August 2016.

authorities before disclosing any records related to the TFTP. The US authorities have refused public access, arguing that the document contains US classified information and that the 'need to know' requirement had not been met. The EU Ombudsman Emily O'Reilly, together with other EU legislators and officials, objected to this decision, arguing that it prevented them from exercising sound democratic oversight of the TFTP in the EU.[27]

These critiques on the functioning of the TFTP today are highly relevant if a European equivalent of the programme is to be developed, especially in the light of the central role that might be played by Europol.

27. European Ombudsman, 'Presentation by the European Ombudsman, Emily O'Reilly – Decision of the European Ombudsman Closing the Inquiry into Complaint 1148/2013/TN as Regards Europol', 8 January 2015, <http://www.ombudsman.europa.eu/en/activities/speech.faces/en/58671/html.bookmark>, accessed 31 August 2016; Nikolaj Nielsen, 'US Gag Order on EU Police Agency Stirs Controversy', *EU Observer*, 8 January 2015.

II. A European Equivalent of the TFTP

One of the seemingly paradoxical outcomes of the heated debates in Europe over the TFTP has been the call for a European equivalent of the programme.[1] During the negotiations on the EU–US TFTP Agreement in spring 2010, MEPs and some EU member states reluctantly endorsed the agreement on the condition that the European Commission would look into the creation of its own legal and technical framework for the extraction of financial data within EU territory. This section recounts the arguments for the creation of an EU Terrorist Finance Tracking System (EU TFTS) in 2010, the proposals made to this end in 2013, and the renewed interest in such a system since 2015.

First Calls for an EU TFTS (2010)

In 2010, some MEPs, later joined by a number of EU member states, felt that the negotiations on the EU–US TFTP Agreement did not address all their concerns sufficiently. Consequently, they proposed instead a European equivalent to the TFTP which would permit the extraction of financial data within EU territory.

There were four main drivers behind this idea. First, an EU TFTS would negate the need for the systematic transfer of European financial data in bulk to the US. European and national data protection authorities considered the transfer of European citizens' personal financial data on such a massive scale to be one of the major problems of the TFTP and a potential breach of EU privacy and data protection legislation. Second, it was claimed that, despite the safeguards and joint reviews confirming their proper application, questions regarding the level of data protection and privacy remained, due to fundamental differences between US and EU legislation in this regard. These differences could only be fully addressed by an equivalent EU programme. Third, an EU TFTS would involve EU authorities conducting TFTP searches themselves, thereby affording them enhanced control not only over the TFTP's analytical and filtering practices, but also over European security decisions more broadly. As stressed by some MEPs and EU member states, this would avoid the outsourcing of EU security decisions and lead to a more balanced transatlantic alliance on security matters. Fourth, some member states saw additional value in developing an independent European system for tracking terrorist finance in the longer term,

1. Anthony Amicelle, *The EU's Paradoxical Efforts at Tracking the Financing of Terrorism: From Criticism to Imitation of Dataveillance* (Brussels: CEPS Paper in Liberty and Security, No. 56, August 2013); Wesseling, *The European Fight against Terrorism Financing*; Mara Wesseling 'Terrorism in Europe: The Decade-long Struggle over European Banking Data and a Policy Paradox', *Global*, <http://www.kib.be/articles/1206/terrorism-in-europe-the-decade-long-struggle-over-european-banking-data-and-a-policy-paradox>, accessed 17 August 2016.

as this would increase their ability to access relevant data and could strengthen their analytical capacities to track and identify terrorists through financial transactions.[2]

In response to these arguments, the EU–US TFTP Agreement included the provision (Article 11) that the European Commission would investigate the possible development of a sustainable, legally sound European solution to the issue of the extraction of financial messaging data within the EU (see Box 3). In practical terms, this meant that the Commission was invited to submit to the European Parliament and Council '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.[3]

Box 3: The Text of Article 11 of the EU–US TFTP Agreement.

1. During the course of this Agreement, the European Commission will carry out a study into the possible introduction of an equivalent EU system allowing for a more targeted transfer of data.
2. If, following this study, the European Union decides to establish an EU system, the United States shall cooperate and provide assistance and advice to contribute to the effective establishment of such a system.
3. Since the establishment of an EU system could substantially change the context of this Agreement, if the European Union decides to establish such a system, the Parties should consult to determine whether this Agreement would need to be adjusted accordingly. In that regard, U.S. and EU authorities shall cooperate to ensure the complementariness and efficiencies of the U.S. and EU systems in a manner that further enhances the security of citizens of the United States, the European Union, and elsewhere. In the spirit of this cooperation, the Parties shall actively pursue, on the basis of reciprocity and appropriate safeguards, the cooperation of any relevant international financial payment messaging service providers which are based in their respective territories for the purposes of ensuring the continued and effective viability of the US and EU systems.

2. The European Commission's impact assessment of 2013 also provides a detailed overview of problems relating to the design of an EU TFTS; see European Commission, 'Commission Staff Working Document', pp. 11–13.
3. European Union, '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', p. 3; European Parliament, 'European Parliament Resolution of 5 May 2010 on the Recommendation from the Commission to the Council to Authorise the Opening of Negotiations for an Agreement Between the European Union and the United States of America to Make Available to the United States Treasury Department Financial Messaging Data to Prevent and Combat Terrorism and Terrorist Financing', 5 May 2010, <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2010-0143&language=EN>, accessed 17 August 2016.

The 2013 EU TFTS Proposals

On 13 July 2011, the European Commission published a first Communication to the European Parliament and the Council entitled 'A European Terrorist Finance Tracking System: Available Options'.[4] It presented five different options and set out a roadmap for establishing an EU TFTS. Two of the options advanced by the Commission – situated at the extreme ends of the spectrum, which ranged from a purely centralised approach at the EU level and a purely national approach within each member state – were quickly excluded from further analysis on the grounds that they were undesirable from a political, legal and operational viewpoint. Three hybrid options remained and can be described as follows:

1. A coordination and analytical service provided by a centralised EU TFTS unit, with most tasks and functions carried out at the EU level.
2. An EU TFTS extraction service involving the establishment of a centralised EU TFTS unit that would handle the raw data but would lack analytical capabilities.
3. An upgraded financial intelligence unit (FIU) platform made up of all the FIUs of the EU member states and a newly created EU-level authority based on the current FIUs responsible for issuing requests for raw data to the provider(s) of international financial payment messaging services (the 'Designated Provider(s)').

These options for an equivalent EU system suggest an independent system for tracking terrorist finance through access to, and searches and analysis of, the data held by Designated Provider(s) and would therefore require a modification of the EU–US TFTP Agreement.

The roadmap set out by the European Commission's Directorate-General for Home Affairs (Directorate-General for Migration and Home Affairs since 2014) specified the possible scope of a future EU TFTS, which could include additional financial service providers beyond SWIFT and cooperation with third countries. The roadmap also set out the estimated costs of establishing such a system, which ranged from €33 million to €47 million to set up a centralised European or a hybrid system, and an estimated annual running cost of €7–11 million. The costs for a purely national system were estimated to be significantly higher, at €390 million to set up and €37 million to run each year.[5]

In late November 2013, a few months later than scheduled, the European Commission issued a 57-page impact assessment.[6] This included detailed scenarios and cost estimations based on the three hybrid models, an additional option of a data retention and extraction regime on EU territory that had been requested by some MEPs, and a 'status quo plus' option. Four principles guided the European Commission in assessing each option: necessity; proportionality; cost-

4. European Commission, 'A European Terrorist Finance Tracking System: Available Options', COM(2011) 429 final, 13 July 2011, <http://ec.europa.eu/dgs/home-affairs/what-is-new/news/pdf/1_act_part1_v15_en.pdf>, accessed 17 August 2016.
5. *Ibid*.
6. European Commission, 'Commission Staff Working Document', p. 57.

effectiveness; and respect of fundamental rights, most notably the right to privacy and personal data protection.

Surprisingly, the result of this impact assessment was the abandonment of an EU TFTS. The European Commission concluded in its second communication of 27 November 2013 that although each of the three short-listed options had advantages and disadvantages, 'the case to present at this stage a proposal for an EU TFTS is not clearly demonstrated'.[7] The impact assessment raised doubts as to the 'potential impacts in terms of fundamental rights and substantial additional costs' of the proposed new and broader system.[8] Then-European Commissioner of Home Affairs Cecilia Malmström confirmed that the Commission did not intend to table a specific proposal for an EU TFTS, since 'it would not bring any additional intelligence improvements as compared to the current situation'.[9]

Demands Since 2015 for an EU TFTS: A Complementary Instrument

Despite the rejection of the proposals for an EU TFTS in 2013, debates have occasionally occurred within some policy circles about the Single Euro Payments Area (SEPA). As specified in Article 4 of the EU–US TFTP Agreement, the US can request data from the Designated Provider (that is, SWIFT) which is stored within the territory of the EU. However, the agreement explicitly excludes the request of any data relating to the SEPA (Article 4.2 [d]). In practice, this means that under the current agreement, payments denominated in euros – for instance, a transfer denominated in euros from an account in Belgium or even from a non-euro EU state such as Sweden to an account in Germany – made through the SWIFT system in the SEPA format are not accessible to US authorities via the TFTP. Hence, some officials at both the national and European levels have argued that an EU TFTS could address the information gap with regard to intra-European financial transactions. This is the view of the EU's Counter-Terrorism Coordinator (CTC) Gilles de Kerchove, who has suggested that what is required is a system that can provide 'a tool to trace terrorist [financing] activities within and across SEPA countries for SEPA transactions'.[10] In his view, the inability to access SEPA data means fewer 'opportunities to detect and disrupt terrorist (support) networks, including the related financing activities'.[11]

7. 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.
8. European Commission, 'Commission Staff Working Document', p. 37.
9. European Parliament, 'MEPs Not Convinced by Positive Reports of Data Exchange Deals with the US', Committee on Civil Liberties, Justice and Home Affairs, European Parliament News, 27 November 2013, <http://www.europarl.europa.eu/news/en/news-room/20131127IPR27769/MEPs-not-convinced-by-positive-reports-of-data-exchange-deals-with-the-US>, accessed 8 September 2016.
10. EU Counter-Terrorism Coordinator, 'State of Play on Implementation of the Statement of the Members of the European Council of 12 February 2015, the JHA Council Conclusions of 20 November 2015, and the Conclusions of the European Council of 18 December 2015', 6450/16, Council of the European Union, 1 March 2016, p. 30, <http://data.consilium.europa.eu/doc/document/ST-6450-2016-INIT/en/pdf>, accessed 17 August 2016.
11. Nikolaj Nielsen, 'EU Wants to Give Police Greater Digital Access', *EU Observer*, 10 March 2016.

Moreover, as SWIFT covers only a small part of all payments in the EU, and given that all European financial services providers now use the SEPA format for euro transfers, additional Designated Providers could be included within an EU TFTS.[12] These could include:

- Other financial data-processing companies, competitors of SWIFT.
- (Pan-European) automated clearing houses.
- Domestic in-house payments systems, accessed via the bank's internal communication tools.
- Cross-border payments systems (correspondent banking) via banks' communication networks.
- E-money businesses such as PayPal.[13]
- Money transfer businesses such as Western Union and MoneyGram.

The idea of an EU TFTS has also been lent greater political salience by the recent major terrorist attacks on European soil.[14] The growing political urgency to tackle terrorism has prompted some MEPs and state actors to renew their demands for a European equivalent of the TFTP. For instance, in response to the terrorist attacks targeting the staff of French satirical weekly magazine *Charlie Hebdo* on 7 January 2015, and against the backdrop of concern across Europe over the radicalisation and departure (and return) of EU citizens to join terrorist organisations in Iraq and Syria, French Conservative MEP Rachida Dati actively relaunched the idea of an EU TFTS during a parliamentary questions session with the European Commission on 28 January 2015.[15] Dati repeated the need for an EU TFTS on many occasions, notably in her report on the prevention of radicalisation and recruitment of European citizens by terrorist organisations adopted by the European Parliament on 3 November 2015.[16] In her view, the creation of an EU TFTS should be part of a comprehensive approach to combating terrorism as it would enhance the EU's capacity to prevent terrorist attacks by providing additional intelligence for counterterrorism investigations.[17] In the wake of the terrorist attacks in Brussels on 22 March

12. Author interview with a national civil servant dealing with the TFTP, The Hague, 30 March 2016.
13. European Commission, 'Commission Staff Working Document', pp. 11–12.
14. Author interviews with an assistant to an MEP, Paris 23 March 2016 and a national civil servant dealing with the TFTP, The Hague, 30 March 2016.
15. Rachida Dati, 'Parliamentary Questions', 28 January 2015, <http://www.rachida-dati.eu/questions-parlementaires/relancer-la-creation-dun-systeme-europeen-de-detection-des-circuits-de-financement-du-terrorisme/#more-3155>, accessed 17 August 2016.
16. European Parliament, 'Report on the Prevention of Radicalisation and Recruitment of European Citizens by Terrorist Organisations', Committee on Civil Liberties, Justice and Home Affairs, 2015/2063(INI), 3 November 2015, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2015-0316+0+DOC+PDF+V0//EN>, accessed 31 August 2016.
17. *Reuters* reported that officials from France's Ministry of Finance complained about the lack of information sharing from the TFTP after the attacks on *Charlie Hebdo* in Paris in January 2015 and further attacks in November 2015. Another source quoted in the article added that there is a need to 'set up a way to obtain information from SWIFT. It is clearly a sensitive situation. But at the same time we cannot be satisfied that the information is available to some but not for European countries'. *Reuters*, 'U.S. Leaves French Requests on Terror Financing Information Unanswered: Source', 16 December 2015.

2016, new declarations were made calling for the implementation of the February 2016 EU 'Action Plan to Strengthen the Fight Against Terrorist Financing' to be sped up.[18]

These attacks are specific examples of the broader need – highlighted by national officials and law enforcement agencies – for greater cross-border cooperation and of the changed nature of terrorism and its financing since the adoption of the EU–US TFTP Agreement in 2010. The terrorism threat pictures in the EU and the US are different, with the EU facing an evolving and increased threat from European citizens returning from Syria or Iraq or from those inspired by the ideology of Daesh (also known as the Islamic State of Iraq and Syria, ISIS or IS) and willing to carry out attacks on European soil. It is these considerations that prompt calls to reconsider establishing an EU TFTS.

Addressing these two issues, the EU Action Plan states that the European Commission will take forward the initiative for 'a possible European system which would complement the existing EU–US TFTP Agreement by tracing transactions excluded under the mentioned agreement'.[19] In this context, the objective is to publish a communication assessing this option by December 2016 at the latest.

The US government has yet to establish a formal public position regarding this initiative. Yet, in more general terms, a recent congressional report states that 'U.S. policymakers underscore the importance of maintaining close U.S.-EU counterterrorism cooperation in light of the Islamist terrorist threat and the foreign fighter phenomenon.'[20] Furthermore, informal comments of US-based experts on the TFTP suggest that the US would consider an EU TFTS to be of great mutual value and would support its creation under three conditions: a European equivalent system should be complementary and ideally would not require changes to the existing EU–US TFTP Agreement; an EU TFTS should be reciprocal and offer the US similar arrangements for information exchange as are available to the EU under the current EU–US TFTP Agreement; and the system should operate in a robust and timely manner.

In the light of these latest developments, the remaining section highlights some potential opportunities and challenges regarding the formation of an EU TFTS (see Table 1).

18. European Council, 'Joint Statement of EU Ministers for Justice and Home Affairs and Representatives of EU Institutions on the Terrorist Attacks in Brussels on 22 March 2016', press release 158/16, 22 March 2016.
19. European Commission, 'Communication from the Commission to the European Parliament and the Council on an Action Plan for Strengthening the Fight against Terrorist Financing', p. 12.
20. Kristin Archick and Paul Belkin, 'European Security and Islamist Terrorism', Congressional Research Service Insight, 18 July 2016.

Table 1: A Comparison of Previous and Current Debates about an EU TFTS.

	First EU TFTS Proposal (2010–13)	**Second EU TFTS Proposal (2015–16)**
Primary arguments for an EU TFTS	Avoid bulk transfers of financial data. Ensure full conformity with EU data protection and privacy law. Ensure sovereignty over security decisions and enhanced equality in transatlantic security cooperation.	Step up EU fight against terrorism and disrupt more terrorist networks by closing the SEPA data gap.
Aim	Replace the EU–US TFTP Agreement: an EU TFTS would allow data retrieval and filtering on EU soil.	Complement the EU–US TFTP Agreement: an EU TFTS would add value to the existing TFTP Agreement through access to previously inaccessible data.
Proposed design	Three hybrid models that would allow the limitation and filtering of transferred data.	Focus on intra-European (SEPA) data that is not covered by the EU–US TFTP Agreement. Possible addition of Designated Providers.

III. Food for Thought: Debating an EU TFTS

The renewed interest in an EU TFTS that is a complementary tool to the existing EU–US TFTP Agreement, and which focuses on intra-European payments and possibly also includes data from Designated Providers other than SWIFT, raises a number of new questions and invites further reflection on issues raised in earlier debates. This section proposes six questions to stimulate and frame debate on an EU TFTS.

1. What is the Expected Added Value of an EU TFTS in Combating Terrorism?

The first question – and the one at the centre of current debates – concerns the intended purpose and expected added value of an EU TFTS. For the US, the creation of the TFTP in 2001 addressed a perceived intelligence deficiency in monitoring (global) wire transfers and the programme is considered a vital tool for identifying terrorists' activities and thereby preventing future attacks.[1] More recently, US and European authorities have also stressed the value of the TFTP for gathering intelligence and evidence *after* a terrorist act has taken place. Further value can be found in the greater speed and efficiency with which the TFTP is able to provide information for law enforcement agencies in comparison with other methods for gathering financial data. Law enforcement agents argue that querying a database is less complicated and time consuming than pursuing financial intelligence through bilateral cooperation, mutual legal assistance (MLA) arrangements and European evidence warrants, which are not always possible to obtain or implement.[2] Moreover, the TFTP avoids the need to issue an MLA request for the relevant records of every bank in every EU member state, as most of this data is collected in the databases of SWIFT. TFTP analysts submit terrorism-related research queries that are run against sets of raw SWIFT data, which may then lead to the identification of both known or unknown suspects as well as irrelevant false positives. Such a capability is not easily replicated using other data: for example, although the data included in Suspicious Activity Reports (SARs)[3] – which are gathered by national FIUs under the requirements of the EU's Fourth Anti-Money Laundering and Countering the Financing of Terrorism (4th AML/CFT) Directive – are to some

1. Justin Santolli, 'The Terrorist Finance Tracking Program: Illuminating the Shortcomings of the European Union's Antiquated Data Privacy Directive', *George Washington University of International Law Review* (Vol. 40, 2008), pp. 553–82.
2. European Commission, 'Commission Staff Working Document', p. 11.
3. EU member states use different names for suspicious transaction reports – Suspicious Activity Report (SAR), Suspicious Transaction Report (STR), Unusual Transaction Report (UTR), Currency Transaction Report (CTR) – and they may cover different practices ranging, for instance, from compulsory reporting of all transactions above a certain amount to reporting based on risk-based monitoring software and professional expertise. The UK uses SARs, which often include extensive analysis by the reporting entities of suspicious activity.

extent similar to raw SWIFT data, the information available depends on the commitment of reporting entities and the quality of the reports they file.

But while law enforcement agencies may endorse the TFTP, it is virtually impossible to predict the added value of an EU TFTS in terms of the number of prevented terrorist acts or successful prosecutions for terrorism offences. Research into the TFTP has shown that it is difficult – at least for external observers – to pinpoint its exact contribution to those examples that have been made public.[4] Both Europol and the US Treasury have increased their reporting on the results of the existing EU–US TFTP Agreement. For instance, Europol claims that the Paris attacks on 13 November 2015 prompted 28 requests in relation to the TFTP, which in turn resulted in 799 intelligence leads.[5] It remains less clear, however, what is understood by an 'intelligence lead' and to what extent the given numbers indicate success or effectiveness. It is also difficult to assess whether individuals whose connections to terrorist organisations have been identified through the TFTP might have been uncovered by other means, or whether the TFTP is the sole means by which they have been discovered.

In addition, it remains ambiguous whether the value of the programme lies primarily in the prevention of terrorist attacks, as the US Treasury initially claimed, or in the identification and prosecution of suspected terrorists (even where concrete plans for attacks are not known), or in the analysis of terrorist attacks that have already happened. While it is complex to calculate the numbers of cases in which the TFTP played a central role in preventing an attack or in the prosecution of a (would-be) terrorist, it is important to clearly define whether an EU TFTS would be a primarily preventive or reactive instrument. In other words, is the creation of an EU TFTS worth the investment if its added value is mainly in post-event analysis rather than the disruption of planned attacks?

It must also be noted that the perceived added value of an EU TFTS will fluctuate as the threat picture changes. In 2013, while some member states noted 'the added-value of an EU internal system, a considerable number of Member States was much more sceptical'.[6] The European Commission also concluded that 'it appears difficult to justify the EU added value of the introduction of a new and broader system'.[7] Today, however, an EU TFTS might be deemed more valuable. There have been significant changes to the level of terrorist threat as well as to its profile; for example, the increase in the number of jihadists now travelling to the Middle East from Europe (and back), where they already have a financial profile, creates opportunities for financial intelligence collection based on SEPA transaction data. The broader European political context and the urgency of fighting terrorism have also changed since 2013. Due to the increase of attacks within the EU – in Paris, Brussels and Nice as well as a series of smaller-scale attacks carried out by individuals who pledged alliance to Daesh – both the demands

4. Wesseling, *The European Fight against Terrorism Financing.*
5. Europol, European Counter Terrorism Centre infographic, 25 January 2016, <https://www.europol.europa.eu/content/ectc-european-counter-terrorism-centre-infographic>, accessed 31 August 2016.
6. European Commission, 'Commission Staff Working Document', p. 5.
7. *Ibid*., p. 37.

from law enforcement authorities for improved access to financial data and the political will to undertake action have increased. These factors combine with the changed conceptualisation of an EU TFTS, which has shifted from a system aimed at limiting the transfer of data to the US to a complementary system that would enable access to a set of data currently excluded from analysis, SEPA payments.

Added value can also be expressed in terms of procedural efficiency. As stated above, searching for transactions and financial connections via the TFTP is considered relatively fast and straightforward, but further analysis is needed to ascertain whether similar advantages can also be obtained by other existing means – such as through increased cooperation among FIUs or through the information exchange tools at their disposal. The February 2016 EU 'Action Plan to Strengthen the Fight against Terrorist Financing' also proposes mandating access to centralised bank and payment account registers, as well as electronic data retrieval systems. It is worth analysing whether such a tool – which registers all the national bank accounts listed to one person – could offer efficiency gains without the creation of an EU TFTS.

Similarly, one could think of other tools for more rapid and fluid information sharing between public and private actors. Section 314(a) of the US PATRIOT Act enables local, federal, state and foreign (EU) law enforcement agencies to reach out, through FinCEN (the US FIU), to more than 43,000 points of contact at more than 22,000 financial institutions in order to identify the accounts and transactions of those who may be involved in terrorism.[8] As David Carlisle observes: 'The process saves law enforcement agencies valuable time and resources by allowing them to survey the US financial sector quickly for investigative leads not available elsewhere; and it provides the private sector with concrete information about individuals and entities whose transactions the security services believe warrant scrutiny'.[9] The creation of a similar tool for obtaining information is possible under the EU's 4th AML/CFT Directive and could be developed at national or transnational level with the appropriate legal safeguards as an alternative to the creation of an EU TFTS.

In more practical terms, debates about the desirability of an EU TFTS should also consider the question of how crucial SEPA payment data might be in uncovering and tracing current and future terrorist cells and their networks. Gaining access to intra-European financial transfer data seems to match the various terrorist threats with which EU member states are currently confronted. It may reveal cross-border payments made to individuals inspired by Daesh to help to prepare attacks on European soil, or uncover intentions to join the battlegrounds in Syria and Iraq. More generally, access to SEPA data could provide insights into the activities of separatist or other violent movements acting within and across Europe. An EU TFTS might therefore expose those less cautious individuals who make use of the formal financial services system in Europe and may be unaware that each of their electronic payments (including money transfers and

8. Financial Crimes Enforcement Network (FinCEN), Department of the US Treasury, 'FinCEN's 314(a) Fact Sheet', <https://www.fincen.gov/statutes_regs/patriot/pdf/314afactsheet.pdf>, accessed 2 August 2016.
9. David Carlisle, 'Targeting Security Threats Using Financial Intelligence: The US Experience in Public–Private Information Sharing Since 9/11', *RUSI Occasional Papers* (April 2016).

e-payments) leaves a trace. Moreover, the incorporation of other financial services companies that have previously been used by (suspected) terrorists into an EU TFTS will increase the volumes as well as the variety of information that can be analysed and will offer extended possibilities for mapping social networks. It should, however, be remembered that self-financed terrorist cells, low-budget, lone-wolf terrorists and terrorist financiers using other methods of financing such as cash payments, the use of cryptocurrencies, loans and prepaid cards will remain hidden even from an expanded formal EU TFTS.

2. Are the Costs of an EU TFTS Proportional to the Expected Benefits?

The financial implications of developing and maintaining an EU TFTS will likely be a major concern. The 2013 proposal estimated that the cost of setting up a hybrid model EU TFTS would range from €33 million to €47 million, while annual operating costs ranged between €7 million and €11 million, depending on the chosen model. The answer to the question of whether these costs are proportional to the expected benefits may vary over time. In 2013, it was not considered cost effective to allocate such significant sums to the creation of a separate European system. Costs were deemed an important reason for maintaining the status quo.[10]

However, as mentioned above – the new framing of the EU TFTS as a complementary system accessing new sets of data and the current urgency of combating terrorism and avoiding new attacks on European soil in the near future constitute a radically different political context that may have increased EU member states' willingness to invest in a European system. Nevertheless, the cost-benefit analysis of an EU TFTS – especially in comparison with the current situation, where the costs are largely paid by the US – will play an important role in upcoming discussions. In this context, alternative and more cost-effective approaches to the creation of an EU TFTS – based on the expansion or adaptation of existing European and national agencies, programmes and tools – should definitely be taken into account.[11]

3. How Will an EU TFTS Affect Relations with the US and Other Third Countries?

The creation of a European system may also have implications for the current EU–US TFTP Agreement and future relations in this field with the US. Article 11 of the EU–US TFTP Agreement commits the US to providing assistance and advice in the creation of an EU TFTS, and to cooperating with it once established.

One key question is whether the creation of an EU TFTS would require an adjustment of the existing EU–US TFTP Agreement or the development of a separate legal framework. Focusing on the interconnection of an EU TFTS, current discussions seem to suggest the latter, as it would avoid the political risk of reopening debates over a potentially sensitive security initiative. A separate legal framework would likely have to take account of the desire on the part of the US and other third countries outside the EU and SEPA to issue their own requests in order

10. European Commission, 'Commission Staff Working Document', p. 37.
11. Author interviews with two national civil servants dealing with the TFTP, The Hague, 30 March 2016, and one European civil servant, Brussels, 31 March 2016.

to gain access to intra-European transactions. The current EU–US TFTP Agreement contains two provisions on reciprocity (Articles 9 and 10). One can therefore imagine that a similar provision on reciprocity would be included in a new framework, allowing for search requests to be submitted by the US or other third countries concerning intra-European data.[12] This in turn raises the question as to whether the sharing of personal data about EU citizens and European security analysis under an EU TFTS would be covered by, for instance, the provisions of the EU–US Data Protection 'Umbrella Agreement', signed in June 2016.[13]

4. Is an EU TFTS Compatible with EU Fundamental Rights?

In 2013, the demand for an EU TFTS was driven by the prospect of enhanced data protection and privacy safeguards, two aspects which were duly considered in the 2013 impact assessment. But these civil rights arguments seem to have disappeared from the current discussions, even though, as the European Commission stated very clearly in its 2013 assessment, 'By its nature, a TFTP like system requires the use and processing of bulk data which is privately held and collected by service providers for a different purpose than law enforcement'.[14] Hence, even if data is not transferred to the US, an EU TFTS would still constitute a form of mass surveillance. In fact, if the EU TFTS is to address the SEPA information gap, the amount of data collected would increase, possibly substantially. Under EU law, this interference could, however, be justified in the interest of national security and public safety.

Responding to the findings of the 2013 impact assessment, the European Data Protection Supervisor (EDPS) stressed that the study of the formation of an EU TFTS should also take into account the impact of the EU–US TFTP Agreement on data protection rights and the conclusion of the Joint Supervisory Body that it might be impossible to fulfil all the intended safeguards under Article 4 of the agreement. The EDPS pointed out that the assessment did not address whether the EU–US TFTP Agreement was necessary and proportionate and questioned whether the data requests made under the existing agreement were indeed limited in their scope.[15] The EDPS also noted that the impact assessment did not give full attention to the positive impact on citizens' fundamental rights of the options called 'status quo plus' (amending the existing

12. Author interview with a European civil servant dealing with the TFTP, Brussels, 31 March 2016.
13. The EU–US Data Protection Umbrella Agreement puts in place a comprehensive data protection framework for criminal law enforcement (including terrorism) cooperation between police and criminal justice authorities of EU member states and the US federal authorities covering all personal data. See European Union, 'Agreement Between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection and Prosecution of Criminal Offenses' ("Umbrella Agreement")', signed 2 June 2016, <http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf>, accessed 31 August 2016.
14. European Commission, 'Commission Staff Working Document', p. 16.
15. European Data Protection Supervisor, 'EDPS Comments on the Communication from the Commission to the European Parliament and the Council on a European Terrorist Finance Tracking System (TFTS) and on the Commission Staff Working Document – Impact Assessment Accompanying the Communication from the Commission to the European Parliament and the Council on a European Terrorist Finance Tracking System (TFTS)', 17 April 2014, p. 4.

agreement) and the 'zero option' (terminating the current agreement).[16] All these fundamental questions remain relevant in relation to a European system: is a complementary EU TFTS necessary and proportionate? And how would it overcome the existing technical obstacles to narrowing data requests?

Finally, if the EU TFTS were extended to cover organised crime (as was desired by some EU stakeholders and member states in 2013) or allow real-time access to data, there would be significant implications for the upholding of human rights, with many more individuals likely to be investigated on the basis of false suspicions.[17]

5. How Should Democratic and Judicial Oversight Over an EU TFTS be Organised?

The 2010–13 debates about creating an EU TFTS were largely motivated by the need to assure full compliance with EU data protection legislation. According to the EDPS, the EU–US TFTP Agreement is problematic in terms of political accountability as there is an absence of judicial oversight by the EU.[18] Oversight is performed by the EU overseer, Europol, Europol's Joint Supervisory Body and an EU review delegation. However, as discussed in Chapter II, various media reports since the EU–US TFTP Agreement came into force suggest that none of these authorities has performed this function as effectively as intended, negatively impacting the transparency and accountability of the programme. This point has also been stressed by the EDPS, who stated that 'verification by Europol should not be considered as a sufficient safeguard, as this task should be carried out by a judicial authority'.[19] Should a complementary EU TFTS be established, thorough reflection on arrangements for sound democratic and judicial oversight and regular review would therefore be needed. Depending on its design, a European oversight committee might be necessary, either imbued with specific powers of inquiry or tasked with a coordinating function that brings together the various national oversight bodies. This raises the question of who should assure this oversight – for example, appointed (anonymous) individuals, Europol, Eurojust, MEPs, representatives of the EDPS, or national data protection authorities – and what powers they should have.

However, in considering the options for increasing EU-based access to financial data, it may be noted that in their functions of gathering, analysing, requesting and disseminating specific financial information, FIUs are already subject to democratic and judicial control and European

16. *Ibid*.
17. European Commission, 'Commission Staff Working Document', p. 35.
18. Cian C Murphy, *EU Counter-Terrorism Law: Pre-emption and the Rule of Law* (Oxford: Hart Publishing, 2012), p. 158.
19. EDPS, 'EDPS Comments on the Communication from the Commission to the European Parliament and the Council on a European Terrorist Finance Tracking System (TFTS) and on the Commission Staff Working Document – Impact Assessment Accompanying the Communication from the Commission to the European Parliament and the Council on a European Terrorist Finance Tracking System (TFTS)', p. 7.

privacy legislation.[20] This might be another factor in favour of extending the scope and tasks of established bodies such as FIUs, instead of creating an EU TFTS.

An EU TFTP would also need to address the issues of (EU) citizens' right of access to information, and the right to rectification and redress. It has become clear that the legal arrangements included in the EU–US TFTP Agreement to ensure access to one's own personal information and to judicial and administrative redress appear to be of limited effect. The fact that TFTP searches are strictly confidential, being used for intelligence gathering purposes, makes it unlikely that data subjects receive confirmation that their data have been processed – thereby preventing them from substantiating their request for access or redress. However, it is known from other counterterrorism programmes that occasionally individuals have been wrongly identified as terrorist suspects or had the same name as a suspected terrorist. The direct supervision of EU TFTS requests by national data protection authorities or the EDPS could ensure data subjects' access to appropriate administrative and judicial redress in such cases.

6. What Are the Broader Societal Implications of an EU TFTS?

In addition to economic and legal considerations, the daily operational aspects of the TFTP and a future European equivalent also merit reflection. The TFTP does not entail politically controversial investigative methods such as data mining or profiling, but is based on less-debated practices of link analysis and network mapping. Before deciding on the formation of an EU TFTS, public discussion is needed on the effects of mapping social networks on the basis of vast numbers of financial transactions and the extension of 'suspicion by association'. What sort of transaction is to be considered suspect? Which links in the network analysis are considered significant? What are the boundaries of a suspect network?[21] Does the selection of certain categories of data and the practice of link analysis amount to structural discrimination? How can the inadvertent victimisation of innocent individuals through pre-emptive policing be avoided? These practical questions are important for understanding the ethical and societal aspects of security initiatives such as the TFTP and need to be openly discussed in order to strengthen the legitimacy of an EU TFTS, should it be created.

20. European Union, 'Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, Amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and Repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC', *Official Journal of the European Union* (L 141/73, 5 June 2015), <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2015_141_R_0003&from=ES>, accessed 2 August 2016.
21. De Goede, *Speculative Security,* pp. 67–68.

IV. Conclusion

THIS PAPER HAS highlighted a set of themes and issues to be taken into account should an EU TFTS be established. In the search for an effective response to the phenomenon of Daesh and its ability to recruit European fighters and supporters, debates have focused on a system that complements the US TFTP, and which incorporates currently excluded financial data from the SEPA.

EU member states are also considering other options for the collection and analysis of financial intelligence by the EU, based on expanding existing means to obtain similar results. These alternatives may prove to be more cost effective, quicker to implement and easier to adopt, as they are already embedded in European legal and oversight frameworks assuring the respect for fundamental rights, such as the protection of personal data, private life, the right to good administration and effective remedy.

Depending on its design, however, an EU TFTS may provide benefits in terms of intelligence or efficiency that other arrangements cannot offer. This is likely to be the subject of intensive debate among EU member states in the coming months as the EU grapples with the changing terrorist threat picture.

About the Author

Mara Wesseling is a Research Associate at the Centre des Sociologie des Organisations (Sciences Po Paris/CNRS). She has studied European counterterrorism financing policies for over a decade. Her research in this area focuses on risk-based approaches, effectiveness, international coordination and public–private cooperation. In 2013, Mara successfully defended her PhD thesis entitled 'The European Fight against Terrorism Financing: Professional Fields and New Governing Practices' at the University of Amsterdam. She has provided expertise on combating terrorism financing to the European Parliament, the OECD, the Dutch Ministry of Finance and to private companies. Previously she held positions at the European Institute of Public Administration (EIPA) and the University of Amsterdam.