Combating the financing of terrorism has been a core component of the global War on Terror that began after the 9/11 terrorist attacks. This book shows how the fight against terrorism financing has taken shape and become important in Europe. An examination of two case studies – the EU’s Third AML/CFT (Anti-Money Laundering and Combating the Financing of Terrorism) Directive and the Terrorist Finance Tracking Program – sheds light on the emerging structures of European security governing, characterized by increased public-private cooperation and the almost invisible new governing practices involving the risk and link-based analysis of massive sets of personal financial data. In this dissertation the author presents a critical reflection on and discussion of the societal and political implications of these measures.
The European Fight against Terrorism Financing:
Professional Fields and New Governing Practices

ACADEMISCH PROEFSCHRIFT

ter verkrijging van de graad van doctor

aan de Universiteit van Amsterdam

op gezag van de Rector Magnificus

prof. dr. D.C. van den Boom

ten overstaan van een door het college voor promoties ingestelde
commissie, in het openbaar te verdedigen in de Agnietenkapel

op dinsdag 3 september 2013, om 12.00 uur

door

Mara Wesseling

geboren te Amsterdam.
Promotores: Prof. dr. M. de Goede
Prof. dr. M.J. Wintle

Overige leden: Prof. dr. L. Amoore
Dr. L.A. Bialasiewicz
Prof. dr. M.W.G. den Boer
Prof. dr. M.E. Glasius
Dr. V. Mamadouh

Faculteit der Maatschappij- en Gedragswetenschappen
# Contents

ACKNOWLEDGEMENTS 5  
LIST OF ILLUSTRATIONS 8  
LIST OF ACRONYMS AND ABBREVIATIONS 9  
THE EUROPEAN FIGHT AGAINST TERRORISM FINANCING 11  
   1.1 LAPLACE’S DEMON AND GOVERNING THE FUTURE 11  
   1.2 COMBATING TERRORISM FINANCING: A WAR THAT NO ONE SAW 13  
   1.3 EUROPEAN POLICIES FOR COMBATING TERRORISM FINANCING 16  
   1.4 ACADEMIC DEBATES ON THE EUROPEAN FIGHT AGAINST TERRORISM FINANCING 19  
   1.5 CHAPTER OVERVIEWS 24  
THE EUROPEAN FIELD OF GOVERNING 27  
   2.1 INTRODUCTION 27  
   2.2 THEORIZING THE EUROPEAN UNION 30  
   2.3 (FINANCIAL) SURVEILLANCE STUDIES AFTER 9/11 35  
   2.4 GOVERNMENTALITY 42  
   2.5 FIELD THEORY 46  
   2.6 METHODOLOGY 51  
      2.6.1 Case Studies 52  
      2.6.2 Documentary Research and Textual Analysis 53  
      2.6.3 Elite Interviewing 57  
   2.7 MAPPING THE PARTICIPANTS OF THE PROFESSIONAL FIELDS 61  
      2.7.1 The Professional Field Map of the SWIFT Affair 62  
      2.7.2 The Professional Field Map of the EU’s Third Directive 63  
      2.7.3 Governmentality and the EU’s Fight against Terrorism Financing 65  
A GENEALOGY OF THE EUROPEAN FIGHT AGAINST TERRORISM FINANCE 69  
   3.1 INTRODUCTION 69  
   3.2 GENEALOGY AND THE GENEALOGICAL METHOD 72  
   3.3 THE CONSTRUCTION OF TERRORISM FINANCING AS A NATIONAL SECURITY ISSUE 76  
   3.4 THE EMERGENCE OF DOMINANT DISCOURSES ON TERRORISM FINANCING 85  
   3.5 THE BIRTH OF THE EUROPEAN FIGHT AGAINST TERRORISM FINANCE 93  
TRANSATLANTIC PERSPECTIVES ON THE ‘SWIFT AFFAIR’ 97  
   4.1 ‘BANK DATA IS SIFTED BY U.S. IN SECRET TO BLOCK TERROR’ 97  
   4.2 (DE)POLITICIZATION OF THE SWIFT AFFAIR 101  
   4.3 THE US DEBATE 105  
      4.3.1 Moment of Openness: an Emerging Debate During the Weekend 105  
      4.3.2 Politicization: Privacy and Legal Concerns 107  
      4.3.3 Depoliticization: Shoot the Messenger! 111  
      4.3.4 Swift Depoliticization 115  
   4.4 THE EU DEBATE 119  
      4.4.1 Moment of Openness: the Mobilization of the European Parliament 120
4.4.2 Politicization: Privacy and the Data Protection Law
4.4.3 A Series of Ad Hoc Solutions Depoliticizing the ‘SWIFT Affair’
4.4.4 Repoliticizing the TFTP
4.5 CONCLUSION

SWIFT: OPENING THE “BLACK BOX”

5.1 INTRODUCTION
5.2 WE CANNOT KNOW, WE SHOULD NOT KNOW, WE DO NOT WANT TO KNOW
5.3 OPENING THE BLACK BOX
  5.3.1 Obtaining ‘the Rosetta Stone for Financial Data’
  5.3.2 Safeguards Saving the TFTP
  5.3.3 Analysing Six Degrees of Separation . . .
5.4 RESULTS AND “SUCCESSES”
5.5 CONCLUSION

THEATRE OF COMPLIANCE: THE THIRD AML/CFT DIRECTIVE IN PRACTICE

6.1 INTRODUCTION
6.2 THE DEVELOPMENT OF THE EU’S ANTI-MONEY-LAUINERING DIRECTIVES
  6.2.1 The First Anti-Money Laundering Directive
  6.2.2 The Second Anti-Money Laundering Directive
  6.2.3 The Third Anti-Money Laundering/Combating the Financing of Terrorism Directive
6.3 THEATRE OF COMPLIANCE
6.4 THE STAGE
6.5 SCRIPT AND SCENARIOS
  6.5.1 Customer Due Diligence Part One: Customer Identification
  6.5.2 Customer Due Diligence Part Two: Transaction Monitoring
6.6 PERFORMANCE
6.7 CONCLUSION

FINANCIAL SURVEILLANCE IN EUROPE

7.1 EVALUATING TEN YEARS OF WAR ON TERRORISM FINANCING
7.2 TWO CASES, ONE PHILOSOPHY
7.3 PUBLIC-PRIVATE COOPERATION: THE PROLIFERATION OF PRIVATE SECTOR POWER
7.4 POWER EFFECTS OF RISK- AND LINK-BASED GOVERNANCE PRACTICES
7.5 THE COLLECTION OF PERSONAL DATA: GOING BEYOND THE PRIVACY DEBATE
7.6 AN INTELLIGENCE FROM WHICH THE HUMAN MIND WILL ALWAYS REMAIN INFINITELY REMOVED?

ANNEX 1: OVERVIEW OF CONDUCTED INTERVIEWS
ANNEX 2: LIST OF INVESTIGATED NEWSPAPERS
NEDERLANDSE SAMENVATTING
REFERENCES
NOTES
Acknowledgements

This PhD dissertation is part of the British-Dutch research project, ‘Data Wars: New Spaces of Governing in the European War on Terror’, which is being carried out by research teams at Durham University and the University of Amsterdam and is funded by the Nederlandse organisatie voor Wetenschappelijk Onderzoek (NWO) and the Economic and Social Research Council (ESRC). The aim of this research project is to map and analyse the reconfigured spaces of governing that are emerging through the deployment of travel and financial data for pre-emptive security action in the European fight against terrorism. My involvement in the project started in 2008 at the European Studies Department of the University of Amsterdam and, due to the promotion of my supervisor half-way through the project, ended at the Political Science Department of this same university. Throughout the project many people and institutions accompanied and assisted me in realising this PhD project.

First and foremost, I am infinitely grateful for the time, energy, and patience that my PhD supervisor, Marieke de Goede, has given me over the years. She helped me conduct my research in the best conditions possible and I learned a lot as she guided me step by step through the different (theoretical, practical, emotional) aspects of academic work. She stimulated me to participate in conferences and contribute to articles. I also have great memories of the fieldwork we carried out together in Brussels. Enthusiasm, involvement, a strong ability to provide constructive feedback, and of course great expertise in financial security questions are among the many qualities she has as a supervisor. I feel fortunate to have had the opportunity to write my dissertation under her supervision, and her work and achievements have been a continuing inspiration in many ways. I also wish to thank all of my colleagues in the Political Science Department, which provided an intellectually stimulating and active workplace. I especially appreciated collegial discussions with Chris Bickerton, Jasper Blom, Jeroen Doomerik, Jesse Hoffman, Merijn Hoitink, Paul van Hooft, Marlies Glasius, Eefje Steenvoorden, Stephanie Simon, and Floris Vermeulen.

Michael Wintle has been a constant supporter of the Data Wars project, and I am thankful for the time and effort he has put into the supervision of my dissertation. He has read each of the chapters with a great eye for detail regarding their form and content and his suggestions greatly improved the readability of this dissertation. He has also facilitated the start and end phases of my work as a PhD student in the European Studies Department and has given me precious advice on my future steps in the academic world. At the same time, I also wish to thank all my European Studies colleagues, who have provided me with a supportive and enriching intellectual community, including Huub van Baar, Luiza Bialasiewicz, Marjet Brolsma, Robin de Bruin, Sara Crombach, Thomas von der Dunk, Annemarie van Heerikhuizen, Hanna Jansen, Ben de Jong, Michael Kemper, Krisztina Lajosi, Joep Leerssen, Matthijs Lok, Martijn Lunter, László Marácz, Martin Mevius, Manet van Montfrans, Eric
van Ree, Marleen Rensen, Peter Rodenburg, Jamal Shahin, Guido Snel, Menno Spiering, Anne van Wageningen, and P.W. Zuidhof.

I received a warm welcome at Durham University’s Institute for Hazard and Risk Research, where I worked as a visiting scholar from October until December 2009. Louise Amoore and Alexandra Hall were very helpful in organising this stay. Louise has been an inspiring and enthusiastic supervisor during this period, which was devoted to drafting a first version of chapter 3, on the genealogy of the European fight against terrorism financing. I admire Alex for her professional efficiency and expertise and greatly enjoyed the joint fieldwork we did in Brussels and the occasional dive we made into Durham’s swimming pool. Louise and Alex also provided me with precious comments on my draft chapters at later stages of the project.

I am greatly indebted to my interviewees, who remain anonymous in this dissertation but who spent considerable time talking to me and often helped to set up other interviews. Their willingness to provide me with often fascinating insights about daily financial security practices, their knowledge about why things are as they are, and their visions of the past and future fight against terrorism financing, were crucial for the current shape of this dissertation. These interviews were always very pleasant, and this made the gathering of new empirical information one of the most enjoyable aspects of this research project.

Over the years, I have presented draft versions of most chapters of this dissertation at various faculty and international workshops and conferences, including the University of Amsterdam (2008, 2009, 2010, 2011, 2012), the ISA Annual Convention in New York (2009), the Institute for Hazard and Risk Research at Durham University (2009), the Scottish Institute for Policing Research in Glasgow (2009), the GARNET Conference in Brussels (2010), and PRIO in Oslo (2011). I received many useful and stimulating comments and questions during the discussions that followed these presentations, including from Joyce Goggin, Anthony Amicelle, Rocco Bellanova and Gilles Favarel-Garrigues. Parts of chapter 5 have been published as “Data Wars beyond Surveillance: Opening the Black Box of SWIFT,” co-authored with Marieke de Goede and Louise Amoore, in the Journal of Cultural Economy (2012).

Discussions with friends and family have helped me to clearly formulate the questions I was investigating and allowed me to share my excitement about the findings. Their reactions – sometimes of complete astonishment or instant activism – also confirmed the societal relevance of questioning the practices of the post-9/11 fight against terrorism financing. I am thankful for their friendship and the interest that my friends and family have shown in my research topic. I have great memories of discussing terrorism financing and anti-terrorism architectural designs with Enrique Ramos on several occasions in Durham and London. I also recall the lively conversation I had about my work with my relatives in Canada on a Sunday afternoon in July 2012 on their farm. Without being exhaustive, Kirsten Verkley, Femke Besançon, Dorly Castañeda, Gaëlle Dakan, Richt Hiemstra, and Maria Kleis have been indispensable for their emotional support.
My parents, Henk and Tia Wesseling, deserve special mention for their love and support, as they have been closely following my work and well-being. During the entire project, they collected many relevant press articles. Together with my brother Jeroen, they suggested names of people who could help me get interviews with people in the initially almost impenetrable world of international banking. They were always keen to hear about my progress and the latest developments in my writing and teaching. After leaving my apartment in Amsterdam in 2011 and moving to France, they provided me with a wonderful pied-à-terre and office space in their house, which I hope to continue to make use of very regularly in the future. My gratitude to them is beyond words.

Finally, the strong support and encouragement of Jérôme Balland, now my husband, has helped me through the various stages of writing a PhD dissertation. He has always offered a listening ear and enthusiastically shared his views with me about the parallels between the practices of the War on Terror and the ideas of the mathematician Pierre Laplace. He regularly updated me on changes in French anti-money laundering and counter-terrorism financing laws and surprised me with a bibliography of SWIFT investigator Jean-Louis Bruguière on my birthday. Numerous have been the evenings when I was working late and he prepared me an airplane-style tray with a three-course meal (though much tastier than airline food) or a pot of tea with a carefully selected assortment of sweets. I am endlessly grateful for his love and devotion.
List of Illustrations

Tables

1.1 The FATF Special Recommendations
1.2 Overview of EU CFT legislation and the corresponding FATF Special Recommendations
4.1 Detailed timeline of the SWIFT affair
4.2 Phases of politicization and depoliticization of the SWIFT affair
5.1 Historical TFTP Value Examples
6.1 The evolution of the EU’s AML Directives
6.2 Typology of FIUs in the EU
6.3 High-risk country list
6.4 Low-risk country list

Figures

2.1 Professional field map of the SWIFT affair
2.2 Professional field map of the Third Directive
3.1 Discourses on terrorism financing prior 9/11
4.1 If the New York Times had covered the Revolutionary War
5.1 An example of a link analysis
6.1 Connecting liberty and security, but how?
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACLU</td>
<td>American Civil Liberties Union</td>
</tr>
<tr>
<td>ALDE</td>
<td>Alliance of Liberals and Democrats for Europe</td>
</tr>
<tr>
<td>AML</td>
<td>Anti-Money Laundering</td>
</tr>
<tr>
<td>CBPL/CPVP</td>
<td>Commissie voor de Bescherming van de Persoonlijke Levenssfeer/ Commission de la Protection de la Vie Privée (Belgian Privacy Commission)</td>
</tr>
<tr>
<td>CDD</td>
<td>Customer Due Diligence</td>
</tr>
<tr>
<td>CFT</td>
<td>Combating the Financing of Terrorism</td>
</tr>
<tr>
<td>CPB</td>
<td>College Bescherming Persoonsgegevens (Dutch Data Protection Commission)</td>
</tr>
<tr>
<td>ECB</td>
<td>European Central Bank</td>
</tr>
<tr>
<td>ECON</td>
<td>Economic and Monetary Affairs Committee of the EP</td>
</tr>
<tr>
<td>ECR</td>
<td>European Conservatives and Reformists</td>
</tr>
<tr>
<td>EDPS</td>
<td>European Data Protection Supervisor</td>
</tr>
<tr>
<td>EP</td>
<td>European Parliament</td>
</tr>
<tr>
<td>EPP</td>
<td>European People’s Party</td>
</tr>
<tr>
<td>EU-CTC</td>
<td>European Union Counter Terrorism Coordinator</td>
</tr>
<tr>
<td>FATF</td>
<td>Financial Action Task Force</td>
</tr>
<tr>
<td>FIU</td>
<td>Financial Intelligence Unit</td>
</tr>
<tr>
<td>GUE/NGL</td>
<td>European United Left/Nordic Green Left</td>
</tr>
<tr>
<td>IEEPA</td>
<td>International Emergency Economic Powers Act</td>
</tr>
<tr>
<td>KYC</td>
<td>Know Your Customer</td>
</tr>
<tr>
<td>LIBE</td>
<td>Civil Liberties, Justice and Home Affairs Committee of the EP</td>
</tr>
<tr>
<td>MEP</td>
<td>Member of the European Parliament</td>
</tr>
<tr>
<td>MLG</td>
<td>Multi-Level Governance</td>
</tr>
<tr>
<td>MLRO</td>
<td>Money Laundering Reporting Officer</td>
</tr>
<tr>
<td>NA</td>
<td>Non-Attached Member (of the EP)</td>
</tr>
<tr>
<td>NSA</td>
<td>National Security Agency</td>
</tr>
<tr>
<td>NVB</td>
<td>Nederlandse Vereniging van Banken (Dutch Association of Banks)</td>
</tr>
<tr>
<td>OFAC</td>
<td>Office of Foreign Assets Control</td>
</tr>
<tr>
<td>PEP</td>
<td>Politically Exposed Person</td>
</tr>
<tr>
<td>PES</td>
<td>Party of European Socialists</td>
</tr>
<tr>
<td>PI</td>
<td>Privacy International</td>
</tr>
<tr>
<td>PNR</td>
<td>Passenger Name Records</td>
</tr>
<tr>
<td>SOCA</td>
<td>Serious Organised Crime Office</td>
</tr>
<tr>
<td>STR</td>
<td>Suspicious Transaction Report</td>
</tr>
<tr>
<td>SWIFT</td>
<td>Society for Worldwide Interbank Financial Telecommunication</td>
</tr>
<tr>
<td>TFTP</td>
<td>Terrorism Financing Tracking Program</td>
</tr>
<tr>
<td>TFTS</td>
<td>Terrorism Financing Tracking System</td>
</tr>
<tr>
<td>UNSCR</td>
<td>United Nations Security Council Resolution</td>
</tr>
</tbody>
</table>
Chapter 1.

The European Fight against Terrorism Financing

We ought to regard the present state of the universe as the effect of its past and the cause of its future. An intelligence which at a certain moment would know all forces that set nature in motion, and all positions of all items of which nature is composed, if this intellect were also vast enough to submit these data to analysis, it would embrace in a single formula the movements of the greatest bodies of the universe and those of the tiniest atom; for such an intellect nothing would be uncertain and the future just like the past would be present before its eyes.

—Pierre Simon Laplace (1902, p. 4)¹

1.1 Laplace’s Demon and Governing the Future

In *A Philosophical Essay on Probabilities*, first published in French in 1814, French mathematician and astronomer Pierre Simon Laplace introduced a thought experiment involving a superhuman intelligence that later became known as Laplace’s demon. This intelligence, which could be understood as a supercomputer, would be able to know and analyse all the forces of the universe. Capturing all the possible data of the universe into one mathematical formula, this intelligence would be able to render visible both the future and the past. Laplace immediately admits that the human mind only possesses a fraction of this extraordinary calculative capacity and that this universal formula cannot be known. Instead, he suggests that humanity can gradually improve its knowledge of the world through science and in particular through probabilities.

During the past two centuries, critics of Laplace, mostly physicians and mathematicians, have successfully advanced arguments for rejecting his causal determinism in which the present is completely determined by the past and precisely predicts the future, ruling out uncertainty, free choice and chance. Nevertheless, the work of Laplace remains significant because he was one of the first modern thinkers to explain the world purely through science, instead of invoking theological arguments.² His omniscient ‘intelligence’ would render the future knowable and calculable.

Taking Laplace to the twenty-first century, important parallels can be found between Laplace’s demon and the assumptions of the global War on Terror. After 9/11, the phrase
‘connecting the dots’ became a central element of this war. Political leaders—most prominently President George W. Bush, government bodies, and certain academics expressed a belief that the 9/11 terrorist attacks might have been prevented if ‘dots’ had been ‘connected’ in a timely manner (National Commission on Terrorist Attacks upon the United States, 2004, Ham & Atkinson, 2002), and that ‘we must be able to connect the dots before terrorists strike’ (Bush, 2006). In practice, this meant that the personal data held in commercial databases and the integrated analysis of these bits of data were believed sufficient, if correctly manipulated, to prevent future terrorist attacks. Hence, like Laplace’s demon, post-9/11 security practices for combating terrorism aim to make the future knowable through the collection and analysis of massive sets of data.

Moreover, from an operational perspective, data-led security practices for combating terrorism can, almost literally, be seen as the contemporary counterpart of Laplace’s demon. Like the intelligence described by Laplace, supercomputers store and analyse large quantities of data, such as travel information (for example, Passenger Name Records (PNR)), financial transactions, or Internet and telecommunication data. These personal data are then analysed by specialized software using complex mathematical models and formulas, such as risk analysis, in order to detect terrorists and prevent future plots. The great value of such high-tech, data-led initiatives in the War on Terror has often been emphasized by politicians, governments, think tanks and university scholars (see for instance Adviescommissie Informatiestromen en Veiligheid, 2007, Libiki & Pleeger, 2004, Thuraisingham, 2005).

Although Laplace does not think of his “intelligence” as something that can be created by human organisation and invention, his idea that the future is calculable and that uncertainty can be ruled out opened up the possibility of acting upon the future. Roughly two hundred years after his publications on probabilities, the desire for “an intelligence” able to calculate the future and to make uncertainty governable on the basis of present knowledge expressed in Laplace’s demon is still very present. Knowing and preventatively acting upon the future is one of the central assumptions of the War on Terror. In other words, it is assumed that future terrorist attacks can be avoided if data from the past are known and dots are connected.

The use of personal data to take security action in the War on Terror and attempts to govern through acting upon the future raise many questions. In the data-led security practices of the War on Terror the deployment of financial transaction data occupies a special place. A number of scholars has (critically) investigated the importance and the implications of counter-terrorism financing measures. Their work however mainly focuses on the US (Biersteker, 2008, Naylor, 2006, Warde, 2007) and transatlantic relations (De Goede, 2012)
and Europe has been insufficiently studied so far. For this reason, the way in which the war on terrorism financing has taken shape in Europe and its implications for European governing are the central enquiry of this thesis.

1.2 Combating Terrorism Financing: A War That No One Saw

Immediately after the terrorist attacks of 11 September 2001, the EU designed an EU Action Plan for Combating Terrorism, in which combating terrorism financing became a ‘core component’. Political elites, policy makers and law-enforcement officers emphasized the importance of combating terrorism financing as they considered money vital to the survival of terrorism. In the words of the former EU Counter-Terrorism Coordinator (EU-CTC), ‘terrorists need money to prepare and carry out terrorist attacks’ (De Vries, 2004). This argument has often been illustrated by the fact that the 9/11 hijackers needed money for travelling, flight training and to cover living expenses (National Commission on Terrorist Attacks upon the United States, 2004). The perpetrators of the 2005 London attacks bought bomb making equipment, paid rent, hired a car and travelled in the UK in preparation for their acts (UK House of Commons, 2006, p. 23). Following these observations and reversing the argument, it was argued that without money terrorists cannot carry out attacks and therefore, as President Bush put it in September 2001, ‘the world needed to stop payment’ (Bush, 2001b).

In addition to the observation that money is vital for terrorists, targeting their financial flows is also believed to be an effective tool for preventing international terrorism. As international terrorists are often assumed to be very mobile, it is thought that their financial transactions may uncover their identity and location prior to a terrorist act. Moreover, financial transactions may reveal to whom terrorists are (financially) connected. By following the ‘money trail’ financial investigators claim to be able to disrupt entire terrorist networks. In addition, financial information is regarded as very reliable information compared to other forms of intelligence (Biersteker & Eckert, 2008, p. 2), available before terrorist acts are committed, since people usually do not transfer money without a specific reason.

On the basis of these ideas the list of measures and initiatives to combat terrorism and its financing gradually expanded, often in direct relation to terrorist attacks on European soil, most notably the simultaneous bombings on trains in Madrid on 11 March 2004. In December 2004, a separate Strategy on Combating Terrorism Financing was developed to provide a
‘coherent and overall approach for further strengthening the fight against terrorism financing’ (Council of the EU, 2004, p. 1). This strategy, as well as, in more general terms, the 2005 EU Counter-Terrorism Strategy, prescribes an ‘intelligence-led approach and improved information sharing within and between government and the private sector’ (Council of the EU, 2004, p. 9; see also 2005, p. 12). This approach has progressively been adopted by all EU member states and continues to be a central element in European security policies, as attested by the 2010 Stockholm Programme (Council of the European Union, 2010a).

The intelligence-led approach to combat terrorism financing can be characterized as a proactive, preventative form of policing through the collection and analysis of massive sets of personal information with the help of smart technologies and in cooperation with private authorities. From an operational perspective this approach can be described as follows. Financial service providers hold a wealth of data on their customers, including, for example: first and last names, gender, passport number, place and date of birth, bank account and credit card numbers and information about the amount, place, time and destination of financial transactions. These data are monitored and analysed by specialized software programmes, often initially designed for commercial purposes, using techniques such as ‘profiling’, ‘data mining’, ‘social network analysis’, ‘risk analysis’ and other ‘predictive technologies’. On the basis of these programmes unusual or suspicious transactions can be found and subjected to a closer analysis by either compliance officers within banks or (in a later stage) law-enforcement officers and intelligence agencies. The latter can also request specific data from banks and match and crosscheck this information with a multitude of public or private databases and publicly available information.

A decade after 9/11, targeting money in order to cut off terrorists’ access to funding is considered to have a ‘proven effectiveness’ (European Commission, 2011, p. 1). Yet, the practices of tracking terrorism financing remain basically invisible – we know little about the professional practices or political implications of the turn to financial data in the context of pursuing terrorism. Moreover, European citizens seem rather unaware of the scope, possibilities and cumulative effects of the measures taken in the fight against terrorism. In contrast to controversial aggressive military operations to ‘smoke terrorists out of their holes’ (Bush, 2001a) and initiatives to combat terrorism ‘on the dark side’ (Cheney, 2001), the war on terrorism financing is:
a war that no one saw. There was no bloodshed, no guns and no soldiers. [...] This war is fought with bank accounts and financial transactions [...] tracking and attempting to dismantle terrorist organizations or rogue nations (The Washington Post, 2011).

It almost appears as if there are two distinct universes, where the reality of the ‘dirty’ War on Terror, illustrated by the thousands of deaths in the militarily and politically disastrous invasion and occupation of Iraq, or the images and stories of the humiliation, abuse and torture of prisoners, are unrelated to the ‘clean’, preventative approach using high-tech solutions offered by smart software programmes of police and intelligence services, which is perceived to be respectful of human rights, non-violent and successful.

The following chapters aim to shed light on these less visible aspects of the War on Terror and assess the assumptions on which the measures to combat terrorism financing are built. How did financial data become a central element in the global and European fight against terrorism? Is the assumption that increased data gathering is an indispensable condition for success in the fight against terrorism correct? What are the possibilities and limits of fighting the war on terrorism finance through transaction data? How does the fight against terrorism financing change European governing practices and patterns? Which controversies characterized and structured political processes and outcomes of current European counter-terrorism financing (CFT) policies?

In order to elucidate the practices of intelligence-led policing and the assumptions of the European fight against terrorism financing, it is also important to analyse the professional field that has been created in the name of this fight. This involves studying the web of institutions, rules, and practices through which dirty money is targeted. Who is involved in European efforts to combat terrorism? What are the roles of those who govern this fight? Where is decision-making power located? What kind of power is exercised? How are decisions made? Answering these questions makes it possible to account for the War on Terror as a dispersed form of power which appears to have profound implications for the meaning of sovereignty in the current international system and the rule of law within EU member states. Furthermore, some states have made agreements for data transfer with companies in other countries, completely bypassing the national governments of these countries and their sovereign power.

Public-private cooperation is another important aspect of the field of governing. As mentioned above, European legislation demands that the private sector be increasingly involved in monitoring European citizens in order to prevent terrorist acts. At the same time,
the fight against terrorist financing has led to strengthened regulation of the private sector. This apparent paradox of the reassertion of state power over deterritorialized finance through modes of governance that transfer security decisions to the private sector is one of the issues that needs to be examined. What are the consequences of charging private companies with the task of securing the ‘homeland’? To what extent are decisions regarding national security transferred to anonymous employees inside companies such as banks and insurance agencies? Subsequently one may ask whether decisions about who and what are suspicious are legitimate, transparent and accountable, when they are made by private actors from the financial services sector?

Hence, from a broader perspective, the analysis of the turn to financial data to combat terrorist financing and what the EU refers to as intelligence-led policing touches upon some important themes in the social sciences, in particular the evolving relations between liberalization and re-regulation of financial markets, the proliferation of privatised power and ‘pooled sovereignty’, and the relation between freedom and security.

### 1.3 European Policies for Combating Terrorism Financing

The European measures for combating terrorism financing are based on the guidelines of the Financial Action Task Force (FATF). Within two weeks of the 9/11 attacks, this informal platform, consisting of a group of OECD states, drafted eight Special Recommendations (SR) on terrorism financing. A ninth Special Recommendation on cash couriers was added in 2004 (see table 1.1). These recommendations require states worldwide to regulate all sorts of financial transactions in order ‘to detect, prevent and suppress the financing of terrorism and terrorist acts’ (FATF, 2001). The implementation and ratification of the relevant UN Conventions and resolutions are incorporated in the FATF guidelines as the first Special Recommendation.

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

Table 1.1 FATF Special Recommendations, source: www.fatf-gafi.org.
The EU has transposed the FATF’s Special Recommendations into EU law by adopting a number of Directives and Regulations (see table 1.2). In the weeks following 9/11, the freezing and seizing of funds and financial assets on the basis of UN Security Council Resolutions (UNSCR) 1267 (1999) and 1373 (2001) were most prominent actions. These resolutions required the blacklisting of individuals and groups suspected of terrorism, in particular Osama Bin Laden, the Al Qaeda network and the Taliban. The purpose of these economic sanctions was to reduce the flow of funds to terrorists and to disrupt their activities. Moreover, according to the Council of the European Union, the listing procedures give an important political sign and have a deterrent psychological impact (2004, p. 3). However, the practices of blacklisting have also raised controversy, as they were at first not compatible with certain fundamental rights.

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

Table 1.2 Overview of EU CFT legislation and the corresponding FATF Special Recommendations.

Surrounded by far less media attention than the economic sanctions, the other FATF guidelines required more negotiation and were transposed in the years after 9/11. These measures attempt to regulate the financial sector and track financial transactions. Seven of the nine Special Recommendations are addressed in the Directive on the Prevention of the Use of the Financial System against Money Laundering and Combating the Financing of Terrorism (2005/60/EC), also known as the Third (AML/CFT) Directive. Special Recommendations VII and IX have been transposed separately into EU law in the form of the Regulation Controlling
Cash Entering or Leaving the Community (EC) No 1889/2005 and Regulation (EC) No 1781/2006 on information on the Payer Accompanying Transfers of Funds. Additional action with regard to alternative remittance services (FATF SR VI) was taken through the adoption of Directive 2007/64/EC, the so-called ‘Payment Services Directive’.

The EU’s 2004 Strategy on Terrorism Financing explains that the two approaches for combating terrorism financing (freezing financial assets on the one hand and tracking transactions on the other) ‘are not mutually exclusive’ (Council of the European Union, 2004, p. 3). Depending on the specific situation, governments may consider it more useful not to publicly designate a terrorist (group) but silently to track their financial transactions in order to obtain more insights in their activities (ibid.). After an initial wave of designations in the wake of 9/11, the emphasis of the European efforts against terrorism financing has shifted increasingly to tracking terrorist transactions. The two most important elements in this context are the Third Directive on the prevention of the use of the financial system against money laundering, and combating the financing of terrorism, adopted in 2005, and the Terrorism Finance Tracking Programme (TFTP). These two initiatives have been selected as case studies in this thesis.

The Terrorist Finance Tracking Program was not designed as a European instrument for combating terrorism financing. This initially secret American intelligence programme was created shortly after 9/11, and consisted of gathering and analysing financial transaction data from the SWIFT system in order to detect terrorist plots and trace potential terrorists and terrorism financiers. Although the EU was not involved in the development of the TFTP, the programme merits thorough examination in the context of the European fight against terrorism for a number of reasons. First, a large part of the transferred SWIFT data concerns transactions involving bank accounts in EU member states. Second, revelation of the TFTP provoked a yearlong controversy between the EU and the US and within the EU, in which all EU institutions were greatly involved. Between 2006 and 2010 heated debates on the SWIFT affair took place in the European Parliament, and successive (interim) agreements and solutions to continue the programme have been prepared by the European Commission and the Council. Third, the TFTP is now considered a ‘powerful tool’ for both American and EU law-enforcement authorities. Moreover, a European equivalent of the programme is currently being developed in the form of the European Terrorism Financing Tracking System (TFTS). In this light, it is important to understand how the original programme operates, what assumptions underpin the programme, and what implications it has.

The Third Directive is the most comprehensive EU measure to fight terrorism
financing with a broad impact on daily financial lives of citizens and mundane transactions. It obliges professionals in the banking sector or providing financial services to increase surveillance on their clients and the accounts they may hold. Through enhanced ‘Know Your Customer’ and due diligence requirements, regulated professions have to establish the identity of their client, to record and analyse their financial transactions and to report any suspicious transaction to a national Financial Intelligence Unit (FIU). In addition to the central place of the Third Directive in the European CFT policy, two other arguments also justify the choice of this Directive as a case study. The Third Directive is a salient example of large-scale public-private security cooperation, which allows for an investigation of how the Third Directive incorporates and authorizes financial professionals as security actors. Moreover, the Third Directive is an important but largely unknown example of the data- or intelligence-led fight against terrorism in which all European citizens are involved.

1.4 Academic Debates on the European Fight against Terrorism Financing

The adoption of European measures for combating terrorism financing did not cause much debate in academia. Although the number of scholarly publications on the EU’s counter-terrorism policy strongly increased after 9/11 (e.g. Bendiek, 2006, Bures, 2006, Den Boer, 2003, Den Boer & Monar, 2002, Kaunert, 2010a, 2010b, Peers, 2003, Spence, 2007, Zimmerman, 2006), these publications often devote no or only marginal attention to terrorism financing. Literature on terrorist financing, on the other hand, generally examines the American (and sometimes the British) situation or focuses on the methods of terrorism financing deployed by terrorists (e.g. Biersteker & Eckert, 2008, Clunan, 2006, Donohue, 2006, Navias, 2002, Warde, 2007). The body of literature that specifically and profoundly analyses the European fight against terrorism financing is relatively modest. This section discusses these accounts, in order to show how the present thesis builds upon and moves beyond present literature.

William Vlcek (2005, 2006, 2007, 2008, 2009) has published extensively on the European policies combating the financing of terrorism. In his most recent articles Vlcek sees the European CFT policy in terms of financial surveillance and highlights the implications of these measures for the respect of human and fundamental rights. Examining the post-2001 requirements for identification and transaction monitoring, Vlcek states that these practices imply a ‘subtle imposition upon personal privacy’ (2005, p. 1) and that ‘the measures taken in
the financial war on terror have reduced liberty’ (2008, p. 24). He also points to the negative impact of counter-terrorism financial regulations upon civil liberties, in particular for individuals who might have difficulty accessing the formal financial system, such as migrants and the homeless (2005, 2007, 2008). ‘These individuals are not in a position to engage with formal banking structures (due as much to the cost of establishing and maintaining an account as to the requirements for documentation) and as a result may use an informal banking system’ (2005, p. 14). The attempt to regulate informal value transfer systems, such as ‘hawala’, has also been object of his research. He examined, for instance, how the European legal framework to combat terrorism financing affects migrants’ remittances to their countries of origin (2008; on the conceptualization of hawala see Vlcek, 2010). Human and fundamental rights were also central to his analysis of the difficulties of challenging the EU’s regulatory framework against terrorism financing before the European Court of Justice (2005, 2006). In addition to this critical political analysis, Vlcek’s work also investigates the effectiveness of the EU’s CFT policy. Although Vlcek’s work covers many aspects of the EU’s CFT policy – blacklisting and the regulation of the formal and informal banking sectors – his work mainly considers the (potential) impact of the outcomes of this policy. He does not consider how these policies come into being, who participates in their design, how the problem of terrorism financing is shaped during negotiations and how the banking sector chooses to implement the measures. In this thesis, the daily practices in the fight against terrorism financing are analysed in great detail, which leads to a different understanding of financial surveillance.

Anthony Amicelle and Gilles Favarel-Garrigues have studied the European CFT measures through a surveillance studies lens. Specifically, they investigate the intensified control of financial transactions that is based on techniques of traceability and risk-based regulation, and the public-private cooperation that emerges from these surveillance practices (2009, 2012, Amicelle, 2011a). In addition, they have published on the TFTP and the SWIFT affair as an example of financial surveillance (Amicelle 2011b, Amicelle & Favarel-Garrigues 2009, 2012). Separately, Favarel-Garrigues has published on the implementation of CFT policies in France (Favarel-Garrigues et al., 2008, 2009). In these works he considers how the banking industry takes up its assigned task of policing dirty money. He demonstrates how expertise on combating money laundering was developed within banks by analysing the professional background of bank employees responsible for compliance, the emergence of professional networks and training programmes and the AML procedures that have gradually been put in place. On basis of extensive fieldwork he concludes that the banks have a leading
role in combating money laundering, and that ‘their activities have become closely intertwined with those of the policing authorities’ (2008, p. 18).

Other political science or European Studies scholars have examined the CFT policy from a European integration perspective. Oldrich Bures (2010) sets out the EU framework for thwarting terrorism financing and assesses its shortcomings, its legal challenges and its effectiveness. He found that it is ‘rather difficult’ to assess the effectiveness of the European measures in this field, but that a number of internal and external obstacles that hamper the EU efforts to combat terrorism financing can be identified (p. 424). With respect to the latter, Bures refers to erroneous assumptions on which the global CFT efforts have been based and in particular the ‘heavy reliance on the “targeted/smart” sanctions and anti-money-laundering models’ (p. 426). Concerning the functioning of the CFT policy within the EU there are a number of internal obstacles. First, ‘the legal basis is far from being crystal clear’ as various decision-making procedures apply (p. 424). Moreover, implementation of the measures is piecemeal because implementation requires complex coordination within and between the public and private sectors; member states perceive the terrorist threat differently, which affects their motivation for compliance; and the measures sometimes conflict with national politics and judicial procedures (p. 425). Finally, Bures states that: ‘the fact that consensus [over CFT measures] is reached by a small circle of CFT experts excludes or renders less effective national mechanisms of democratic and judicial control’ (p. 426). According to him the EU can and the Lisbon Treaty will improve the internal shortcomings of the CFT framework.

Christian Kaunert and Marina Della Giovanna (2010) consider the role of the European Commission and the Council Secretariat as supranational policy entrepreneurs ‘in order to explore and assess the role played by the EU supranational actors in implementing post-2001 UN and FATF standards on countering terrorist financing at EU level’ (p. 277). They assert that making use of their specific powers, adopting strategies suitable to their respective roles and profiting from the window of opportunity opened by the horror of the 9/11 attacks, the Commission and the Council Secretariat ‘have played a significant role in the transposition of CFT standards into EU legislation, and overall, in the design of the EU-CFT regime’ (p. 284). Consequently, they conclude that supranational European institutions ‘can be important players’ in all aspects of counter-terrorism policy, rejecting the intergovernmentalist assumption that high politics areas such as Justice and Home Affairs remain the exclusive prerogative of nation states (p. 290).
Although these two articles provide interesting insights about the European CFT policy, they both consider the EU and the European institutions as unitary actors and restrict their focus to policy making at the European level. Their respective approaches exclude power struggles that take place within and between the European institutions during the policy making process, and in both articles the European Parliament, for instance, is completely absent. In addition, they exclude the influence of participants outside the European institutions such as the private sector, media and civil society.

Legal scholars have analysed the EU’s AML/CFT measures, but few have specifically addressed the terrorism financing aspects of these laws. An important exception is the article of Valsamis Mitsilegas and Bill Gilmore (2007), in which the authors discuss the evolution of the EU’s legal framework for combating money laundering and terrorist financing from a Justice and Home Affairs perspective. Taking into account the EU’s three Anti Money Laundering (AML) directives, the Regulation on controls of cash entering the EU and the Directive on Payment Services in the internal market, they analyse the changes in the subsequent AML/CFT measures and the challenges these have raised with respect to EU constitutional law. Moreover, they stress the strong relationship between instruments and initiatives taken by international organisations, most notably the FATF and the UN and the EU.

Furthermore, various scholars (Amicelle & Favarel-Garrigues, 2009, 2012, Bulterman 2005, Guild 2008, 2010, Tappeiner, 2005, Vlcek 2005, 2006) have published on the controversial ‘terrorist lists’ requiring the freezing of financial assets of listed individuals and their implementation in EU law. Illustrated by the well-known Yusuf, Kadi, Al Barakaat and OMPI (Organisation of Modjahedines People of Iran) court cases, they highlight a number of shortcomings of both the EU and the UN terrorist lists. These include: the lack of democratic and judicial oversight by the European Parliament and the European Court of Justice, respectively; the lists’ incompatibility with certain human rights, such as the presumption of innocence; and their inefficiency in putting a halt to terrorism. On the basis of recent modifications to the listing processes, Guild asserts that ‘legal order is beginning to work its way into what appears to have been an arbitrary mechanism of designation’ and ‘the rule of law is beginning to make its way to the shady world of lists of suspected terrorists’ (2008, p. 190).

These accounts provide important insights into aspects of the EU’s efforts to combat the financing of terrorism upon which this thesis aims to build further. On four significant points it expands the existing literature. First, the existing literature on the EU’s efforts to
combat terrorism financing is critical with regard to the legality, legitimacy and efficiency of this policy but it does not sufficiently question the assumptions underpinning the War on Terrorism Financing. Bures for instance states that the logic of combating terrorism financing is ‘straightforward’ (2010, p. 418). Likewise Kaunert and Della Giovanna assert that in the immediate aftermath of the 9/11 attacks it became apparent that finance was of ‘crucial importance to the survival of Islamist fundamentalist organisations such as Al Qaeda’ (2010, p. 275). I propose to extend the critique by questioning the assumptions and underpinnings of the European fight against terrorism financing. As Michel Foucault put it: ‘a critique is not a matter of saying that things are not right as they are. It is a matter of pointing out on what kinds of assumptions, what kinds of familiar, unchallenged, unconsidered modes of thought the practices we accept rest’ (1988, p. 154). By denaturalizing the efforts to combat terrorism financing, and ‘making strange’ security practices that appear to be common sense, it becomes possible to step outside the existing frames and think things differently (ibid.). As such, a broader set of political questions can be raised about security programmes targeting daily financial behaviour, going beyond effectiveness and judicial and procedural correctness.

Second, most studies take a conventional approach to the actors involved combating terrorism financing. They mainly focus on the EU institutions and sometimes the role of one or more member states that are considered unitary actors, for instance, the FATF, the European institutions or the EU. While it can be difficult to avoid these generalizations and they may sometimes be correct, they also obscure struggles and controversy within these organizations. Moreover, this conventional approach excludes the role of non-institutional actors. Among the works discussed above, Amicelle and Favarel-Garrigues do consider thoroughly public-private cooperation. However, Bourdieu’s field theory, the theoretical model adopted here (see chapter 2), also includes other actors (participants) such as journalists, civil society, business associations and other private sector stakeholders. As discussed in detail in the next chapter, field theory permits an examination of the exercise of power beyond pre-established institutional structures or formal legal competencies. Considering the European fight against terrorism financing in terms of a professional field implies analysing a fragmented social space that is structured by shared beliefs, practices, and professional and bureaucratic power relations rather than by institutional, sectorial, or geographic boundaries.

Third, the existing literature offers a critical analysis of the political outcomes but does not consider the political processes leading to these outcomes. For instance, Bures (2010) states that ‘it is not surprising that the Financial Action Task Force on Money Laundering
nowadays sets and promotes the adoption of global standards to combat both money laundering and terrorist financing’ (p. 421). Yet, I will show that this choice was not self-evident at first, but rather the product of intense negotiation. A deeper understanding of the political process preceding decisions and adaptations of the law, for instance, the inclusion of terrorism financing in AML law, reveals the gaps, contradictions, and insecurities in the security programmes designed to target terrorist financing. It prevents the current situation from being considered natural and reminds us that alternative solutions existed but were discarded. Thus, such an analysis allows the development of a critical perspective on current policy initiatives for combating terrorism financing that have largely come to be accepted as effective, legitimate, and even ‘self-evident’.

Fourth, instead of focusing on just the legal, political, or operational aspects, a more comprehensive governmentality approach is taken in this thesis. The Foucauldian notion of governmentality refers to the modes of thought or rationality that underpin practices of governing. It implies investigating the techniques of government—this includes institutions, procedures and tactics—that are deployed to exercise power and considering its legal, political, and operational aspects. Moreover, it means that both the political decision-making process and the operational practices of combating terrorism can be subject to investigation. Finally, a governmentality approach goes beyond a legal and operational approach in order to analyse how power is shaped and what is being governed. How does the fight against terrorism financing govern through the identification and prescription of mundane financial normalities and abnormalities? As Amoore and De Goede (2008a) highlight, these are important questions, because contemporary security action based on the minutiae of daily life and the classification techniques on which they rest constitute an almost invisible form of violence and have political implications. These four points are taken up in the following chapters. The next section provides an overview of the themes discussed in each chapter.

1.5 Chapter Overviews

This thesis is further divided into three parts. The first part, consisting of chapters 2 and 3, introduces the theoretical tools with which the European fight against terrorism financing will be studied here. Chapter 2 discusses how the fight against terrorism financing leads to the creation of a field of governing that goes beyond institutional, sectorial and geographic boundaries and how this professional field can be studied. It also introduces the
Foucauldian notion of governmentality, which entails the study of rationalities and practices through which citizens are governed. Chapter 3 offers a historical perspective tracing a genealogy of the European fight against terrorism financing. This chapter considers the structure of the discourse on countering terrorism financing and the framing of terrorism financing as a (European and international) problem. Examining the genealogy of the European fight against terrorism financing has two objectives. It aims to make visible the assumptions on which the post 9/11 fight against terrorist monies is based, and it offers theoretical guidelines that will be used throughout the thesis.

The second part, which is the heart of the thesis, consists of three empirical chapters. In these chapters two case studies are examined in order to identify specific fields of governing that have emerged from the European fight against terrorism finance. Chapters 4 and 5 investigate the Terrorism Financing Tracking Programme (TFTP), also known as the ‘SWIFT affair’. Chapter 4 offers a content analysis of press articles, political debates and official documents that followed the revelation of the TFTP in the US and EU. It shows how discourse surrounding the programme was structured, and how certain aspects of the programme become politicized and led to a policy response, while others were ignored and forgotten. Chapter 5 examines questions that were left unanswered in the SWIFT affair. Opening the TFTP’s black box, so to speak, it considers how the programme probably works and what tangible results and implications it has generated. Chapter 6 addresses the implementation of the EU’s Third AML/CFT Directive. Adopting the metaphor of the theatre, this chapter makes visible the daily governing practices developed in name of the European fight against terrorism financing and opens them up for questioning.

Chapter 7 forms the third and concluding part of the thesis. In this chapter, the focus is broadened by considering the European fight against terrorism financing in terms of financial surveillance. Conclusions are drawn by comparing and summarizing the key findings of the two case studies as examples of financial surveillance.
Chapter 2.

The European Field of Governing

At noon on September 13, a passing agent ducked his head into Dennis Lormel’s office. He said that someone had called from the Omaha FBI office. A company named First Data Corporation, with a huge processing facility out there, wanted to help in any way it could. A red-eyed Lormel looked up from his desk. “Oh, that’s big” he said, breaking into a weary smile. “That could be very, very big.” [. . .] First Data is one of the world’s largest processors of credit card transactions, a company with 6.5 billion in revenues and a global reach. [. . .] “Inside that company” he told the young agent, “is a gem.” Western Union. [. . .] Now sitting in his office, Lormel told the young agent to get him a number for First Data, and he chewed over an idea: “We need to turn this company into a deadly weapon.”

— R. Suskind (2007, pp. 11-13)

2.1 Introduction

As the quote from Suskind’s book illustrates, the American response to 9/11 led to new configurations in which public and private authorities cooperate closely in combating terrorism financing with the ambition to turn the instruments of this combat into “deadly weapons.” National intelligence and law-enforcement agencies quickly asserted the potential for exploiting the massive sets of financial data collected for commercial purposes. In turn, globally leading financial services companies such as the American payment company First Data Corporation, or the banking cooperative SWIFT were willing to provide American police and intelligence agencies with access to their databases. Moreover, new laws adopted in the name of the War on Terror further expanded the involvement of private authorities by obliging them to monitor strictly financial transactions and to report suspicious behaviour.

Although the setting of Suskind’s book is in the US, the War on Terror did not lead to new forms of cooperation and innovative investigation methods only in this part of the world. The European Union adopted a number of measures to combat terrorism financing. In fact, one of the most recent initiatives, officially launched in 2011, the European Terrorism Finance Tracking System (TFTS), is a European equivalent of the American programme that analyses transaction data provided by SWIFT. The FATF Special Recommendations, which shape the European efforts in the field of combating terrorism financing, all require the
involvement of a wide range of private, and to a lesser extent public, authorities mainly in the banking and financial sectors. For instance, the EU’s Third AML/CFT Directive obliges services providers in or related to the banking and financial sectors to further enhance the registration and monitoring of their customer’s financial data and to report ‘suspicious’ transactions to Financial Intelligence Units (FIUs). On the basis of UN resolutions 1267 and 1373, which have both been transposed into EU law, banks and financial services institutions have to freeze all transactions and accounts of individuals and entities listed on international, European, and national lists of terrorism suspects. In addition, financial services providers, including money transfer services, have to make sure their wire transfers are accompanied by accurate and meaningful information on the money sender.

The involvement of private companies in the European fight against terrorism financing increasingly blurs the distinction between public and private authorities and their respective responsibilities. It also raises questions about the character of this cooperation. Are private companies as figurative deadly weapons only instrumental for law-enforcement services or is a more complex picture of cooperation and interests emerging? Furthermore, if public and private authorities reinforce their cooperation in the name of the fight against terrorism financing, what are the implications for our understanding of European governance processes?

Moreover, the adopted measures translate into new practices aimed at combating terrorism. In this respect, the question can be raised how ordinary businesses in the banking and financial services sectors take security action in the War on Terror. In what sense are they considered to be deadly weapons? What new practices, procedures, calculations, and tactics did banks and financial services companies adopt in the name of the European fight against terrorism financing? What do CFT measures exactly attempt to govern? How do these practices shape this fight? So far, these daily practices through which the European fight against terrorism is governed remain mostly invisible and unexplained.

The purpose of this chapter is to provide a theoretical framework and a methodology to examine what is governed in the name of the fight against terrorism financing and how this is done. Taking up the Foucauldian notion of governmentality and Bourdieu’s field theory, it is argued that the initiatives taken in the name of the European fight against terrorism financing create a new field of governing. This field is a transnational field of professionals that cuts across the division between the public and private sectors. Its focus here is on EU and European decision-making but the actors operating in the field are situated in the public and private sectors on various geographic levels. Through the notion of a European
professional field, public-private cooperation in combating terrorism financing can be studied. This theory also permits us to analyse how power is exercised through technologies, tactics, and practices that are at work in the field. Furthermore, this framework aims to make visible both the expansion of public actors who took up responsibilities for governing this new fight and the cooperation between banks and financial service providers on the one hand and law-enforcement agencies, governmental bodies, and international organizations on the other.

However, it is important to stress that the definition of a European field of governing terrorism financing goes beyond the emergence of new governance structures because it does not just imply the changing relations between European (and national) institutions as policymakers and the financial and banking sectors as being regulated. Following Foucault’s (1991) definition, the scope of the word ‘government’ goes beyond the political realm and must be interpreted more broadly, as ‘the practices of government are [. . .] multifarious and concern many kinds of people: the head of a family, the superior of a convent, the teacher or tutor of a child or pupil [. . .]’ (p. 91). In other words, the exercise of power takes place throughout society and must be understood as “productive” (Brown, 2006, p. 72), and “fragmented” and “dispersed” (Larner & Walters, 2004, p. 4). Understood in this way, the field of governing has broad implications because it affects banking practices and the mundane transactions and civil liberties of citizens.

In order to study the new field of governing and the governing practices this thesis considers two sets of literature; European integration theory and Surveillance Studies. The remainder of this chapter is organized as follows. The next section presents an overview of influential theoretical lenses through which European integration has been studied. The discussion of these theories and their critiques helps to place the European field of governing terrorism financing in a broader theoretical framework of European Studies and International Relations, it explains how field theory contributes to the study of the European Union, and it develops the analytical possibilities of the proposed field of governing. The following section introduces the key concepts in Surveillance Studies literature and discusses the financial surveillance practices and their main concerns. Next, building on these two bodies of literature the concept of governmentality is introduced and it is explained how this concept has value for studying the European fight against terrorism financing. Subsequently, it discusses how field theory can contribute to the understanding and to the operationalization of governmentality. Next, the methodology used in this thesis is explained in more detail. The last section of this chapter proposes two maps of European fields governing the fight against terrorism financing.
2.2 Theorizing the European Union

Scholars in International Relations and European Studies have proposed a multitude of theories explaining European integration. In this ‘mosaic of integration theories’, each theory can be understood as ‘a stone that adds to the picture that we gain of the EU’ and ‘each approach contributes to the emerging picture in its own limited way’ (Wiener & Diez, 2009, p. 19). The different colours of the stones that constitute the mosaic represent the different approaches of the European integration theories. For instance, some theories study European integration as a process while others look at the outcomes of integration or try to define the European Union as a political entity. Additionally, the mosaic metaphor suggests that European integration theories are complementary in that they study or emphasize different aspects of the same phenomenon, creating one picture. The purpose here is not to provide a comprehensive overview of all the separate stones of the mosaic but to discuss four great debates in which European integration theories can be broadly divided but that are not necessarily mutually exclusive.

A first set of theories on European integration is mainly concerned with the normative questions of what European integration should ideally achieve and how this should be realized. These theories emerged between the two world wars and just after World War II, when institutionalized European cooperation was in its infancy. Jean Monnet and Robert Schuman, founding fathers of European integration, were inspired by ‘functionalism’ as described for instance in *A Working Peace System* by David Mitrany (1966). Functionalists strive for peaceful international relations through the creation of specialized international organizations in which experts solve international problems and enhance social well-being in a politically neutral manner, making governments redundant. Two points of critique against this theory are relevant for our analysis of the field governing the European fight against terrorism financing. First, far from disappearing, governments have reproduced their power struggles within international organizations. Secondly, and very importantly, decisions are never purely ‘technical’. They are always based on relations of power and reflect politically motivated choices that favour certain groups over others.

‘Federalism’ is another important theory on European integration that emerged during and after World War II. Advocated by Altiero Spinelli, another founding father of the European Union, but also by contemporary politicians such as Joschka Fischer (2000) and Guy Verhofstadt (2005), federalists are in favour of the transfer of most of the powers of national governments to a European government. Although federalism still has some support
throughout Europe and some argue that the EU already resembles a federation (see, e.g., Burgess, 2009), to date most EU governments and citizens do not favour the creation of a ‘United States of Europe’.

A second group of theories emerged between the 1960s and the early 1990s in reaction to the various initiatives for closer European cooperation. These theories were mainly concerned with the driving forces of the integration process. Dominated by International Relations scholars, two schools can be distinguished: neo-functionalism, theorized by, among others, Ernst Haas, Leon Lindberg, and Philippe Schmitter, and intergovernmentalism, represented by Stanley Hoffman. Neo-functionalism modernizes the functionalist assumptions, adding political elements and emphasizing the role and socialization of elites. European integration is believed to be incremental and self-sustaining through “spill-over” processes (Haas, 1958). Cooperation in the steel industry, for example, would favour common legislation and cooperation in related sectors such as the automobile industry. In contrast with functionalism, neo-functionalism does not consider cooperation as a controlled process leading to a pre-established goal but rather as a sequence of unplanned developments.

The many critics of neo-functionalism, including at a later stage Haas himself, point out that European integration is characterized by phases of stagnation and intensification instead of a gradual spill-over process. In their view, spill-over can describe integration processes but cannot explain why the integration process evolves as it does. Another important criticism of neo-functionalism stresses the absence of international political or economic developments in the evolution of European integration (see for example Haas 1975, Hoffman, 1966, Rosamond, 2000, Smith, 2004). In light of this thesis, it is evident that the European field of governing terrorism financing cannot be understood without taking into account the terrorist attacks in the US, Madrid, and London or the public reactions on the revelation of the SWIFT affair.

Intergovernmentalists on the other hand reject the idea of spill-over. According to this school of thought, national governments always remain the ‘gatekeepers’ to integration, aligning the speed and level of European integration with their national interest. For this reason the integration process is not fluid but rather discontinuous, depending on the political will of member states to ‘pool’ their sovereignty. During the 1990s, the assumptions of intergovernmentalism were refined by Andrew Moravscák, who coined the term liberal intergovernmentalism (LI) (1993, 1995). He follows a more systematic three-stage approach and combines the intergovernmentalist idea of the convergence of national preferences with regime theory. The adjective ‘liberal’ refers to the importance Moravscák gives to economic
cooperation and national political processes in defining national interests. Throughout the 1990s LI was a central theory in European integration studies in relation to which other scholars positioned themselves (Pollack, 2000, p. 5, Smith, 2004, p. 20).

Three main criticisms have been raised against (liberal) intergovernmentalism and will also be taken into account in this thesis. First, it is argued that its focus on power struggles and ‘grand bargains’ between states overshadows the prior process of negotiation and cooperation among lower-ranking national (and European) officials. Hence, the changes in positions and the early stage bargaining remain invisible in (liberal) intergovernmentalist approaches. Second, liberal intergovernmentalism tends to overestimate the role of states and underestimate the influence and power of the European Commission, the European Parliament, and the Court of Justice of the EU. A third issue concerns the assumption that interests of the state overlap with the interests of powerful socio-economic actors. Although it may be the case in some situations, critics argue that interests may differ on, for instance, geopolitical or ideological questions. A general criticism of both neo-functionalist and (liberal) intergovernmentalist theories concerns their exclusive focus on the binary question whether the integration process is dominated by supranational or intergovernmental decision-making (Smith, 2004, p. 10). Adopting field theory and a governmentality approach implies the rejection of such a dichotomy.

A third debate, initiated by political scientists and scholars in comparative politics, emerged in the 1980s around the core question of the current nature of the EU as a political system. These approaches share a more actor-oriented and detailed analysis of the legislative, executive, and judicial behaviour of the European Union and often use case studies. However, within the variety of accounts a simplified distinction can again be made between scholars who study the political system on the EU level in similar terms as on the national level, such as Simon Hix (see, e.g., 2008), and others who try to link the national and international politics in one theoretical framework based on the notion of governance. My focus here will be on the latter type of theories.

Governance can be defined as ‘the exercise of authority with or without the formal institutions of government’ (Rosamond, 2000, p. 109). Governance theories, such as policy network analysis (Falkner, 2000, Peterson, 2009), neo-institutionalism(s) (Jupillé & Carporaso 1999, Pollack, 2005, 2009) and multi-level governance (Hooghe & Marks, 2001) do not all share the same concepts or theoretical toolbox but rather share a set of assumptions. They usually emphasize the move of authority away from formal institutions and highlight the importance of individual actors in the functioning of European decision-making dynamics. In
particular the concept of ‘multi-level governance’ (MLG) introduced by Liesbeth Hooghe and Gary Marks became very popular in the 1990s (Piattoni, 2009). Their view is that ‘European integration is a polity-creating process in which authority and policy-making influence are shared across multiple levels of government—subnational, national and supranational’ (Hooghe & Marks, 2001, p. 2). They emphasize that aside from the powerful role of states, other actors, for instance regional governments, members of the Committee of Permanent Representatives to the EU (Coreper), lobbyists, and the European Parliament all exercise power over European decisions. Instead of a ‘two-level game’ between the state and the European level, MLG theorists stress ‘the existence of overlapping competencies among multiple governments and the interaction of political actors across those levels’ (Marks et al. 1996, p. 41). In contrast to the ‘grand theorizing’ that characterizes the first two sets of debates, MLG and other governance theories do not aim to offer a general theory of the EU. MLG rather focuses on specific policy areas and emphasizes the variability, complexity, and fluidity of the European policy system.

Largely a response to the perceived weaknesses of liberal intergovernmentalism, MLG also has shortcomings. Despite their attention to a variety of actors, these studies often investigate the pre-existing institutions and legal distinctions between agencies and institutions, while overlooking the overall inter-institutional context in which they operate (Bigo, 2007, p. 7). Another critique is MLG’s relative blindness to power struggles and political contestation. MLG, like ‘spill-over’, provides a metaphor for describing the European political framework but it does not explain the political significance of this framework. It cannot explain why and how European integration occurs and how Europe becomes a legitimate space for political action.

A fourth debate consisting of critical and constructivist approaches to European integration emerged during the 1980s and 1990s. These approaches do not explain European integration but rather question the ontological and epistemological assumptions on which traditional approaches have been built. They consider political culture, struggles, contestations, and discourses. Constructivist approaches emphasize that ‘the interests of actors cannot be treated as exogenously given or inferred from a given material structure’ and that analysis thus needs to include ‘the social construction of interests and identities’ (Risse, 2009, p. 146).

Critical theories go one step further and question the construction and also the legitimacy of the social order. These approaches focus on the domination of individuals or groups by other individuals or groups and investigate how that domination might be
overcome. Marxist and neo-Gramscian theories concentrate on economic domination, post-colonialist approaches highlight the domination of the West, and feminist approaches emphasize the domination of masculine over feminine values. From a Marxist perspective Holman shows for instance how the eastern enlargement of the EU in 2004 led to the domination of a coalition of transnational capital and international institutions in Central and Eastern Europe due to ‘the absence of an indigenous capitalist class, the denationalization of the respective economies, the dominant role of transnational social forces in imposing neo-liberal restructuring on the post-1989 managerial elites, and the neo-liberal underpinnings of the European Union's (EU) enlargement strategy’ (2004, p. 208).

Poststructuralist (or discursive) approaches differ from these critical theories in that they do not focus on a specific type of domination. They rather question the forms of domination that are present in (political) discourses more generally (Bailey, 2011, p. 41). They study the practice of making and reproducing meanings and are interested in knowing who is in control of these processes. Belsey illustrates the significance of post-structuralist questioning through the relatively simple example of the words ‘democracy’ and ‘dictatorship’. When Western children learn to use these words, they absorb the values their culture assigns to these forms of government at the same time. Without having to be explicitly taught, they learn that dictatorship is oppressive and democracy so precious that it is worth fighting for (2002, pp. 3-4). By destabilizing language, meaning, and social institutions, poststructuralists attempt to reveal power structures that are taken for granted. Through discourse analysis poststructuralist scholars try to ‘find the structures and patterns in public statements that regulate political debate so that certain things can be said while other things will be meaningless or less powerful or reasonable’ (Waever, 2009, p. 165). Central figures that are usually associated with this loosely-knit intellectual movement include, for instance, Foucault, Deleuze, Lacan, and Derrida.

Taking into account the strengths and weaknesses of the various European integration theories discussed above, this thesis situates itself within the third and fourth sets of debates. This chapter develops a theoretical framework to analyse the nature of the European field of governing terrorism financing that emerged since 9/11. In doing so, it speaks to the governance theories by building upon the critique of multi-level governance. Mapping the European field of governing terrorism financing implies looking beyond the formal legal frameworks and pre-established institutions and taking into account economic, societal, and political developments. It is also inspired by questions raised in the fourth set of debates, most notably post-structuralism. The governmentality perspective that will be introduced in section
2.4 draws attention to the production of meaning and the way in which power is distributed and operates. In addition, mapping the participants of the field provides a snapshot of power relations between different participants and also makes it possible to visualize power struggles and political choices.

2.3 (Financial) Surveillance Studies after 9/11

A second body of literature that is relevant for the study of the European fight against terrorism financing is surveillance literature. Surveillance studies is a multi-disciplinary enterprise studying the practices of focused, systematic and routine attention to personal data, such as financial data, for purposes of influence, management, protection or direction, and the potential privacy and civil liberties questions that follow from these practices (Lyon, 2007). The amount of surveillance literature has substantially increased after 2001 in order to make sense of the attacks and the avalanche of security initiatives in response to these and subsequent terrorist attacks.

Scholars in surveillance studies have found that contrary to the enormous impact of the 9/11 terrorist attacks on world politics, they did not dramatically alter the understanding and practices of surveillance. New trends in surveillance have led to exciting research on themes for instance related to borders and migration, the use of surveillance technology such as biometrics and CCTV and, of course, governance through the risk and link analysis of personal data as discussed in this thesis. Yet, the surveillance measures introduced after 9/11 and the theorizing of these measures are not disconnected to the world prior to the attacks. ‘The surveillance systems proposed after 9/11 have the strongest possible connection with those in place before that date’ (Lyon, 2003, p. 23). In fact, the attacks rather revealed and accelerated surveillance trends that were already developing in the 1990s and before, according to this body of literature (ibid.).

From its inception in the 1970s and to a large extent still today, two metaphors or concepts have been absolutely central to surveillance studies: Big Brother and the panopticon. In George Orwell’s novel Nineteen Eighty-Four, Big Brother represents a central yet invisible authority, able to constantly control the citizens of Oceania mainly through omnipresent two-way ‘telescreens’. Permanently watching over and manipulating its citizens, Big Brother deprives citizens of any privacy and freedom. Michel Foucault, on the other hand, theorized Jeremy Bentham’s panopticon: a circular prison with a central watching tower in the centre.
Foucault emphasizes that analogue to the panoptic prison a surveillance model can be distinguished, exercising disciplinary power on individuals and on society.

Both metaphors refer to a surveillant ‘eye’ controlling their subjects for undesired behaviour through continuous and pro-active observation. In Nineteen Eighty-Four the two-way telescreens are omni-present in workplaces, public spaces and even inside people’s houses. Likewise, the panopticon allows watchers to observe all inmates individually while remaining unseen themselves. Subjects are thus completely transparent to their observers but they cannot see them. Another similarity between Big Brother and the panopticon is the exercise of surveillance by a central authority; the figure of Big Brother or the (inner) Party and the watchers in the prison tower. Yet, when the panopticon is understood as a disciplinary model instead of a prison it allows for ‘the penetration of regulation into even the smallest details of everyday life through the mediation of the complete hierarchy that assured the capillary functioning of power’ (Foucault, 1995, p. 198). Hence, according to Foucault the panopticon is a model for exercising power suitable for a wide range of institutions in society. As a disciplinary model the panopticon does not constitute one central state authority, the central power is located within for instance the hospital, the school or the workplace.

Despite the similarities, the two concepts are certainly not completely overlapping with each other and each have their own focus. Orwell’s novel touches upon a number of themes among which the use of technology for surveillance purposes, the totalitarian society resulting from this surveillance and its consequences for civil liberties are particularly evoking for studies of surveillance. The pyramid-shaped centralized state surveillance characterized by heavy bureaucracy through extensive record-keeping in relation to new technologies depicted in the novel, inspired surveillance research in the 1970s and 1980s (Lyon, 2003, p. 29, 2006, p. 13). After 9/11, Big Brother remained at the heart of surveillance theory as a metaphor to be either explanatory or to be dismissed. Yet, from a theoretical perspective the Big Brother metaphor has limited explanatory power since it has not been developed much beyond the initial themes of the novel and, as Lewis summarizes, at present ‘there is no centralized hierarchical power watching and recording our every action’ (2005, p. 102).

Foucault’s panopticon on the other hand has proved a ‘rich and multifaceted concept’ (Lyon, 2006, p. 4). It has led to an enormous amount of theoretical work analysing, applying, adapting or contesting the concept both prior and post 9/11. In fact, Haggerty enumerates almost twenty (!) neologisms inspired by the panopticon (2006, p. 26). It is not the purpose to describe all these concepts or to assess all facets of Foucault’s theorizing of the panoptic
mechanism here, but rather to discuss a few key aspects that are central to the disciplinary power exercised through the panopticon and some of its derivatives.

First, as shortly indicated above, visibility is crucial to the panopticon. The panopticon is a machine for dissociating the seeing/being seen dyad: ‘in the peripheric ring, one is totally seen, without ever seeing; in the central tower, one sees everything without being seen’ (Foucault, 1995, pp. 201-202). The architecture of the panopticon facilitates the observation of many inmates by few guards. Moreover, objects of observation are constantly visible as individuals to their observers. An important consequence of this visibility is that it ‘induces (…) a state of conscious and permanent visibility that assures the automatic functioning of power’ (ibid., p. 201). In other words, because subjects expect themselves to be watched, they will adhere to certain expectations of normality or desired behaviour. Disciplinary power precisely works through the awareness of being observed.

Analysis is a second aspect through which the disciplinary power of the panopticon works. Visibility serves the purpose of recording, distributing, examining, diagnosing, assessing, separating, classifying, mapping, comparing and thus, subjecting each individual to a targeted form of control or surveillance. In this process behavioural norms become established through a distinction between the normal and abnormal. According to Foucault discipline normalizes in the sense that ‘it breaks down individuals, places, time, movements actions and operations (…) into components’. Then it ‘classifies the components thus identified according to definite objectives’. ‘Third, discipline establishes optimal sequences or co-ordinations’. ‘(…) [it] fixes the processes of progressive training and permanent control and finally, on the basis of this it establishes the division between those considered unsuitable or incapable and the others’ (2007, pp. 56-57). From the perspective of the subject it constitutes a ‘power over the mind’ (Foucault, 1995, p. 206) ‘designed to encourage an inmate to reflect upon the minutia of their behaviour in a subtle and on-going effort to transform their selves in prescribed directions’ (Haggerty, 2006, p. 25). On the level of the individual, disciplinary power produces (to a certain extent) the self-subjection and disciplining of individuals to the system. As a societal model on the other hand the panoptic mechanism can be applied to a range of institutions including: the army, the church, schools, workplaces, hospitals and of course prisons. In these institutions disciplinary power arranges power in a preventive, homogeneous and efficient manner.

However, the Big Brother and panopticon metaphors have also met substantial criticism. Scholars have argued that the Big Brother and the panopticon metaphors are too restrictive to study today’s surveillance practices (Lyon, 1994, 2006, Haggerty, 2006, Lewis,
They assert that although the 9/11 attacks did not fundamentally change our understanding and the practices of surveillance, they justified: (1) an intensification, (2) integration and (3) globalization of surveillance sustained by (4) the increased use of cutting edge technology (Lyon, 2003). These four trends imply that through intensification, surveillance became more generalized and has created an atmosphere of permanent suspicion. Moreover, limits on the reach and scope of surveillance practices, for instance safeguarding privacy, have often been suspended. In addition, high-tech solutions allow for matching of dispersed sets of data over long distances.

New developments in surveillance practice led to either modifying the existing concepts or dismissing them completely. In fact, the numerous new ‘opticons’ identified by Haggerty are all attempts to adapt the initial concept of the prison to better fit contemporary surveillance practices. The ‘electronic panopticon’ (Lyon, 1994) and the ‘superpanopticon’ (Poster, 1995) are examples in which an attempt was made to integrate the proliferation of monitoring and investigation via electronic databases. Other scholars avoid the words Big Brother and panopticon and referred to these novel practices of surveillance as ‘dataveillance’, a blend of the words data and surveillance. (Amoore & De Goede, 2005, 2008b, Bigo 2006, Clarke, 1988, Haggerty, 2006, Levi & Wall, 2004).

In contrast to the vast body of literature on surveillance, there is surprisingly little literature specifically on financial surveillance. In authoritative work in surveillance studies (for instance Lyon, 2003, 2006) the financial aspect is virtually or completely absent. Nevertheless, among scholars studying the financial war on terror, there is a small group implicitly or explicitly focussing on financial surveillance. Several authors aim to shed light on the dynamics of financial surveillance.

Ibrahim Warde (2007) argues that after 9/11 free market fundamentalism that has become predominant in the 1990s had to be united with a ‘national security fundamentalism’. He argues that these contradicting logics of openness and deregulation on one hand, and surveillance and suspicion on the other, became compatible with each other through the notion of “gated finance”. This implies that ‘[a]s in gated communities, for a community to enjoy all freedoms, it had to be walled off from its messy surroundings. Outside those gates, ceaseless scrutiny would prevail’ (Warde, 2007, p. 109). Hence, after 11 September the free and open system of finance continued to exist for the financial institutions, businesses and citizens in the main industrialised countries while countries, businesses and individuals in or just connected to the rest of the world, especially the Islamic world, were considered risky
and placed under more scrutiny and surveillance. This latter group suddenly faced major restrictions and barriers and even exclusion from the global financial system.

From a similar perspective yet observing more continuity before and after 9/11, Peter Shields (2005) contends that liberalization of cross border financial flows and the innovations in IT led to a “loss-of-control narrative” with respect to the U.S. War on Drugs and subsequently the War on Terror. The storyline of this narrative is that besides the benefits of financial deregulation, increased openness of the financial system provides terrorists, drug traffickers and other criminals with new opportunities to commit crimes and to evade the eye of law enforcement. For this reason, increased financial surveillance is justified to ‘regain’ control over the financial system. As underscored by Shields, in the loss-of-control narrative the problem is presented as purely technological and procedural, leading to ever more surveillance to ‘close the technology gap on criminals’ (2005, p. 496). He convincingly argues that this logic successfully narrows down the scope of policy analysis and benefited certain institutional interests. Yet, the proliferating surveillance measures, or “finance warfare” (Shields, 2004) have not reduced the flow of illicit funds or terrorist attacks over the last decades.

The European regulatory initiatives are central to the work of William Vlcek. In relation to the broader field of surveillance studies, he introduces the term ‘financial panopticon’ (2008) or the discrete panopticon (2007, p. 102). While these notions are not yet fully developed, he argues that after 2001 financial surveillance has increased in scope and in intensity. He shows that on the one hand, suspicious transaction reporting duties have been imposed on new professions outside the finance and banking sectors and on the other hand, that the number of suspicious transaction reports has tremendously increased (2008, pp. 26-27). This increased monitoring and (in case of suspicion) reporting of financial transactions nationally and internationally appears to lead to what he calls a ‘financial panopticon’. He uses the term ‘discrete panopticon’ to emphasize that the under the EU’s Third AML/CFT Directive it is forbidden to inform clients that a transaction considered suspicious has been reported. Hence, this surveillance occurs in a covert manner. According to Vlcek the institutionalisation of CFT measures, such as UNSCR 1373 and 1617 give rise to the financial panopticon exerting a disciplinary power on a global scale (2007, p. 100).

While scholars studying financial surveillance often focus on particular aspects of the financial system and its regulation or on specific geographic zones or entities (charities for instance), there seems to be a quite common understanding about the practices that can be labelled as financial surveillance. Although there is a growing amount of literature on
financial surveillance and the informal banking sector, in particular ‘hawala’ banking (Atia, 2007, De Goede, 2003, Passas & Maimbo, 2008, Vlcek, 2010), the focus here is on the formal (Western) financial system. Concentrating on the formal banking sector, financial surveillance can be defined as ‘interrogating normal financial transactions of citizens and non-citizens in an attempt to identify the future terrorist’ (Vlcek, 2007, p. 100), money launderers or other types of criminals. In addition to their transactions, clients themselves are also subject to banking scrutiny.

Surveillance literature, including the works on financial surveillance, highlights two main concerns of surveillance practices: the violation of fundamental rights and exclusionary practices. Most critical and conventional scholarly work discusses concerns with regard to civil liberties, and in particular privacy. However, the precise meaning and the value of privacy is often left implicit. Aside from the slightly superficial debate on having (or not) something to hide, there is something more fundamental at stake when privacy is violated. Roessler explains lucidly that the value of privacy lies in the fact that, if privacy is a precondition for an autonomous life and if an autonomous life is at least one of the necessary conditions for a life that is good or rewarding, then the protection of privacy is necessary for a rewarding life (2005, p. 18). Surveillance through the collection of for instance biometric, travel, financial or other personal data, may lead to undesired access and interference in personal data of individuals. In other words, “informational privacy” may be violated through the lost control over personal information leading to a restriction of autonomy and freedom (Roessler, 2005, 2008).

However, due to the invisibility of the measures and the intangibility of their consequences it is often rather difficult to point out which civil liberties are at stake and how privacy is violated through financial surveillance techniques. Levi and Wall (2004) emphasize that financial surveillance restricts privacy in its three most common understandings; as the right to be left alone, in terms of control of one’s identity and as a right to be autonomous. In addition, it can be added that, the accumulation of surveillance intensive AML initiatives eroded traditional presumptions of financial privacy (Amicelle & Favarel-Garrigues 2009, p. 62, Shields, 2005, p. 490, 492), financial surveillance measures may be disproportionate in the sense that they may lead to harsh decisions on [innocent] customers (Amicelle & Favarel-Garrigues, 2009). More generally, it is argued that financial surveillance turns citizens into suspects deprived from their anonymity if they do not pay cash (Levi & Wall, 2004, Vlcek 2008).
Increased social exclusion is another important concern evoked in surveillance literature. Scholars have pointed out that the explanatory force of the panopticon and Big Brother seems to have shortcomings with regard to the societal effects of power. In contrast to the disciplinary effects of the panopticon over all subjects, they emphasized the exclusionary effects of surveillance. Bigo (2006) has referred to the exclusionary effects of surveillance, in physical or legal terms as a ‘ban-opticon’. He argues that today’s surveillance practices do not discipline and potentially transform all but they ‘deal with the notion of exception’ ‘surveillance for all but the control of only a few’ (Bigo, 2007, p. 6).

With regard to financial surveillance several scholars have highlighted that Know Your Customer obligations such as official identification documents and residence requirements, as well as a certain regular income to cover the costs of maintaining an account, exclude certain groups from participating in the formal banking sector. This may for instance be the case for migrant workers, recent immigrants, students, the unemployed, the homeless (Vlcek, 2007, p. 108, Amoore & De Goede, 2005, p. 154) and Muslims or those related to the Islamic world (Warde, 2007, p. 111). While it is not uncommon for poorer population groups in developed states to have neither a passport nor a proof of residency, this problem may be even more acute in developing countries (Amoore & De Goede, 2005, pp. 155-156). In addition, when individuals or institutions from developing countries have the necessary documents, financial institutions in the West often approach them with suspicion considering them (a too) high risk (Warde, 2007, pp. 110-114).

Building on the Surveillance Studies literature and its critiques, this thesis proposes an examination of the European fight against terrorism financing beyond the state as surveillant eye. Despite the fact that many scholars have moved beyond the iconic metaphors, contemporary surveillance literature often continues to be concerned with the state as the central authority carrying out surveillance. In this sense the panoptic gaze or Big Brother are certainly alive. Brouwer (2006), for instance highlights the quest for increased interoperability and integrated control through the support of new technologies in her analysis of databases related to border control in Europe (SIS, VIS, Eurodac). The study focuses on surveillance through national databases ‘allowing [national] authorities to collect more information’ (p. 138). Similarly, in his study on biometrics and European databases, Bonditti (2007) addresses their increased use by national authorities in particular the intelligence, police and customs services. While it is true that with regard to the crossing of borders national authorities play an important role and the SIS, VIS, and Eurodac databases are managed by customs and police services, this state-centred view appears to overshadow the growing contribution of
and entanglement with private authorities in providing surveillance. For example: the transfer of PNR data by airline companies or the development of biometric technology by private companies. Examining the fight against terrorism financing through the notions of governmentality and the professional field makes it possible to include a broader range of institutions and individuals that exercise power over society.

Second, the critique on surveillance practices can be extended and becomes more fundamental by broadening the angle of enquiry. For instance, Lyon argues that a surveillance society can be considered as ‘unjust and unfree’ (2003, p. 6). Contemporary surveillance, be it for instance CCTV, PNR or financial transaction monitoring, emphasizes individual behaviour. In combination with a culture of suspicion in which individuals are supposed to watch over each other and report anything suspect, surveillance undermines mutual trust and social solidarity. At the same time, it becomes more difficult to deviate from ‘the norm’. On the other hand, surveillance alters society since it withdraws trust and morality from social interaction transferring this responsibility to technological security devices. This implies that ‘surveillance (…) is deeply de-socializing as it disengages its subjects (…) from social belonging’ (Lianos quoted in Los, 2006, p. 84). In addition, despite its focus on individual behaviour and social interaction, surveillance technology is incapable of exactly reproducing the social considerations taking place amongst human beings since it is based on the programming of binary codes and the aggregation of a-contextual information that is analysed at a distant location.

The analysis of the European fight against terrorism financing through the theoretical notions of ‘governmentality’ and the ‘professional field’, allow us to go beyond a state-centric analysis of this fight and to establish its broader implications. The next sections will explain these theoretical tools in detail.

2.4 Governmentality

This section discusses the concept ‘governmentality’ which Michel Foucault introduced in his 1977-1978 lectures at the Collège de France entitled ‘Security, Territory and Population’ (2007, p. 115). During his lectures Foucault did not provide a finished or rigid theoretical framework of governmentality but indicated possible tracks for future research. Inspired by Foucault, numerous scholars have carried out research using the concept either in a general manner or following more closely the definitions given during the lectures (see, e.g.,

From a general perspective governmentality draws attention to the way in which power is shaped. Contrary to governance approaches such as multi-level governance that ask who holds power, Foucault is interested in asking what governance governs and how it does so. Being a combination of the words ‘government’ and ‘rationality’ (or according to some ‘mentality’ (Dale, 2004, pp. 178-179)), governmentality highlights the modes of thought that underpin practices of governing. It examines how governing involves ‘the production of particular truths’, drawing upon specific representations, knowledges, and expertise, and “how the history of these truths offers critical insights about the constitution of our societies and our present” (Larner & Walters, 2004, p. 2). In other words, the general understanding of governmentality focuses on ways in which a specific element of reality is represented and how this representation is inherently problematic as it is always bound up with power relations.

Foucault offers a more specific understanding of governmentality as being the result of a process that can be traced back to eighteenth-century Europe, by which the exercise of power has become gradually governmentalized. In this context, governmentality can be understood as:

> the ensemble formed by institutions, procedures, analyses and reflections, calculations and tactics that allow the exercise of this very specific, albeit very complex, power that has the population as its target, political economy as its major form of knowledge, and apparatuses of security as its essential technical instrument. (Foucault, 1991, pp.102-103, 2007, p. 108)

Following this definition, governmentality is a form of exercising power that is currently prevalent. However, it does not replace the other two mechanisms of power distinguished by Foucault: the legal or juridical mechanism and the disciplinary mechanism. These three forms of exercising power can co-exist, as ‘we could say that sovereignty is exercised within the borders of a territory, discipline is exercised on the bodies of individuals, and security is exercised over the whole population’ (Foucault, 2007, p. 11). The objective of this specific and complex form of power is to maintain itself and assure the survival of the state by governing over the population through the apparatus or mechanism of security. In order to make this form of control over the population possible, knowledge of the economy, broadly defined by Foucault as ‘all the processes revolving around population’ (2007, p. 106), is indispensable.
Studying the European fight against terrorism financing in line with this definition of governmentality means considering it as a apparatus exercising a specific form of power and implies examining the institutions, arts, techniques, and tactics that are mobilized in the fight. The meaning of ‘institutions’ is perhaps slightly confusing here, as Foucault also suggests going beyond the institution (see chapter 3) and highlights the importance of ‘free[ing] relations of power from the institution in order to analyse them from the point of view of technologies’ (2007, p. 118). To bridge this ambiguity, the word ‘institutions’ must be understood in a broad sense that includes not only formal institutions but all the participants in the field of governing. In order to emphasize this more fluid and informal understanding of the word institution and to avoid confusion, I rather use the word ‘participant’.

The exercise of power through procedures, analyses, calculations, and tactics can be summarized as arts or techniques of government, although Foucault did not exactly define these terms during his lectures. Examples of these techniques of government are, for instance, norms, regulation, and discipline. Fejes (2008) suggests that the arts of government attached to the apparatus of security can be understood as practices that intend to shape the conduct of the population by working through its desires, aspirations and beliefs. This expresses itself through multiple tactics such as regulations and standardizations of people’s conduct.

Concrete examples of techniques and arts of governing have been proposed by Foucault and other scholars through the use of case studies. For instance, Hindess (2004) contends that liberalism is to be understood not only as an ideology or political philosophy but also as a technique of governing. This implies that populations can be (partially) governed through the promotion of liberty. Likewise, Dean (2004) states that the domestic arts of government are based on liberalism in relation to political economy, which means that ‘rather than an act or decision on the part of the sovereign, governing [. . .] is about the subtle manipulation of the laws of production, consumption and distribution’ (p. 53). Considering the nature of governing in the European Union, it can be argued that harmonization (Barry, 1993) and the Open Method of Coordination (OMC) (Dale, 2004) are examples of arts of European government. The latter, for instance, is a form of government developed by the EU in the context of the Lisbon Agenda. It entails the use of means such as benchmarking, setting guidelines and peer review to further ambitious economic and social policies. Dale emphasizes that this method of supranational governance is ‘more than a merely technical device,’ as its introduction reinforces the idea that the European institutions have decision-making powers in these areas and that they can act effectively outside the conventional legislative decision-making process; this is the so-called community method (p. 175). The
strength of this focus on arts or techniques of governing is that it highlights the connection between the political, bureaucratic, and operational spheres, often taken for granted or artificially separated in EU studies.

Larner and Walters (2004) have made an important contribution to the debate by extending Foucault’s concept of governmentality to international concerns. Although Foucault and more general governmentality studies have mainly focused on the exercise of power within states, Larner and Walters assert that governmentality is not necessarily conceptually limited to the state. They argue that examining global governmentality contributes to ‘focussing more fully on the various ways in which governance at the level of the world has been problematized’ (Larner & Walters, 2004, p. 5). Global governmentality allows us to study and question power relations beyond the nation-state while taking economic, social, and political aspects into consideration. Moreover, the (global) governmentality perspective makes it possible to render visible a broader range of participants acting in the European field governing the fight against terrorism. It entails rejecting the assumptions of pre-existing political scales above and within the nation state and questioning the power constructions that produced these scales instead. In the words of Larner and Walters, it involves ‘problematizing the constitution, and governance of spaces above, beyond, between and across states’ (p. 2).

Walters (2004) offers an inspiring case study on the governmentality of the EU that combines the three approaches to governmentality described above. First, he explores the discursive framing of Europe. In which different ways has ‘Europe’ been explained and understood? What are the rationalities and mentalities that underpin political thinking and the policies of European integration? To answer these questions Walters takes the writings of the neofunctionalist Ernst Haas as example. He shows that Haas’s ideas on the governance of Europe are strongly inspired by the dominant societal discourses of the 1950s and 1960s and how these ideas make possible a particular style of governance, based on technocratic decision-making, modernization, and supranationality. A competing but less successful mentality of European government during the 1960s was for instance the idea of a European free trade area.

Secondly, Walters (2004) interrogates European governance at the level of its changing practices. He suggests the analysis of technologies of European government at three levels. The first level of analysis concentrates on micro-practices to describe the mundane techniques that have brought European integration into being. This includes ‘tabulations’, for instance, through scoreboards that show each member state’s progress with implementing
certain measures, making European integration calculable; ‘temporalization’ by means of setting out timetables and deadlines; and ‘geo-spatializations’ mapping out ‘Europe’ in specific ways (p. 161). A second level for analyzing the technologies of European government is what Walters calls ‘the machine’, after Foucault’s ‘apparatus’. By this he means ‘relatively durable arrangements of bodies, technologies, practices, instruments and spaces’ (p. 162). From this perspective, European integration can be understood in terms of different interconnected machines that form a new regime of governance. Examples of such machines are the welfare machine and the social market machine. A third level of analysis involves thinking about the EU as a site of novel ways of governing, ‘a laboratory of governmental arts and techniques’ (p. 165). Examples of political innovations that are specific to the EU are for instance comitology and the capacity for supranational law-making. But also practices of harmonization as argued by Barry and the development of a denationalized form of citizenship have been central technologies of European government.

This thesis adopts Walter’s dual approach to the governmentality of the EU, combining historical and empirical analysis. The analysis of the EU’s fight against terrorism financing must therefore be broadened beyond the decision-making institutions on the national and European level to the understanding of a transnational field also encompassing international organizations such as the FATF and the UN agencies as well as institutions within nation-states such as police and intelligence agencies. The governmentality approach also recognizes that non-state actors such as businesses, experts, NGOs, and citizens are all engaged in forms of governmental activity, both in relation to themselves and to others (Barry, 2004, p. 196). The inclusion of transnational entities such as the financial and banking sectors into this theoretical framework is indispensable, as private actors are increasingly expected to govern at a distance and participate in the War on Terror. Like governance theories, the theory of governmentality makes it possible to study the complex forms of governance between High Street retail banks and the institutions of the European Union.

2.5 Field Theory

One of the criticisms of governmentality studies concerns their strong focus on processes and the absence of identifiable actors in these processes (Larner & Walters, 2004, p. 4, Dale, 2004, pp. 184-185). The statements of Foucault quoted in the previous section seem to confirm his emphasis on the analysis of techniques of governing and a certain reticence in
the study of institutions. Yet, the possibility for analysing a broad and diverse range of participants opened up by the concept of governmentality is in fact one of its strengths. The governmentality perspective on the role of participants in the European fight against terrorism financing can be fleshed out by adopting a more actor-oriented analysis. Field theory, which shares a number of important assumptions with governmentality, offers such a theoretic lens.

Pierre Bourdieu developed the notion of field (champ) in order to examine the exercise of power beyond institutional and legal boundaries, and to study the consenting and conflicting relations of actors in a particular social space (inter alia 1983, 1992, 2005). A champ can be defined as

a field of forces within which the agents occupy positions that [. . .] determine the positions they will take with respect to the field, these position takings being aimed either at conserving or transforming the structure of relations of forces that is constitutive of the field. (Bourdieu, 2005, p. 30)

Thus, instead of studying individuals or institutions, for instance the European Commission or a national parliament, Bourdieu suggests examining a ‘field of politics’, an invisible structure of relations among a range of individuals and institutions. Countless fields can be distinguished. Bourdieu for instance explored the fields of politics, social science, journalism (2005), and religion (1991) but also fields such as German philosophy (1991) and cultural production (1983).

Like governmentality, field theory considers a heterogeneous set of participants, in Bourdieu’s terminology ‘agents’, irrespective of institutional, legal, and, we could add, geographic boundaries. Fields are social universes with a certain degree of autonomy with respect to other fields. Bourdieu (2005) makes clear that studying the field of for instance philosophy should not only involve the texts of a philosopher but should also include a larger social context, for instance other philosophers, and the caste of commentators, publishers, and universities. What holds a field together is the fact that ‘each field obeys certain specific and more general rules and is structured by conflict of those who want to maintain their power and others who want to take over this power’ (Bourdieu, 1992, p. 171). In other words, a field makes visible what power relations exist within the field and how the field is structured by the relative positions taken by the actors.

Didier Bigo has developed field theory further by analysing the ‘field of professionals of management of unease’ (2005, 2006) and the ‘field of EU internal security agencies’ (Bigo et al. 2007). Bigo et al. (2007) define a field (referring to the field of professionals of security) as ‘a bordered and fragmented social space that, in spite of its heterogeneities, can be
analysed as being structured by a set of common beliefs, practices and meanings’ (p. 8). The field is structured by professional and/or bureaucratic power relations and struggles over specific social resources, called ‘capital’ by Bourdieu, determining what is at stake in this field. The positions of the social actors in the field and the relational and relative positions between these actors can be mapped by analysing their discourses, practices, institutional characteristics, and objective positions (ibid., pp. 8-11).

This theorisation draws attention to another parallel between governmentality and field theory. Both approaches emphasize the importance of representation in terms of discourses, common beliefs, and meanings. In fact, Bigo’s work can be understood as a way to operationalize what Foucault called ‘the ensemble of institutions, procedures, analyses and reflections’ (Foucault, 1991, pp. 102-103), and establishes a link between actors and processes.

It also provides an indication of how power is exercised in the professional field. In his study on the field of professionals of the management of unease, Bigo (2006) distinguishes four non-mutually exclusive dimensions in which the field may operate. First, the field can be understood as a ‘field of force’. This implies that pressure is exercised on the actors in the field to share a specific definition and reading of a problem, pulling actors together like magnets and creating a homogenization of the field. Secondly, the field can be one of struggle. This means, as alluded to above, that actors in a field do not share the same beliefs and interests and use their resources to compete with other actors in the field. A third understanding concerns the field as a field of domination. In this case, one field dominates over others by its participants claiming superior expertise on a certain issue and imposing their view and definition of this issue. As a consequence of the domination of one field, alternative views are excluded. Finally, the field can entirely or partially shift into a new transversal field. This term refers to the demarcation of a space beyond the nation-state but without inscribing it into an international or European space. It expresses that the field (of (in)security) ‘is deployed at a level that is reducible neither to the national political field nor to a level between two nations or the European level’ (Bigo, 2006, p. 29). In this thesis, Bigo’s typology will be taken into account to characterize the exercise of power in the European fight against terrorism financing.

If the European fight against terrorism financing is understood in terms of a transnational field, some practical questions immediately arise. A first question is how to determine which participants are part of the professional field. Although governmentality and field theory open up analysis to ‘new’ participants, the social space of the field is not
unlimited but bordered and fragmented. These two features are important since they allow us to value hierarchies, underscore processes of exclusion and inclusion, and help distinguish between central and peripheral actors (Bigo, 2007, p. 8). The exact borders of the field are however difficult to define in black and white; rather they emerge from the analysis of formal and informal relations between actors, for instance through the study of legal documents and interviewing key actors in the field. Moreover, the field is not homogeneous, but on the contrary, a heterogeneous set of actors. The field of security professionals for instance includes: police, the military, customs officers, judges, and border guards. Furthermore, field theory does not consider institutions as a monolithic bloc but as a collection of individuals who are also subject to inter-institutional power struggles. Within the European Commission for instance, Direction General (DG) Home Affairs, DG Justice, and DG Relex (Foreign Affairs) may have differing priorities, views and interests in the fight against terrorism. These inter-institutional turf wars have been widely discussed in the European studies literature (inter alia Den Boer, 2003, Dijkstra, 2009, Spence 2012).

Secondly, to understand what is at stake in a particular field it is important to render visible the social practices between actors in the field such as ‘professional and/or bureaucratic struggles, power relations and bordering mechanisms’ (Bigo et al., 2007, p. 8). Although the various actors are interdependent and brought together in one social space, their interests may diverge and they may not share a coherent set of beliefs (Bigo, 2006; Bigo et al., 2007). Yet, even if they do not agree on the same possible solutions, actors in the field largely share a common definition of the problem. For example, privacy groups and national governments may disagree on privacy safeguards that need to be included in a counter-terrorism law or international agreements but agree on the privacy issues involved.

Last but not least, the borders of the field as well as the definition of what is at stake are mobile and evolve over time, as ‘[t]he fundamental thing is that any action undertaken by one agent to shift the economy of forces in his favour has repercussions on all the other actors as a whole’ (Bigo, 2006, p. 24).

Building on this discussion of field theory, in the European field of governing terrorism financing there are three new directions for the analysis of the field: the inclusion of the private sector, vertical analysis of the field and a focus on technology. First, considering the importance of the use of commercial data to the fight against terrorism financing, the inclusion of private authorities seems indispensable for the analysis of this fight. In current research on the European Union inspired by field theory, private actors are often absent. Indeed, Bigo acknowledges that ‘our understanding of these private actors is still incomplete’
(2006, p. 26) and has not yet received extensive scrutiny (2007, p. 10). This gap in existing literature will be addressed here as private actors are taken seriously as part of the field of governing the European fight against terrorism financing.

A second new direction is the focus on a vertical rather than horizontal field of relations. The field of the EU internal security agencies assessed by Bigo et al. (2007) is concentrated —for practical reasons rather than principled ones— on the European level. Consequently, what becomes visible from mapping the field of EU internal security professionals are the power relations between them. This focus on actors operating on the same geographic level is what I describe as horizontal. The objective of this thesis is to examine the fight against terrorism financing from the inception of CFT measures to implementation, output, and monitoring, including decision-making and decision-makers at an international, European, and national level in the public and private sectors. This approach from Brussels to banks is what I would call a vertical analysis.

A thorough investigation of all 27 EU Member States is impossible here. Yet, the objective is not to give a complete overview of all actors involved in the field but to understand by which actors and what practices the European fight against terrorism financing is governed and how international, European, and national efforts translate into daily security practices. Even though incomplete, examples from various countries will illustrate the ways in which the fight against terrorism financing produces new modes of governing within the EU and what the political and societal implications of this fight are.

Thirdly, an important aspect of Bigo’s analysis of the field is the understanding of this field as relational and transversal (Bigo et al. 2007, p. 8, Bigo & Toukala, 2008, p. 14, Bigo, 2011). This means looking at the value-based assumptions, discourses, and rules of the game that have been established among the participants of the field. Instead of following an exclusively institutional, sectoral, or national approach, field theory highlights the similarity of the professional and educational backgrounds and the motivations of, as well as the solidarity or struggles among, the participants in the field. Although this is a very interesting approach and shared values and social trajectories of participants are also visible in the field governing the European fight against terrorism financing, I will put less stress on relative positions and social trajectories. Instead, given the centrality of financial data in this thesis and the crucial role of databases and analytical software programmes for governing terrorism financing, more attention is given to the role of technology.6 Scholars in science and technology studies, notably Donald MacKenzie and Bruno Latour, have argued that ‘the process of creating and adopting technologies is complex, interactive and political’ (Mort,
They show that technologies are not appearing and developing in a neutral and static manner but are shaped and given meaning by human beings and society as a whole. They highlight that technologies have histories and may embody specific knowledge and values. In turn, technology also shapes and alters society. This approach to studying technology corresponds with and enriches the governmentality and field approaches described above. The last section of this chapter proposes two separate fields of governing the European fight against terrorism that are mapped along the theoretical assumptions discussed in this section. However, in the next section I first discuss the methodology adopted in this thesis.

2.6 Methodology

The discussion of governmentality and field theory leads us to the following three research foci that have inspired the methodological framework of this thesis. First, the general understanding of governmentality draws our attention to representational practices. How does a problem emerge? How is it defined? Which aspects are subject to political contestation and which are not? This is developed in more detail in the next chapter through the Foucauldian notion of genealogy. There, I discuss the way in which the European fight against terrorism financing is represented, and what construction of truths this involves.

Techniques of governing are a second research focus. Foucault’s detailed definition of governmentality emphasizes the study of governing practices. Which money and what behaviour is precisely targeted through CFT measures? What kind of governing practices emerged in the fight against terrorism financing? What are the political and societal implications of these practices? From this perspective, power is exercised through technocratic and technological processes at the micro level dispersed over a range of public and private actors. Special attention is given to the role of technology, in particular risk and link analysis software and international financial databases.

The professional field is a third research focus in this thesis. Field theory contributes to governmentality by providing a more actor-oriented approach. Analysis of the professional field highlights who is participating in the European field of governing terrorism financing. How have interests and understandings developed and diverged in the field? What are the tensions and problems?

The following paragraphs explain the choice for case studies, documentary research, textual analysis, and elite interviewing as suitable methods in relation to these research foci.
They also describe how these research tools have been used and reflect on the limitations of these methods.

2.6.1 Case Studies

As mentioned in the introduction, the ‘SWIFT affair’ and the EU’s Third AML/CFT Directive have been selected as case studies in this thesis. The use of case studies is very suitable for the type of research carried out in this thesis for three reasons. First, case studies are a preferred method when the research focuses on a contemporary topic with a real life context (Yin, 2009, p. 2). This is precisely the case when exploring the practices created in name of the European fight against terrorism financing. When the Data Wars project, carried out by Durham University and the University of Amsterdam and of which this dissertation is part, started in 2008, there was little academic information available on this fight and even less on the daily practices set in motion. Concentrating on these two specific case studies has helped to gather and open up a lot of detailed information.

Secondly, case studies are useful for investigating social processes (Swanborn, 1994, p. 316). By concentrating on a specific case it becomes possible to analyse interaction on the micro level. This can include, for instance, the creation and reproduction of meaning, the emergence of disagreements, the different steps in the decision-making process, or the mapping of the various perspectives and motives of participants. The analysis of social processes taking place in these two case studies has been crucial for studying the exercise of power in name of the European fight against terrorism.

Thirdly, a case study allows for a thorough investigation of a complex issue (Swanborn, 1996, p. 38). Contrary to a causal model that measures specific pre-defined variables among a significant set of respondents at the moment of the survey, a case study considers a range of meaningful features or causes of one specific case over a certain period of time. In other words, case studies can offer a holistic approach (Swanborn, 1996, p. 26, Yin, 2009, p. 4). This holistic aspect of the case study also explains why case studies have been used very frequently in studies of governmentality.

The selection of the case studies must respond to the core concepts of the research question (Klotz, 2009). The SWIFT affair and the Third Directive have been selected as case studies because these are the main ways in which the war on terrorism financing has taken shape in Europe. They are both examples of the use of personal financial data for security and, more specifically, counter-terrorism purposes in Europe. Both are also part of a broader
turn to commercial databases for security purposes and fit in a spectrum of examples such as the PNR and e-border cases investigated by the British research team of the Data Wars project, and the use of telecommunication and internet data, and even purchase information.

Yet, the two case studies also have important differences. First of all, the Third Directive is a legal framework concerned with suspicious transaction reporting that has never raised much societal or political controversy. It is a rather specific and detailed instrument that requires specific entities mainly in the banking and financial sectors to comply with certain counter-terrorism requirements. Because of its seemingly undisputed character and the fact that the Directive mainly affects the internal organization of a specific group of businesses, it has been largely invisible. The SWIFT affair on the other hand has been highly visible and controversial as it entailed the transfer and surveillance of international wire transfers, that were initially illegal according to European law. In this case, the US and European political scenes play an important role. The difference between the two cases is important to provide a more complete understanding of the practices at work through the European fight against terrorism financing. The next section discusses the qualitative research tools adopted to investigate the two cases.

2.6.2 Documentary Research and Textual Analysis

In addition to the study of academic literature, this thesis is based on extensive documentary research. This includes the analysis of: official reports from public and private authorities, press releases, political statements, laws, policy documents, (transcripts of) parliamentary hearings and debates, international press articles, internet blogs and journalistic books. These have been very valuable sources for examining the way in which the European fight against terrorism financing has been defined and represented. Documentary research helps in reconstructing events, tracing decision-making procedures, and examining the range of arguments and opinions held by the participants governing the European fight against terrorism financing. In addition, documentary research helps to shed light on the techniques of governing. For instance, legislative texts prescribe the action required from banks and financial service providers and banks’ annual reports often mention which steps have been undertaken by the bank to comply with the law. Journalistic works, on the other hand, were crucial to reconstructing the practices developed in the Terrorism Finance Tracking Program (TFTP). In chapter 4 documents have been used more systematically for a textual analysis in order to investigate how participants in the field governing terrorism financing supported or
contested the TFTP. This section discusses the potential pitfalls of documentary research and the adopted methodology for textual analysis.

Although (official) documents appear to constitute stable and objective evidence, they are in fact socially produced for a certain purpose on the basis of certain ideas, theories, or principles (Atkinson & Coffey, 2004, Bryman, 2008, Gilbert 2008). For this reason, it is important to reflect on the interpretation and meaning of documents. Scott (1990) distinguishes four criteria for assessing the quality of documents. First, the authenticity of the documents needs to be established. Given the fact that most documents used in this thesis are of very recent date and available through libraries or on the official websites of the investigated public and private authorities or media outlets, it is not very likely that these are falsified or wrongly copied. In this sense authenticity has not been a matter of concern. Authenticity can also be an issue of concern when the authorship of the articles is unclear (Bryman, 2008, p. 525). However, in the context of this thesis, this has not been problematic.

Secondly, the credibility of the texts merits consideration. One can for instance wonder whether the quotes from anonymous sources in journalistic books or articles are reliable. But also official statements made by politicians and government officials can be biased and in strong contrast with for instance the actual legal arrangements. The credibility of the text can be assessed by reflecting on the following questions: Who produced the document? Does the author have an interest in distorting the truth? And why, when, and in what context was the text written? (Gilbert, 2008, p. 294). Although it is unquestionably important to know if statements or documents can be attributed with certainty to a person or organization, it must, however, be stressed that the aim in this thesis is not to establish the credibility of texts in the sense of being representative of the truth. In fact, it is through the confrontation of differences in the presentation and interpretation of arguments and facts that the rationalities that underpin the European fight against terrorism become visible and can be understood.

A third criterion is the representativeness of the document or the set of documents. This issue has been especially important with regard to the textual analysis discussed below. In general it can be said that with the help of Internet search engines and public databases a wide range of documents published by public and private actors have been consulted on each of the case studies. Nevertheless, it must be noted that only official and publicly available documents have been consulted. Internal or confidential correspondence, minutes, and memos fall beyond the scope of this research.
Last but not least, Scott (1990) states that the meaning of the document needs to be established. In this respect, a distinction can be made between the literal meaning and the interpretative understanding. According to him, ‘at its simplest, interpretation requires an understanding of the particular definitions and recording practices adopted and of the genre and stylisation employed in the text’ (p. 30). The hermeneutic process of interpretation goes a step further as it also involves ‘interpretative understanding of individual concepts, appreciation of the social and cultural context through which the various concepts are related in a particular discourse and a judgement on the meaning and significance of the text as a whole’ (Scott, 1990, p. 31). Hence, in order to interpret the meaning of the text it is important to investigate the situation and the intentions of the author as well as the societal context in which the text was written. This kind of interpretative research can be carried out through textual analysis.

Chapter 4 offers a textual analysis of the debates concerning the SWIFT affair in, respectively, the US and the EU. There are various approaches to textual analysis ranging from semiotics to more quantitative forms of context analysis. In chapter 4 the approach followed by Huysmans and Buonfino (2008) has been adopted. In their article they have investigated how and in what instances British politicians represent or contest nexuses between terrorism and immigration. For their analysis, they selected all parliamentary debates on terrorism that took place in the House of Commons and the House of Lords during a certain period. The dates they have chosen include the debates following 9/11 and the Madrid bombings. They also included some key debates held in 2005 especially debates that took place after the London bombings, to verify of any important changes had taken place. In a first stage Huysmans and Buonfino have searched the written transcriptions of the parliamentary debates through Hansard, the edited verbatim reports of the proceedings of the British parliament, using the keyword ‘terrorism’. Then, they refined their search through words related to immigration. Next, debates containing both themes were read for meaning, structure and connection with other themes. As such they analysed how certain dangers were politicized and how insecurity was framed around the migration/terrorism nexus (2008, p. 768).

Chapter 4 investigates how and at which moments the SWIFT affair was (de)politicized in the US and in the EU. The main sources for this analysis are newspaper articles. Two different considerations explain this choice. Aside from the fact that journalists initially revealed the SWIFT affair, so far most information has been published by the press. Moreover, newspaper articles are also a place where the multiple participants involved in the
field (political leaders, privacy groups, law-enforcement officers, and spokespersons from SWIFT) are made to interact and different opinions can be traced. While other sources, including parliamentary debates, international agreements, court rulings, and the study of the relations between the participants in the field, are also taken into account and enhance our understanding of the SWIFT affair, they are far less comprehensive with regard to the quantity of information and often offer a less all-round view on the affair.

However, the importance of investigative journalism for our analysis of the SWIFT affair provokes some reflection on the value and the risks of using media sources. Gilbert emphasizes that the media are selective in what they decide to publish and from what angle they report on issues (2008, p. 289). This selectivity and even self-censorship is illustrated in the discussion of the revelation of the SWIFT affair in chapter 4 and is also discussed in the context of the discussion of the SWIFT programme as a black box in chapter 5. In addition, it must be kept in mind that newspaper articles may contain errors in the facts they present, they may be subject to distortion at the level of the editor, the journalist, or the initial source, and they are written with a specific audience in mind (Gilbert, 2008, p. 289). These potential risks have been carefully taken into account in the examination of newspaper articles.

The textual analysis of the debates on the SWIFT affair in the US and in the EU is based on newspaper articles available in the Lexis-Nexis newspaper database between 23 June 2006—the revelation of the Swift affair—and 31 August 2010, the month during which the latest US-EU agreement was adopted. This database contains all major and regional American and European newspapers as well as Canadian, Australian, and Asian newspapers. All English, French and Dutch newspapers offered in the database have been included in the search and have been systematically investigated (for a complete overview see Annex 2). I believe that this comprehensive approach, yet with a focus on the leading US and EU newspapers, constitutes a representative selection for the analysis of newspaper articles.

The articles on the SWIFT affair have been selected through searching for the acronym “SWIFT.” Subsequently, all articles containing the word ‘swift’ but referring to for instance a specific car, football clubs or doing something rapidly instead of to the SWIFT affair were filtered out. Additional searches were made using the words “banking data.” The next stage involved reading the articles and searching for and listing the arguments made in relation to the SWIFT affair. Which words were used? Which themes were raised in the debate? Which arguments were used to defend the various views held in the SWIFT affair? Which solutions were proposed to ‘solve’ the SWIFT affair?
A last comment with regard to document research is the fact that organizations’ official documents usually disregard social interaction and struggles, as they are considered irrelevant or undesirable for the final version of the document. For this reason Atkinson and Coffey (2004) argue that documents have a distinctive ontological status, in that they form a separate reality, which they refer to as a “documentary reality.” In order to complement and question the “documentary reality,” interviews with key persons have been carried out.

2.6.3 Elite Interviewing

Qualitative interviews have been a preferred methodological tool for understanding the construction of meaning in, as well as the practices and struggles of, the professional field of governing terrorism financing. This form of interviewing helps to discover the reasoning, motivations, attitudes and opinions of the respondent with respect to a certain subject. Qualitative interviews are also useful to unfold the content and pattern of daily practices and experiences (Gilbert, 2008, Kvale, 1996, McCracken, 1988). Furthermore, interviewing can provide insights into organizational and institutional processes and can make connections between different individuals and organizations visible (DeVault & McCoy, 2003).

The interviews carried out for this research project have been extremely valuable in reconstructing the social interaction that has taken place between different participants in the field of governing as produced through the European fight against terrorism financing. They provided insight into the self-definition of participants in the field and the problems they encountered. The interviews provided information about the way in which issues have been solved, how ideas evolved, or how they remained points of disagreement and contestation. Interviews were also an important tool to understand how measures for combating terrorism financing have been translated into daily practices and how the technologies used for this purpose operate.

The approach taken in selecting respondents and carrying out the interviews can be qualified as elite interviewing, which is a distinct form of qualitative interviewing. Despite the use of the word elite, this form of interviewing ‘can be used whenever it is appropriate to treat the respondent as an expert about the topic at hand’ (Leech, 2002, p. 663). An elite interview is therefore ‘an interview with any interviewee who in terms of the current purposes of the interviewer is given special non-standardized treatment’ (Dexter, 1970, p. 5).

In practice, the interviews were semi-structured around a set of major open-ended questions in order to guide the conversation. The advantage of semi-structured interviews is
that they allow the interviewer to ‘alter the sequence of questions and probe for more
information’ (Gilbert, 2008, p. 246). They also leave more freedom for the respondent to
illustrate his or her answers with examples or anecdotes or to touch upon related issues. The
questions of the interviews can be divided between a core set of introductory questions—
Gusterson speaks of “icebreakers” (2009, p. 104)—and thematic questions that were asked of
everyone. For example, most interviews started with the question, ‘Can you describe your role
in [organization X or situation Y]?’ After establishing the role and practices of the
interviewee and the situation, other general questions were, ‘What is your opinion on the
usefulness of financial data for combating terrorism?’ and ‘Do you believe that security
practices based on financial data will remain of key importance in the future?’ Depending on
the expertise of the interviewee the questions concentrated either on the Third Directive or on
the TFTP and in some cases on both topics.

In addition, more tailored questions were asked in relation to the particular function
and expertise of the respondent. For instance, ‘Can you explain how a financial transaction
becomes seen as suspicious?’; ‘When do you send a suspicious transaction report to the
Financial Intelligence Unit?’; ‘What are according to you the most important improvements
that are needed to render the TFTP acceptable?’ and, ‘Can you give examples of how your
government tried to influence the FATF negotiations?’

Furthermore, it must be stressed that ‘a non-standardized approach is valuable where
the subject matter is sensitive or complicated’ (Gilbert, 2008, p. 248). Such was precisely the
case with the Third AML/CFT Directive and the SWIFT affair, which were both surrounded
with certain levels of secrecy and arrangements little known beyond circles of financial
specialists and a small group of European officials. Open and non-standardized questions are
well adapted to these situations as they leave some leeway to the interviewee to choose his or
her own words and interpretation of the situation to respond to the question.

For the purposes of this research project, 28 elite interviews with key persons were
carried out (for an anonymised list, see annex 1). Key persons or respondents for interviews
were selected through three strategies. First, important public and private actors such as the
European institutions, banks, and non-governmental organizations were mapped and key
persons within these organizations were identified and contacted. Secondly, a ‘snowball
method’ was used, asking the first (and most visible) key informants for further contacts in
the field governing the fight against terrorism financing. Thirdly, evaluating the preliminary
results of the interviews and the literature survey of the case studies, a last set of respondents
was interviewed in order to cover certain specific topics in more depth.
All interviews were tape-recorded and subsequently transcribed, except for two cases in which the interviewees preferred not to be recorded. In these two cases only handwritten notes were taken. Compared to note taking, recording allows a more thorough examination of the respondent’s answer because of the possibility to repeat to hear the complete answer in the original wording. As such, the context remained intact and could be verified or played back in later stages of the research. It was important to conserve the exact wording of the answers because of the sensitivity of the subject on the one hand and in order to compare the opinions and positions of the different actors carefully on the other. On a few occasions the respondent wished to speak off the record. However, the ‘off the record’ information or statements relevant to this research also became available in public documents at a later stage of the research project. Interviews took place on location in Amsterdam, Brussels, London, Paris, and Washington D.C. in English, French and Dutch. Two interviews were carried out and recorded by telephone. The duration of the interviews was on average between one hour and one and a half hours. In order to guarantee the anonymity requested by some interviewees, all respondents were assigned numbers and divided into broader professional categories.

As interviewing is a social activity and the interviewer and the interviewee will react to each other’s appearance, declarations, and behaviour, the methodology of interviewing also merits some reflection. Qualitative interviewing literature widely recognizes ‘interviewer effects’, that is, the influence of the interviewer on the interviewee. Respondents can be influenced by the appearance and language of the interviewer (McCracken, 1988, pp. 25-26) as well as by the interviewer’s behaviour and conduct of the interview (Gilbert, 2008, p. 256), which can for instance be too formal or too informal. Attempting to minimize the interviewer effects, a professional and open style was adopted during the interviews.

Another important, but less acknowledged, pitfall of the interview as methodological tool is the decreasing distance from the research object that may affect the interviewer. This could be called the ‘interviewee effect’. For the use of elite interviews as part of a research project, the interviewer is entirely dependent on the interviewees to share their time and knowledge. Moreover, the activity of elite interviewing may create empathy for the interviewee as the interviewer and the interviewee spend a considerable amount of time discussing a topic in which they are both interested and they often have coffee together. The willingness of the interviewees to participate in the research project and the attempts of the interviewer to understand the opinions and situation of the interviewee may consciously or unconsciously affect the independence and objectivity of the interviewer’s analysis. Awareness of the occurrence of interviewee effects as well as the anonymisation of
interviewee’s statements help to maintain an appropriate distance and independence towards the interviewee.

According to Latour (2000), the structure of the interview as a methodological tool (i.e., where the interviewee responds to the questions of the interviewer) may also influence the objectivity of the research outcomes. He argues that the results of a research interview might be distorted because the interviewees’ objections to the researchers’ questions or the research agenda are not accurately taken into account (p. 116). Yet, instead of ignoring the objections raised because they do not follow the research agenda or because they embarrass the interviewer, these objections can provide new insights into the research topic or alert the interviewer to his or her erroneous assumptions about the interviewee (Tanggaard, 2008).

Another concern is the reliability of the response to the interview questions. It is important to keep in mind that respondents are not obliged to give objective and truthful answers (Berry, 2002, p. 680). They can also be tempted to give politically correct answers, answers anticipating what interviewers want to hear (Gilbert, 2008, p. 255), or to exaggerate their own role (Berry, 2002, pp. 680-81). These issues were considered when deciding to send the interview questions and a short introduction of the research project to respondents ahead of the interview. To limit the influence of these documents on the response of the interviewee these documents were phrased in a rather open and general style. Yet, considering the chances of biased answers through prior knowledge of the questions versus the advantages of prepared and reassured respondents, the latter was deemed more important. Moreover, since the topics discussed in the interviews were often considered as sensitive by respondents, I believe it is desirable from an ethical perspective to assure a high level of transparency towards respondents. Furthermore, the same questions were asked of several persons of the same professional group, making it possible to compare the responses. It must be stressed however, that one of the objectives of carrying out interviews in this research project was also to discover the interviewees’ (biased) views on a particular situation or practice as well as their opinions on their role and the roles played by others.

The sensitivity of the information discussed during the interview was also at stake with respect to the request of many respondents—in particular some of the lower ranking ones—for anonymity. This does not only protect the respondent in his professional environment, but as McCracken highlights; it also permits respondents to speak with more candour (1988, p. 27). Indeed, for the present research, it is not the identity of the respondent that is relevant but the role of this person within a specific institution or professional category and the larger professional field.
2.7 Mapping the Participants of the Professional Fields

This section presents two maps of European professional fields of governing terrorism financing. For this mapping exercise, the field can be defined as a relational space that encompasses all private and public, national and international participants that are involved in standard setting, decision-making, implementing monitoring, or otherwise influencing the EU’s measures to combat terrorism finance. These maps help visualize at a glance the heterogeneous set of public and private participants operating in the field and also provide an overview of the key persons that have been analysed in this thesis through interviews and documentary research. As in (most of) the field maps produced by Bigo et al. (2005, 2007), the participants in the field are divided over two axes. Yet, the meaning given to the axes differs. The horizontal axis contrasts representational with operational power. In short, representational power involves the contribution to the production of particular truths, while the operational power entails the daily practices carried out to execute the law. The vertical axis reflects different geographic scales and is comparable to the vertical division of the field map of European Security Agencies (Bigo et al., 2007). However, instead of a transatlantic, European and national level, the field maps in this chapter distinguish between a local, national, and an international/transatlantic level for the SWIFT affair and a local, national, and international level for the Third Directive. In addition, it must be emphasized that the axes on the map are not impenetrable dividing lines and interaction and influence between representational and operational powers as well as between geographic scales occurs.

These maps are limited because they provide a snapshot of the professional field at a certain moment in time, while in reality the field is continually evolving as participants may enter or leave the field at some point. Moreover, the distinction between groups of participants is in reality messier than the maps may suggest for at least two reasons. First, during the interviews it became clear that it was not uncommon for interviewees to have gained professional experience in for instance both banking and law-enforcement environments. One of the interviewees had even combined three different positions in the field as he had worked on anti-money laundering cases within the national police, for a major international bank, and as a consultant and trainer on AML-CFT issues. This finding is in accordance with the works of, for instance, Favarell-Garrigues et al. (2008, 2009) considering the professional trajectories of professionals fighting dirty money. Secondly, organizations pictured on the map are not unitary actors but consist of different services and individuals that may have conflicting interests. Furthermore, like all models, the positioning of participants on
the map is to a certain extent a simplification as the field is in constant flux and relative positions may change.

Despite these weaknesses, the value of the maps is that they help us visualize the fragmented and heterogeneous set of participants that operate in the European field of governing terrorism finance. Contrary to certain more conventional models of European governance, these field maps make it possible to transcend the divisions between national and international actors on the one hand and public and private actors on the other. In addition these maps also reveal something about the techniques of governing that are used in the field.

Although this thesis speaks of a European field of governing terrorism finance, each case study has a distinct professional map. This choice has been made for analytical purposes. The overview of and relations between participants of each case study are easier to grasp in separate maps. A comparison of the separate maps shows that there is some overlap between the two maps, notably in the section in the upper right showing international representational powers such as the European institutions. Yet, including the participants of the two case studies into one European field of governing could also lead to confusion because certain participants are specific to only one case study. The Financial Intelligence Units for instance are absent in the field map of the SWIFT affair as they have no role with regard to this case study. On the other hand, privacy and civil liberties groups have not mobilized themselves in response to the EU’s Third Directive. These considerations have to be taken into account of in the professional field maps described below.

2.7.1 The Professional Field Map of the SWIFT Affair

Most participants in the SWIFT affair are positioned in the upper left quadrant of the map which indicates that they exercise representational power acting on an international, or, to be more precise, transatlantic level (see figure 2.1). In this field map, to exercise representational power means being involved — as a decision maker or as a stakeholder— in the development of CFT policies and through this involvement advancing or contesting particular discourses and practices regarding (the fight against) terrorism financing and the use of financial data. It includes the US government and in particular the US Department of Treasury and the European institutions. The European Data Protection Supervisor (EDPS) and the Article 29 Working Party of national privacy commissions of the EU member states were also actively involved in the SWIFT affair. This quadrant also includes non-state actors such as civil liberties groups that have mobilized themselves regarding this case in several
countries, the largest international banks that have been aware of the TFTP, consultancies, and last but not least SWIFT representatives who were directly involved in the development and negotiation of the TFTP.

The representational powers at the national level that are involved in the SWIFT affair, represented in the lower left quadrant, include the Ministries of Finance in the EU member states. Some of these ministries and national central banks or financial services authorities were aware of the TFTP since before the revelation of the programme. All were involved in the negotiations with the US following the publications on the SWIFT affair. Other participants at the national level include national parliaments that discussed the affair as well as national privacy commissions in all member states and in particular the Belgian Privacy Commission. Privacy and civil liberties groups have also been engaged at a national level. Journalists who have revealed or investigated the TFTP are considered representational powers as their reporting structured the SWIFT affair. They are positioned at the national level on the map as they work for leading national newspapers and write for national audiences to begin with. However, their contribution to the way in which the SWIFT affair became represented had a global reach in some cases.

Participants holding operational power, shown in the quadrants on the right, are involved in the implementation of CFT policies and actually attempting to track terrorists and their financiers. However, these participants are not mere ‘executers’; it must be stressed that these activities have a political dimension and are structured by certain beliefs and values. In the SWIFT affair, the thousands of nationally implanted correspondence and investments banks that make use of SWIFT’s financial services network, SWIFTNet FIN, can be qualified as operational powers. SWIFTNet FIN is located on different servers around the globe, and supports the vast majority of international transactions between banks worldwide; as this network needs maintenance and development it can also be seen as an operational power. Furthermore, the CIA played a crucial role in developing the TFTP and analysing SWIFT’s financial data. Another important private sector participant is the Booz Allen Hamilton Corporation. In 2010 Europol also acquired a role in the TFTP.

2.7.2 The Professional Field Map of the EU’s Third Directive

As in the SWIFT affair, most participants in the professional field map of the EU’s Third Directive are representational powers operating on the international level (see figure 2.2). However, in this map the focus is rather on international organizations such as the UN,
the Council of Europe, and the FATF, instead of the US authorities. Of course this map also includes the EU institutions. In addition to the European Commission, the Parliament, and the Council, the European Court of Justice has also had some power in this professional field. The private actors present in this part of the field consist of national and international professional interest groups such as the European Bar Association, and various associations representing the banking and financial services sectors. International banks are also represented at the European and international levels. Internationally operating consulting firms such as John Howell and Deloitte are also part of the professional field.

On the national level there is again some overlap between the participants of the two case studies. With regard to the Third Directive, national parliaments, Ministries of Finance, and national banks and financial services authorities were involved in negotiating and/or monitoring the Third Directive. National central banks and financial services authorities also have responsibilities in monitoring compliance with the Third Directive. There is also a minor role for the ministry, often either the Ministry of the Interior, Justice, or Foreign Affairs, that determines the blacklisting of individuals suspected of terrorism.

The professional field map of the EU’s Third Directive includes more actors on the national and sub-national operational level compared to the SWIFT affair. First of all, it comprises the Money Laundering Reporting Officers (MLRO) who are operating in all the local bank offices spread throughout the EU member states. These local banks are in turn controlled, supported, and monitored by the national legal and compliance departments of banks. These are for instance located in ‘the City’ of London, and along the ‘Zuidas’ in Amsterdam. Nationally operating consultancy and training companies can also be considered operational powers as they are for instance asked to assist banks or other financial services providers with the implementation of the Third Directive. Their work can be interpreted as more representational when consultancies advise governments or banks on strategies to shape or influence a legislative proposal. The operational powers from the public sector on the national level that deserve particular attention are the Financial Intelligence Units. They gather, analyse, and may exchange the suspicious transaction records issued by banks.

Operational powers on the international level include mutually cooperating European FIUs facilitated by FIU.net and Egmont Secure Web. These are virtual networks that make the exchange of suspicious transaction reports among the members of the network possible. In relation to these networks but especially to the practices for combating terrorism financing carried out within banks, international software companies providing specialized transaction monitoring programmes must be included as important operational powers operating on the
international (or transnational) level. Worldcheck, Mantas, and Fiserv are examples of leading providers of financial risk analysis software. A global network of FIUs known as the Egmont Group, is another operational power on the international level.

A final consideration with regard to both professional field maps is the inclusion of academic scholars on the map. Latour (2005) has argued that social scientists defining and studying specific groups are by no means independent observers but also part of the groups they help bring into existence (pp. 30-34). During this project, the influence of academic work on the European field of governing terrorism finance became visible when the European Data Protection Supervisor Peter Hustinx referred to the work of the privacy scholar Paul de Hert during an interview, when a member of the European Parliament mentioned the work of Marieke de Goede in her conference speech, or even from the academic books displayed in the offices of some of the key persons who were interviewed. More generally, European institutions and national governments have regularly invited scholars such as Nikos Passas and Loretta Napoleoni to hold speeches or write reports on terrorism financing. Nevertheless, academic scholars are not included on the maps because aside from these few examples their influence on the representation of the European fight against terrorism financing and the practices developed in the name of this fight is difficult to quantify. Moreover, including academics as one group of participants would be an oversimplification as they may hold heterogeneous and even opposing views on the subject. However, the influence of academic work on the understanding of terrorism and terrorism financing has explicitly been included in the next chapter, which considers the genealogy of terrorism financing.

2.7.3 Governmentality and the EU’s Fight against Terrorism Financing

The theoretical framework and the methodology described in this chapter inform the analysis of the governance practices that have emerged in the name of the European fight against terrorism financing. Looking at the professional field maps of the SWIFT affair and the Third Directive and their description, three elements of governmentality in the EU’s fight against terrorism financing already become apparent. First, the maps make visible a shift towards informal and ad hoc forms of governing. The FATF is illustrative in this sense as it was created by the G7 and does not have any international legal standing. According to one of the interviewees, the success of the FATF as a central player in the international war on terrorism financing can be explained by its informal character and the use of peer pressure instead of binding legal instruments (interview 19). The FATF governs the financing of
terrorism rather through processes of standard setting, benchmarking mechanisms, and establishing best practices and stimulating their adoption (Heng & McDonagh, 2008).

The Egmont Group of FIUs is another informal international network that meets on a regular basis. Like the FATF, to which it is closely linked, the Egmont Group was created in response to a specific anti-money laundering context and extended its mandate to include terrorism financing after 9/11. According to the European Commission, the Egmont Group ‘has become a genuine international forum and, though having no official status, has become an essential element in the international fight against money laundering’ (quoted in Gilmore, 2004, p. 79). This tendency towards ad hoc and informal ways of governing has also been highlighted in a more general context by the former Dutch Minister of Foreign Affairs Ben Bot (AIV, 2010, p. 6).

Secondly, the field maps make clear that in the fight against terrorism financing power is exercised through cooperation between representatives of the public and the private sectors. Either as operational power or as a representational power, in this thesis it is argued that private authorities are more than passively serving as a ‘deadly weapon’ instrumental to law-enforcement agencies. Private authorities, most notably banks but also software producers, professional associations, journalists, consulting firms, and civil liberties groups are closely involved in shaping and legitimizing discourses and practices about (combating) terrorism financing.

Thirdly, the field maps make the importance of financial databases for the collection and international exchange of data as a technique of governing visible. The inclusion of these databases in the field map highlights their existence, which is often taken for granted in other theoretical frameworks, but also their agency in the professional field. Their presence raises questions how technology opens up possibilities and helps in shaping and structuring the fight against terrorism financing.

Building on these three elements—a tendency towards ad hoc and informal ways of governing, public-private cooperation, and the agency of technology—the governmentality of the EU’s fight against terrorism financing and the corresponding professional fields will be examined in more detail in the following chapters. The next chapter investigates the emergence and representation of the European fight against terrorism financing.
Fig. 2.1 Professional field map of the SWIFT affair
Fig. 2.2 Professional field map of the Third Directive

Operational power

Representational power

International

FATF

CoE

MONEYVAL

UN CTC and 1267 Committee

European Commission

European Parliament

Council (of the EU)

International Professional Interest Groups

International Banks

Top Consulting Firms

National

National Legal and Compliance departments

Consultancies and training companies

National Central Banks/ Financial Services Authorities

Ministry of Finance/ Ministry of Economy

Ministry of the Interior/ Ministry of Foreign Affairs

National Parliament

National Financial Intelligence Units

FIU.net

AML/CFT Officers in local banks

Local

National Parliaments

MINISTRY OF THE INTERIOR

MINISTRY OF FOREIGN AFFAIRS

EUROPEAN COMMISSION

MONEYVAL

COE

UNE CTC AND 1267 COMMITTEE

FIG. 2.2 PROFESSIONAL FIELD MAP OF THE THIRD DIRECTIVE

FATF

INTERNATIONAL PROFESSIONAL INTEREST GROUPS

INTERNATIONAL BANKS

TOP CONSULTING FIRMS

NATIONAL LEGAL AND COMPLIANCE DEPARTMENTS

CONSULTANCIES AND TRAINING COMPANIES

NATIONAL CENTRAL BANKS/ FINANCIAL SERVICES AUTHORITIES

MINISTRY OF FINANCE/ MINISTRY OF ECONOMY

MINISTRY OF THE INTERIOR/ MINISTRY OF FOREIGN AFFAIRS

NATIONAL PARLIAMENTS

NATIONAL FINANCIAL INTELLIGENCE UNITS

FIU.NET

AML/CFT OFFICERS IN LOCAL BANKS

LOCAL
Chapter 3.

A Genealogy of the European Fight against Terrorism Finance

Money is the lifeblood of terrorist operations. Today, we're asking the world to stop payment.

—President George W. Bush (2001)

For money is the oxygen of terrorism. Without the means to raise and move money around the world, terrorists cannot function.

—Colin Powell, US Secretary of State (2001)

3.1 Introduction

Political leaders have often referred to combating the financing of terrorism (CFT) as an important front in the War on Terror. As illustrated by the quotes of former President George W. Bush and former Secretary of State Colin Powell, money is seen as the lifeblood for preparing and carrying out terrorist operations, and it is emphasized that without money terrorism cannot survive. Similar views have been expressed by European politicians. Like his American counterparts, British Chancellor of the Exchequer (later Prime Minister) Gordon Brown stated that ‘the ready supply of finance is the lifeblood of modern terrorism’ (UK Treasury, 2001) and more provocatively, ‘if fanaticism is the heart of modern terrorism, then finance is its lifeblood’ (BBC, 2001). Other European politicians and policymakers have usually used less sensationalist language but they equally consider money indispensable for undertaking acts of terrorism. At a joint conference between the EU and the Gulf Cooperation Council, former EU Counter-Terrorism Coordinator Gijs de Vries stated that ‘the amounts will vary according to the strategies and methods adopted by the terrorists. [. . .] But they all need funds, if only for day-to-day living expenses’ (2005).

Few academics have questioned the assumptions that place combating terrorism financing at the centre of the War on Terror. Biersteker and Eckert (2008), for instance, examine the appropriateness and efficiency of the current measures to combat terrorism financing in their renowned book Combating the Financing of Terrorism. Yet, from page one they assume that ‘new financial measures have been among the most powerful tools deployed by the United States and the international community’ and that ‘there is little doubt that such controls can have important effects’ (p. 1). In a similar vein, in Terrorism Financing and State
Responses, Giraldo and Trinkunas (2007) start with the observation that ‘financial and material goods are correctly perceived as the lifeblood of terrorist operations, and governments have determined that fighting the financial infrastructure is key to their defeat’ (p. 1).

The frequent use of metaphors such as ‘oxygen’ and ‘lifeblood’ to emphasize the essential role of money for terrorists is significant in two ways. First, it indicates a homogenization of the dominant discourse. Many politicians, policymakers, and academics define the problem along the same lines and in strikingly similar terms. Secondly, the use of the words ‘oxygen’ and ‘lifeblood’ shapes our understanding of terrorism financing in a particular way. The words evoke an image of terrorist money continuously circulating over the world like blood through the body, and imagine terrorism as a body that can be starved off by depriving it of oxygen or blood. Michael Chertoff, at that time the head of the Criminal Division of the US Department of Justice, made this reasoning explicit when he said ‘the lifeblood of terrorism is money, and if we cut off the money, we cut off the blood supply’ (Associated Press, 25 October 2001).

Although the use of metaphors may initially aid the understanding of an intangible concept by changing it into a more familiar and often tangible equivalent, some subtle meanings may be lost where the metaphor and reality part company (Paul, 2010, p. 1). Hence, understanding terrorism financing appears to become easier when the seemingly obscure and intangible practices of terrorism financing are transformed into more familiar concepts of the body. However, speaking about terrorism financing in terms of lifeblood and oxygen also makes combating terrorism financing appear as something obvious and uncontroversial, as if it emerged from laws of nature. It shapes our understanding of combating terrorism financing as a natural response to terrorism, erasing other interpretations.

This chapter challenges the perception that this new focus for fighting terrorism is natural and self-explanatory. Instead, it considers the European fight against terrorism financing, or CFT policy, as a construction reflecting certain political choices. Inspired by Foucault’s concept of genealogy, the objective of this chapter is to make the evolving representation of terrorism financing visible by providing a critical historical perspective. Examining this fight through what Foucault has called a ‘history of law’ (2008, p. 35), it traces when, why, and how finance came to be seen as crucial for the EU’s current fight against terrorism, while it was considered irrelevant when various European countries struggled with persisting terrorism in the 1960s and 1970s.
In addition, writing a genealogy goes beyond legal analysis or questions of efficiency; it entails denaturalising and destabilising the European fight against terrorism financing. This involves analysing the construction of truths and highlighting the counter-discourses concerning the European CFT policy that disappeared during the negotiation process and in the written legal outcomes. It entails mapping shifts in meaning and taking into account the societal and political context in which the decision-making took place. Furthermore, it means looking beyond the ‘9/11’ attacks and connecting the current European CFT policy with pre-existing policies and policy debates.

In the broader context of this thesis, the theoretical concepts and the methodological principles presented in this chapter underpin and enable the subsequent chapters. As a theoretical tool, genealogical analysis draws attention to the rationalities that shape practices of governing. It helps in questioning and opening up a subject. Consequently, if terrorism financing is not assumed to be the lifeblood of terrorism, other questions can be raised and it becomes possible to criticize (the prominence of) the fight against it. What are for instance the political and societal implications of this fight? Do the measures taken in the name of this fight affect ‘ordinary citizens’, and if so, how? What forms of governing do they create and is this desirable? Writing a genealogy helps to analyse the rationality of government (i.e., governmentality as a representational practice). It is complementary to the professional field in two ways. While the field approach concentrates on the practical aspects of governing, writing a genealogy provides an analysis of the construction of techniques of governing. In addition, like field theory, it focuses on the importance of struggles and negotiation in the exercise of power.

This chapter is divided into four sections. The following section introduces the meaning of genealogy and a corresponding methodology proposed by Foucault in more detail. The subsequent section presents a genealogy understood as Herkunft (on this term and the contrasting term Entstehung, see below). This means tracing the descent or the multiple beginnings of the EU’s fight against terrorism financing. How has terrorism financing emerged as a problem and how has what constitutes terrorism financing been defined? Next, genealogy is understood as Entstehung, examining the history of ideas leading to the emergence of the EU’s fight against terrorism financing. This section considers and questions the dominant discourses of combating terrorism financing and examines the position of these discourses in relation to other discourses in society. The last section of this chapter discusses how the birth of the EU’s fight against terrorism financing ‘became possible’ (Foucault, 2008, p. 33).
3.2 Genealogy and the Genealogical Method

In his essay ‘Nietzsche, Genealogy, History’, Michel Foucault introduces the concept of genealogy and, in his lectures at the Collège de France, he suggests a methodology for analysis. The common understanding of genealogy is that of tracing the ancestry of an individual. The further one traces back the family tree the more diverse the ancestors will be and the lesser the relations between one another. Yet, the individual relates to all these different ancestors. Foucault argues that this practice of tracing of origins can also be used to question objects or concepts that ‘we tend to feel [are] without history’ (Foucault 1977, p. 139) and to examine them in new ways. The objects examined or suggested by Foucault and many of those inspired by him include, among others, ‘love, conscience, instincts’ (Foucault, 1977, pp. 139-140), reason and freedom (Foucault, 1977, p. 142), the market (Foucault, 2008, p. 35), finance (De Goede, 2005), benchmarking (Larner & Le Heron, 2004), and capital (Pasquino, 1991).

This chapter offers a genealogical analysis of the European fight against terrorism financing and studies how this fight became constituted as an object of governing in the European Union. Compared to some of the more abstract objects cited above, this is a more specific object. Its scope is limited by the focus on the EU and the initiatives to combat terrorism finance and in particular the use of financial data. It also needs to be emphasized that a genealogy of the fight against terrorism financing is different from a genealogy of terrorism financing. In fact, the understanding of terrorism financing and the emergence of CFT policies do not necessarily mirror the actual practices of terrorism financing but they rather relate to the perception of how terrorism is financed, framed in such a manner that a particular response becomes possible.

Genealogical analysis implies looking differently at objects that are often thought of as stable by investigating their construction. It does not claim to search for ‘the truth’ but considers the construction of truths that are always controversial. It means making visible that objects acquire their meaning in a piecemeal fashion. It emphasizes that meaning is shaped in line with certain interests and necessities. Struggles, negotiations, and incidents define what becomes considered as priorities and what as trivial. What counts at a particular moment and what does not count? In other words, writing a genealogy may reveal relations of power that structure our understanding of the world.

Moreover, carrying out a genealogical analysis means refusing to understand history as a set of linear developments pointing in one clear direction. On the contrary, it stresses the
changes in meaning, the conflicts, and the discourses constructing the object that occurred over time. Objects may even disappear from societal discourses when they are (temporarily) considered irrelevant. Foucault argues that even those instances when an object is absent or the moment when it remains unrealized should be defined to underline the discontinuities that have taken place in the history of the object (1977, p. 140). However, although a non-linear approach may strengthen alternative understandings of the object, there is inevitably a limit to the number of perspectives and the timeframe that can be taken into account. Moreover, too much detail may obscure as much as a univocal linear analysis of the object. Foucault’s statement that it is equally important to highlight discontinuity and absence must therefore be qualified. But while it might prove very difficult to answer the question why something did not exist or was not considered relevant, describing and explaining absence does reveal something about how we structure the world.

In addition, writing a genealogy entails showing how something ‘became possible’. This involves ‘taking up a history of truth under different angles’ (Foucault, 2008 p. 33), or rather, ‘taking up a history of truth that is coupled, from the start, with a history of law’, (ibid., p. 35). In other words, it implies mapping which discussions took place and which other options were considered before a decision was taken or a law was adopted. Genealogy also investigates how the making of law, and consequently what is legal and illegal, is coupled to ‘truth’ and how this influences our understanding of the world. Analogous to Foucault’s assertion that certain conditions in the rules of medicine had to be met to hold a discourse on madness (2008, p. 36), there is a need for an investigation of how and when terrorism finance became perceived as a problem that required governing on an EU level. Essentially this implies mapping the (shifts in) meaning of the object over time and the conditions facilitating the construction of the object.

Instead of searching for the origin of an object, Foucault asserts that writing a genealogy rather involves an examination of their Herkunft and Entstehung. Although these two German words can both be translated as ‘origin’, Foucault emphasizes that they have distinct connotations. Herkunft refers to group affiliation and stresses the documentation of the genealogy of the object, which may have sprung from countless beginnings or origins (Foucault, 1977, p. 145). To examine the Herkunft of an object is to destabilize a univocal and stable understanding of that object by reintroducing parallel developments and moments of prioritization, redefinition, and absence. On the other hand, Entstehung signifies the emergence of ideas resulting from negotiations, discussions and struggles reflecting the relations of power and domination in a particular instance (ibid., p. 148). By bringing back
forgotten contexts, marginalized discourses, and shifts in meaning, the political choices upon which the object is constructed become visible.

In his lectures on *Security, Territory and Population* at the Collège de France in 1977-1978, Foucault sets out three methodological principles for genealogical analysis. These principles help to look at objects in a different manner and to make the relations of power visible. I will now describe the three principles and the questions that they may raise in the context of this thesis.

The first principle involves a shift of the locus of analysis to the outside of the institution (Foucault, 2007, p. 116). Instead of analysing the institution from within, for instance its structures, its institutional destiny, and the deployment of specific knowledge, Foucault suggests analysing institutions from the outside, in interaction and in relation to a broader framework directed to society as a whole. The displacement of the institution entails ‘going behind the institution and trying to discover in a wider and more overall perspective what we can broadly call a technology of power’ (Foucault, 2007, p. 117). As such, the institution not only governs but it is placed in a broader framework in which it also becomes an instrument of governing. During his lecture Foucault illustrates this shift through the example of a psychiatric hospital. He argues that the psychiatric hospital can only be understood as an institution on the basis of something external and general that is the psychiatric order, or beyond that, public hygiene (2007, pp. 116-117). From the latter perspective the psychiatric hospital is a means to intensify medical power and to realise the psychiatric order.

Similarly, instead of only studying the laws, initiatives, and statements that make up the European fight against terrorism financing, to step outside the institution means placing this fight in the broader framework of the War on Terror and global processes of securitization. How does the European fight against terrorism finance enable the objectives of the War on Terror and which forms of power and domination are exercised through the fight against terrorism financing? In the following chapters of the dissertation this shift outside the institution is realised through the notion of the field, which allows for analysing a broader set of participants. The last section of this chapter considers the shifts in the understanding of terrorism financing that took place in response to the declaration of the global War on Terror. The last chapter of this thesis considers how power is exercised through the European fight against terrorism financing in the context of the War on Terror.

The second principle is to substitute the external point of view of strategies and tactics for the internal point of view of function (Foucault 2007, p. 118). Foucault takes up the case
of the prison to describe what he calls the displacement to the outside of the function. He asserts that it is necessary to resituate the prison in the general economy of power by contrasting the expected (ideal) functions of an institution and the optimal way of exercising them against the real functions assured by that institution (*ibid.*, pp. 117-118). Drawing a historical assessment of what is intended and what is actually achieved allows for highlighting the technologies of power that are at work. As such we discover that the functions of the prison go beyond individual punishment; the prison exercises a much broader power of normalization over society (Foucault, 1995).

In a similar vein, one may investigate the ideal and the ‘real’ or alternative functions of the EU’s fight against terrorism finance. As discussed in the introduction of this thesis, the stated objectives of the fight against terrorism financing can be summarized as preventive, deterrent, and investigative. However, whether consciously created or not, the implications of this regulatory framework go beyond these ideal functions and affect society as a whole. For instance, by defining what normal or suspicious financial transactions are, these measures exercise a normalizing power over people’s financial behaviour. The case studies and the last chapter in this thesis will address the ‘real’ functions of the EU’s CFT policy in more detail. This chapter will highlight how the ideal functions of the fight against terrorism financing came into existence.

The displacement of the locus of analysis outside of the object constitutes the third methodological exercise. A shift outside the object means questioning ready-made definitions of an object and investigating the field of truth by which the object was constituted. For clarification Foucault uses the example of madness. On the one hand, madness is not a tangible object and it can be argued that it does not exist, at least not in a material manner. On the other hand, material absence does not mean that madness is nothing (2007, p. 118). It is a constructed phenomenon that was able to surface under certain circumstances and of which the meaning or definition may change over time.

With respect to the EU’s fight against terrorism financing, an examination outside the object implies asking how terrorism financing emerged as an important aspect of the fight against terrorism and which preconditions were needed to make this fight possible. The next sections of this chapter will reconstruct how targeting terrorists’ money became a crucial aspect of combating terrorism and which discussions, struggles, and negotiations took place for CFT to become a security issue and an official EU policy in 2001.

In sum, the three displacements proposed by Foucault’s methodology are tools for conceptualization that help to look at objects differently. Questions following from the
displacement of the institution, the function, and the object offer three approaches to make
technologies of power more visible. Analytically separable, Foucault’s methodology actually
results in much overlap when one tries to ‘apply’ the methodology in a structured manner.
Placing the function in a broader perspective automatically entails taking into account more
institutions. Describing shifts in the object is very difficult without relating it to either
functions or institutions. Hence, the three forms of displacement are strongly interrelated and
exact labelling of these displacements is neither self-evident nor of key importance. Rather
than rigidly applying the proposed methodology for genealogical analysis, these thinking
tools can be used in a more flexible manner to discuss the genealogy of the European fight
against terrorism finance in terms of Herkunft, Entstehung, and birth.

3.3 The Construction of Terrorism Financing as a National Security Issue

Accounts of policies combating the financing of terrorism often identify the 9/11
attacks as the origin of, or as a major turning point in, thinking about terrorist money as an
urgent security issue. Although some authors briefly mention earlier initiatives such as the
adoption of the UN Convention on the Suppression of Terrorism Financing in 1999, these
initiatives are often presented as rather insignificant to decisions that were made after 11
210), ‘changed the international approach dramatically’ (Biersteker et al., 2008, p. 236), or
‘changed everything’ (Meyers, 2005, p. 34) are not necessarily incorrect, they do obscure a
number of other interpretations. Identifying the 9/11 hijacking attacks as the origin offers a
reduced and linear explanation and justification for the existence of a European CFT policy.
This is problematic since it excludes earlier or parallel developments from consideration.
Moreover, a focus on origins pushes questions about the construction of the content of the
policy to the background by making it appear as if combating terrorism financing descends
from that particular day without any connection to the past.

Investigating the Herkunft, or descent, of an object highlights the multiple ideas and
initiatives that have shaped its meaning. ‘The search for descent is not the erecting of
foundations: on the contrary, it disturbs what was previously considered immobile; it
fragments what was thought unified; it shows the heterogeneity of what was imagined
consistent with itself’ (Foucault 1977, p. 147). By tracing both the terminology and the
practices of the European fight against terrorism financing, its multiple beginnings can be
placed further back in time. Yet the purpose of this exercise is not merely to look beyond the
9/11 attacks, nor is the intention to deny the importance of the attacks. Writing a genealogy understood as *Herkunft* disturbs the univocal understanding of an object, it makes shifts in the meaning of the object visible, and it provides a deeper understanding of the assumptions and decisions the current understanding of an object is based on. In order to do this, the *Herkunft* of the European fight against terrorism financing must start at the moment that terrorism became an important political issue in Europe and the first international and European initiatives to combat terrorism were developed.

Although terrorism has been present in many societies and has existed for centuries, political and academic preoccupation with terrorism increased considerably in the 1960s and much more so in the 1970s (Wilkinson, 2011). In response to a series of terrorist acts various international organizations adopted legal instruments. The United Nations adopted a first Convention on aircraft safety in 1963. In the 1970s, two other conventions were adopted related to aircraft safety and one by the end of the decade on hostage taking. Furthermore, beginning with the Bonn Summit in 1978 terrorism appeared officially on the agenda of the G7 countries (Masciandaro, 2004, p. 5), which aimed to put an end to air hijacking by furthering international cooperation on issues such as transportation security, denying arms and free movement to terrorists, and improving the exchange of information.

In the mid-1970s, both the Council of Europe and the twelve member states of the European Community (EC) took initiatives to combat terrorism. The former adopted a Convention for the Suppression of Terrorism in 1977, encouraging the extradition of suspected terrorists. The EC member states responded to domestic terrorism, for instance the *Brigate Rosse* in Italy and the *Rote Armee Fraktion* in Germany, by creating the informal and initially secret TREVI (Terrorisme, Radicalisme, Extémisme et Violence Internationale) group for ad hoc police cooperation against terrorism. Following a decision of the EC Ministers of Interior in 1976, five working groups were established, but only the one on terrorism played a prominent and operational role. In this framework, Interior Ministers and national top security officials met on a regular basis and established counter-terrorism policies (Den Boer, 2003, p. 1). More specifically, they produced joint analyses of terrorist threats and shared strategies and tactics to counter international terrorist groups; they also set up a fax system for information exchange (Bunyan, 1993, p. 2).

Academic literature from the 1970s mainly consists of case studies of terrorist groups that operated in various countries as well as some attempts to theorize terrorism. The main issues discussed in this literature were: the causes of terrorism (Crenshaw, 1981), the definition of terrorism, and the creation of typologies of terrorism (see for instance Wilkinson,
1974). Later studies of counter-terrorism efforts in the 1970s demonstrate that in Italy, Germany, and the Netherlands, governments were initially reticent to adopt specific counter-terrorism legislation or a coherent counter-terrorism strategy (Abels, 2007, De Graaf 2010). Only at a later stage did Germany and Italy adopt a range of specific counter-terrorism measures, which included increasing police forces and competences, improving the exchange of information among government services, and lowering the requirements for investigations and arrests (De Graaf, 2010).

Despite all the concern with terrorism, the legal, political, and academic response to the terrorist attacks throughout Europe in the 1970s did not include combating the financing of terrorism. States did not consider financing as a priority at that time as the amounts of money involved in terrorism were modest and investigating financial flows prior to the growth of the modern banking and credit industries would have been difficult (Donohue, 2006, pp. 326-327). Moreover, the debates on terrorism were structured around the question of the causes of terrorism. As the terrorism of the time was largely understood to stem from ideological struggle, decolonization, and opposition to autocratic or alien regimes, there was quite a bit of understanding of the causes of terrorism, and the political agendas of terrorists were taken seriously. In this context, focussing on the (il)legitimacy of the terrorists’ claims, the question of terrorism financing was considered pointless. Hence, in order to frame the financing of terrorism as a security concern and to have a discourse on combating terrorist finance, the understanding of terrorism itself needed to change.

In the 1980s a less tolerant stand, pointing out the devastating effects of terrorism, became the norm. This shift is nicely illustrated by contrasting the writings of terrorism researcher Paul Wilkinson from 1974 with an academic essay from an American perspective on the Western approach to terrorism from US diplomat Paul Bremer published in 1993. The former stresses that:

much of the dedicated support given to dangerous (and sometimes suicidal) international terrorist missions stems from conviction, anger, hatred and despair. [. . . ]The underlying causes of international terrorism are to a large extent to be found in political, social and economic problems that have defied attempts to resolve them by national governments, regional organisations and the United Nations. (Wilkinson, 1974, pp. 146-147)

Seventeen years later, Bremer states:
To nurture political will, the West had to change the whole dynamic of the international discussion of terrorism. We had to move away from the early 1970s defensive, muddled reaction to terrorist violence [. . .] We had to shift the public debate on terrorism from understanding the ‘root causes’ to condemning crimes terrorist commit. (Bremer, 1993, p. 257)

Hence, by actively framing terrorism as a crime, understanding the motivation of terrorists becomes redundant and is excluded from the debate.

Analogous to Woodiwiss’s (2003) analysis of the concept of organised crime, it can be argued that terrorism had become ‘a threat to society rather than a part of society’ (p. 3). In order to fight this threat, terrorists themselves, rather than the causes they were said to strive for, became central in the discourse. Consequently, the relevant question became how to stop these individual groups of evildoers from committing attacks on society. Part of the response to this question appeared in journalistic work from the late 1970s and 1980s. For instance, a slightly sensationalist book by the journalists Christopher Dobson and Ronald Payne (1979), with full colour pictures of weapons commonly used by terrorists, includes a chapter on terrorist money or ‘the budget of death’. Another journalist, James Adams (1986), wrote a less passionate book called The Financing of Terror, involving detailed research into the financial sources of terrorist groups. He states that ‘much has already been written concerning the motivation, structure and operations of international terrorist groups but one essential part of the terrorist equation has so far been ignored—money’. In these books money is considered as either ‘the fuel of terrorism’ (Dobson & Payne, 1979, p. 78) or as a tool for understanding the nature and workings of terrorism by following the money chain (Adams, 1986).

Although Adams’s book is occasionally quoted and praised in academic work, scholars in the 1980s and 1990s did not generally take up the issue of terrorism financing. Mainstream academic literature (Crenshaw, 1995, Freedman et al., 1986, Kushner, 1998, Laqueur, 1987, 1999, Schmid & Crelinsten 1993, Wilkinson, 1986a) often briefly mentioned terrorism financing but only in the margins of the larger debate on terrorism. When financing was discussed, it was mainly in relation to the issue of ‘state-sponsored terrorism’, which became a popular term in the 1980s. State terrorism having become ‘a major preoccupation of Western governments’ (Roberts, 1986, p. 11), Iran, Iraq, Libya, Syria, Cuba and to a lesser extent Sudan and North Korea were often mentioned as state sponsors of terrorism. Interestingly, three of these countries, Iran, Iraq, and North Korea, were later included in the ‘axis of evil’ in President George W. Bush’s terminology of the ‘War on Terror’. Although state-sponsored terrorism has existed for centuries, making states explicitly responsible for terrorist groups operating on their territory made it possible to deal with terrorism in the
Westphalian normative system of international relations. Consequently, hostile states, instead of certain violent groups or movements without a recognized status in international law, could be pointed out as the real cause of terrorism and could hence be sanctioned according to UN guidelines (Crenshaw, 1995, p. 10).

The concept of state-sponsored terrorism made it possible for states to issue international sanctions in order to eliminate terrorism. The purpose of these sanctions was to change the attitude of states supporting terrorism as well as to stigmatize terrorism (De Jonge Oudraat, 2003, p. 167). Individual states, most prominently the US, but also groups of states such as the EC’s TREVI group, have adopted various diplomatic, economic, or even military sanctions to combat the funding of terrorism by states (see, e.g., Jimenez, 1993, Kash 1998). Since terrorism financing was defined as being intimately related to states and because of the freedom of the UN to respond to a wider range of threats after the Cold War, the UN Security Council could also take action.

Throughout the 1990s, which has been called the ‘sanctions decade’ (Cortright & Lopez, 2000), the UN issued three sanctions regimes combating state support for terrorism. In 1992 and 1993, sanctions, including travel restrictions, an arms embargo, and the freezing of Libyan funds and financial resources in other countries, were issued against Libya in response to the 1988 Lockerbie attack. In 1996 Sudan faced diplomatic sanctions and the threat of travel restrictions, punishing the country for offering shelter to the suspects in the attempt to assassinate Egyptian President Mubarak. In 1999, the UN Security Council adopted resolution 1267 against the Taliban regime in Afghanistan for sheltering Osama bin Laden and his associates who were accused of, among other things, the 1998 US Embassy bombings in Nairobi and Dar-es-Salaam and of providing sanctuary and training international terrorists. An amended resolution was adopted in 2000 (UNSCR 1333) expanding the travel ban and asset freezing to Osama bin Laden, the Al Qaida network, and their associates. This sanctions regime is significant for the shift towards more selective ‘smart’ sanctions targeting individuals rather than states. Moreover, after 9/11 resolution 1267 constituted one of the first measures on which the War on Terror was built.

Parallel to the international law approach to terrorism financing, another ‘beginning’ emerged in the 1980s and 1990s in the field of law enforcement. During these years terrorism financing appeared first as an aspect of the War on Drugs and subsequently in relation to organised crime. In the early 1980s ‘narco-terrorism’ became a fashionable term linking terrorism and (revenues from) the drug trade. Initially, the term was coined to describe the violent attacks of drug dealers against the Peruvian anti-narcotics police (Smith, 1991), but
quickly the understanding of the US government became predominant, defining narco-terrorism as the involvement of terrorist organizations in the production and trafficking of drugs. Groups that were typically mentioned in relation to narco-terrorism included Colombian movements such as the FARC and M19, but also groups like the Palestine Liberation Organization (PLO), the Irish Republican Army (IRA), and, beginning in the 1990s, the Taliban.

In the 1990s, terrorism became increasingly linked to the overstretched notion of organised crime. This ‘major threat package’ (Beare, 2003, p. xv) referred to a range of threats including drug trafficking, corruption, and money laundering and justified a multitude of national and international measures. Although there was no strong empirical evidence that a nexus between organised crime and terrorism really existed, the mainstream opinion seemed to be that ‘to find examples of cooperation [. . .] ‘would be hardly surprising’ (Williams, 2008, p. 127). For instance, the UN’s Economic and Social Council did not ascertain that any significant links existed but it considered both phenomena as dangerous and a formidable challenge to governments (UN, 1996a). Organised crime and terrorist funding was also discussed in parallel during the G8 Justice and Interior Ministers’ virtual meeting on 15 December 1998, which was exclusively dedicated to this topic.

Although most academic literature in the 1990s discussed terrorism financing in terms of state sponsorship and devoted only a few sentences or paragraphs to other fundraising techniques, two influential scholars published on the link between organised crime and terrorism. In a comparison, Schmid (1996) concluded that although terrorism and organised crime are distinct phenomena, ‘there are links’ between them (1996, p. 40). Lacqueur (1999) dedicated a whole chapter of his book The New Terrorism to the relation between terrorism and organised crime, asserting that ‘in some cases a symbiosis between terrorism and organised crime has occurred that did not exist before’ (1999, p. 211).

The association with the declared War on Drugs and the war on organised crime added a new dimension to the understanding of terrorism. As the attitude towards criminal behaviour changed in the mid-1980s, governments and law-enforcement agencies became increasingly interested in punishing and deterring criminals rather than considering their economic, psychological, and social conditions. Highlighting the potential links between terrorism and the drug trade or organised crime helped to stigmatize and delegitimize terrorist organizations and those who help them as evil criminals. The attractiveness of this strategy for political purposes is illustrated by Adams’s examples of Israeli propaganda exaggerating the PLO’s involvement in marijuana exportation through Lebanon and of a US Senator accusing Cuba of
Machiavellian support of terrorist groups’ use of the drug trade to try to destabilize American society (1986, pp. 215-234).

Moreover, it became possible to extend governments’ responses to the drug trade and organised crime, in particular their anti-money laundering initiatives, to terrorism. In the 1980s follow-the-money practices became a central objective in the fight against drugs and organised crime. Governments justified this focus on money on the one hand by arguing that the financial power of drug syndicates and organised crime groups could be a potential danger for global financial institutions, the formal economy, and society in general (Gilmore, 2004, Tsingou, 2010). On the other hand, it was believed that in order to deter and punish criminals and terrorists, they needed to be deprived of their motive, in terms of profit, and/or their means, in terms of operating capital (Naylor, 1999). In the words of Warren Christopher, US Secretary of State at that time, it was not enough to condemn the terrorism of Hamas, Hezbollah, and other extremists. ‘A real penalty must be imposed. We must join together to turn off all foreign sources of funding for terrorism’ (speech of 1994 quoted in Kash, 1998, pp. 48-49, emphasis added). This association of terrorism financing and the follow-the-money philosophy constituted an essential step in the construction of the post-9/11 fight against terrorism financing.

It must be emphasized, however, that although the international and national initiatives against money laundering flourished, most notably through the creation of the Financial Action Task Force (FATF) in 1989, terrorism and its financing were not central in these initiatives. In the absence of a suitable definition of terrorism, only a few states undertook action to criminalize terrorist funding (Gilmore, 2004, Pieth, 2002). The UK, for instance, in response to the conflict in Northern Ireland, had already adopted laws criminalizing the financing of terrorism in the form of the Northern Ireland Emergency Provisions Act in 1973 and the Prevention of Terrorism Act in 1974. In the 1980s the provisions in these acts were gradually expanded and strengthened and included: the forfeiture and freezing of terrorists’ assets, the obligation to report information on money allegedly related to terrorism, and the criminal liability of those who (help) fund terrorism (Bonner, 1993, pp. 180-181, Donohue, 2006, pp. 325-343). In 1996, the US adopted the International Crime Control Act, expanding the list of money-laundering predicate crimes to include terrorism (Kash, 1998, p. 167). The FATF anti-money laundering guidelines left it up to the member states to decide on including terrorism as one of the predicate offences. This was also the case for the EC’s First Anti-Money Laundering Directive of 1991 (Mitsilegas, 2003, p. 99).
In the 1990s, terrorism finance also started to be defined as a crime in itself, autonomous from drug trafficking or organised crime. In 1992, the UK hosted seminars within the TREVI framework during which the Judicial Cooperation Working Group started investigating terrorist funding and laws in each country (Bunyan, 1993, p. 2). One year later, Jimenez (1993) declares in his study of terrorism in Spain that ‘international action needs to be taken to cut the flow of funds to terrorist groups. It becomes essential to investigate financial resources of these groups’ (1993, p. 118). In the mid-1990s the funding of terrorism was discussed during several G7/G8 summits and states were encouraged to take measures to prevent terrorists from raising funds (G7 1995, 1996a, 1996b, G8, 1998). At the 1996 Sharm el-Sheikh Summit for instance, the G7 called for ‘the ending of terrorism by cutting the flow of money from private Arab individuals to terrorist groups’ (quoted in Kash 1998, p. 169). Political leaders, especially in the US, were increasingly concerned about wealthy Arab businessmen and Islamic leaders, such as Osama Bin Laden, financing terrorist groups throughout the Middle East (Donohue, 2006, p. 350, Kash, 1998, p.169, Laqueur, 1999, p. 182). At the same time, the prevention of terrorism funding also made its first appearance in a UN resolution on Measures to Eliminate International Terrorism (1996 UN Res. 51/210).

It is important to highlight that by defining terrorism financing as a separate problem, it became possible to add a new element to its definition. It opened up the understanding of terrorism financing for funding unconnected to criminal activity. Consequently, it became possible to discuss the use of charities as a vehicle for financing terrorists. Beginning in the mid-1990s states were urged to

prevent and take steps to counteract, through appropriate domestic measures, the financing of terrorists and terrorist organizations, whether such financing is direct or indirect through organizations which also have, or claim to have charitable, social or cultural goals, or which are also engaged in unlawful activities such as illicit arms trafficking, drug dealing, and racketeering. (G7, 1996b, UN 1996b)

The understanding of terrorism financing as being either legally or illegally acquired money for the purpose of preparing or committing terrorist acts is still an important assumption in the War on Terror.

The 1999 UN Convention for the Suppression of the Financing of Terrorism, proposed by France and supported by the G8, was a milestone for the construction of the notion of terrorism financing in the sense that it established combating terrorism financing as an object of international law. Compared to previous UN counter-terrorism conventions, ‘the Terrorist Financing Convention is in fact a radically different instrument which breaks new ground with regard to not only the obligations of states but also, in particular questions of individual
criminal responsibility’ (Letho, 2008, p. 344). As a legal instrument it is remarkable in the sense that it criminalizes behaviour that is non-violent in itself and not necessarily illegal. Unlike terrorism, which consists of violent acts committed in the name of a political ideal, the act of terrorism financing does not involve violence and does not make victims in a direct and obvious manner. Moreover, the sources of terrorist money may consist of legal donations to charities or revenues from legitimate businesses that only become criminal due to the intention or knowledge that the money will be used for terrorism.

Another important element of the Convention is its focus on prevention (Letho, 2008). Instead of prosecuting suspected terrorists and punishing state sponsors of terrorism after the occurrence of a terrorist act, the Convention has been designed effectively to cut off financial flows of terrorist networks in order to prevent terrorist acts from happening. In this respect it can be argued that the Convention introduces into international law the focus on prevention and non-state actors that characterize the follow-the-money methods. After the 9/11 attacks, the rapid ratification of the Convention became one of the priorities in the early days of the War on Terror.

The investigation of the beginnings of the fight against terrorism financing shows that the role of the European Union in the definition of the problem of terrorism financing is strongly tied up with international initiatives undertaken in the context of the UN, the G7/G8, and the Council of Europe and propelled by the US but also by EU member states, like France and the UK, and to a certain extent the TREVI group. The analysis of international initiatives and academic literature has shown that to frame the financing of terrorism as an urgent security problem, the perception of terrorism needed to be shifted. Instead of understanding the root causes of terrorist acts, terrorist groups and their financing were increasingly qualified as criminal and a threat to (democratic) society. Subsequently, a link was made between terrorism and state sponsorship permitting this threat to be dealt with in the framework of international law, notably through economic sanctions. Parallel to this, first on a national level in some countries and then ‘exported’ to an international level, terrorism was debated in relation to the War on Drugs, organised crime, and financial crime measures. Through the image of wealthy terrorist organisations and donors, terrorism financing was redefined as a crime on its own, opening up new possibilities of governance. Understanding these multiple beginnings through which terrorism financing was defined and tracing the evolution in the understanding of terrorism financing is essential in order fully to appreciate the CFT policies that emerged after 11 September 2001, when terrorism financing became an issue of national security.
In the first hours after the 9/11 attacks the perception of terrorism shifted again. Terrorism was no longer perceived as a criminal act but was interpreted as a declaration of war. Within two weeks of these attacks ‘financial warfare’ (Navias, 2002, Shields, 2004) or a ‘financial war on terror’ (Warde, 2007) became one of the prominent tools for combating terrorism. This new terminology and the sudden urgency of combating terrorism opened up a new range of policy opportunities; but the declared war on terrorism financing also built upon the earlier shifts discussed in this section. The (dis)continuity in the understanding of terrorism financing after 9/11 will be discussed in more detail in section 3.5. The next section provides a fuller picture of the importance of terrorism financing in relation to other societal issues prior to 9/11.

3.4 The Emergence of Dominant Discourses on Terrorism Financing

In her influential book *Terror Inc.: Tracing the Money Behind Global Terrorism* (2004), Loretta Napoleoni argues that the financing of terrorism has developed over the recent decades into a ‘new economy of terror’. Starting her analysis from the Cold War, she discusses how terrorist organizations were first financed through direct state involvement and state sponsorship, followed by a phase of ‘privatization’ of terrorist financing, for example through narco-terrorism, to become highly sophisticated private enterprises using advanced business techniques and financial vehicles in the last decade of the millennium. Although her analysis is impressively detailed, the structure of her book represents terrorism financing as a linear development reflecting the successive mainstream discourses on terrorism financing and disregarding information that does not seem to fit within the story line.

The reconstruction of the *Herkunft* of terrorism finance as an object requiring governing, on the contrary, does not suggest a sequence of different phases but rather parallel and unrelated beginnings from various sources. Yet, the reconstruction of *Herkunft* remains a rather smooth story deprived from debate and controversies. While filtering out these debates enhances clarity and readability, the construction of the notion of terrorism financing obviously did not take place in a political and societal vacuum. In this section genealogy is understood as *Entstehung*. It further destabilizes the linear narrative by investigating the struggles, negotiations, and incidents that contributed to shaping the understanding of terrorism financing and the fight against it.
Genealogy, understood as an analysis of Entstehung, investigates the emergence of ideas and the relation between different forces, ‘the hazardous play of dominations’ over time (Foucault, 1977, p. 148). Hence, it must trace the interaction of mainstream discourses with alternative discourses, and with absences and discontinuities. Entstehung is a continuous process of transformation of the meaning and purpose of objects. In order to provide a fuller understanding of the political context from which today’s CFT measures in Europe emerged (see chapter 1), this section traces some of the discourses that have been overshadowed or abandoned in favour of more dominant discourses, it recalls the uncertainties and controversies that have been forgotten, and it highlights alternative political choices and conclusions that were not drawn.

When terrorism finance became a concern in the 1980s, political leaders and academics understood terrorism financing as an activity carried out by states. Stressing the importance of state involvement, Wilkinson asserted that over 25% of terrorist attacks were state-sponsored or state-directed, ranging from moral and diplomatic encouragement to providing weapons, training, funds, and sanctuary (1986a, p. 275, 1986b, p. 47). However, this means that the remaining almost 75% of the attacks were not financed through states. Donohue’s examination of Northern Irish paramilitary funding illustrates these numbers. In the 1970s the Provisional Irish Republican Army (PIRA) received some money, arms, and equipment from Libyan dictator Moammar Gaddafi, but Irish terrorist groups raised most of their money through donations, tax fraud, extortion, drinking clubs, black taxis, smuggling operations, drug trafficking, and kidnapping (2006, pp. 314-321). Yet the importance of financial sources beyond states seemed to be entirely ignored in the discourse on terrorism financing at that time. In a similar vein, the issue of state-sponsored terrorism became absent or marginal as the focus of terrorism financing shifted in favour of links between terrorism and organised crime or charities in the 1990s and to alternative remittance systems like hawala after 9/11. Nevertheless, as evidenced by Wittig’s (2009) case study of the Chechnya conflict and the report of the National Commission on Terrorist Attacks upon the United States (the 9/11 Commission) (2004), states continue to sponsor terrorist movements. Likewise, the Commission’s report also states that ‘[its] investigation uncovered no evidence that the 9/11 conspirators employed hawala as a means to move the money that funded the operation’ (2004, p. 516).

In the 1980s and 1990s, the increasing popularity of the follow-the-money methods in the War on Drugs and against organised crime with which terrorism became associated overshadowed critical perspectives that questioned the effectiveness and logic of attacking
financial assets. Naylor (1999), for instance, challenges the assumptions on which the proceeds-of-crime theories are based. He argues that seizing assets is not a strong deterrent to criminal behaviour because criminals are on the one hand not only motivated by profits and on the other hand taking away their profits may even force them to continue their crimes as they may have few alternative career paths. Moreover, seizing assets does not punish criminals very severely, as they often consider illegally earned income as ‘easy-come, easy-go’. Likewise, Naylor states that the investment of illegally earned money in the legitimate economy is unlikely to corrupt markets and legitimate businesses. He is also critical of the idea that asset seizure takes away the capital essential to commit future crimes (pp. 11-15). These arguments are perhaps even truer for terrorists, as self-enrichment is usually not their main objective. Yet, arguments against follow-the-money methods remained marginal in this period.

The definition and recognition of terrorism financing as a problem for international politics has also been source of intense and fundamental debates. Notwithstanding the relatively swift negotiations and the unanimous adoption of the 1999 UN Convention for the Suppression of Terrorism Financing, ‘terrorism financing was not a familiar concept’ and it was ‘not easily accepted or readily understood’ (Letho, 2008, p. 357). As mentioned above, it was not evident how terrorism financing constituted a crime since the criminality of the act is purely based on terrorist intent and it does not (necessarily) involve illegal transactions or violence. Therefore, some Western European States questioned the need for a separate convention on terrorism financing, as they considered that financiers of terrorism should be deemed accomplices of terrorism as defined in other international conventions. Other states in Western Europe and beyond were in favour of establishing terrorism financing as a principal offence by adopting a new convention, because they considered that financiers should face the same treatment as terrorists (Aust, 2001, p. 288).

A second important contentious issue was the definition of terrorism on which the crime of terrorism financing fully depends. So far, states had not succeeded in reaching an internationally accepted definition of terrorism due to its political sensitivity. However, if one were to criminalize terrorism finance, it was not possible anymore to elude the definition of terrorism. Two approaches were advanced: a list enumerating specific terrorist offences circumventing the debate on the definition of terrorism, and what was called a mini-definition of terrorism – a definition of terrorism that goes beyond the listing of specific terrorist offences but that does not touch upon the question how terrorists differ from freedom fighters. Despite the fear of some states that the latter would delay or threaten the adoption of the
convention, it proved to be not too difficult to reach a consensus on a generic mini-definition of a terrorist crime (Aust, 2001, 292, Letho, 2008, p. 358). To emphasize the instability of terrorism financing as a natural object of international law, it is important to emphasize that the negotiation of the Convention was a ‘torturous path’ that ‘required creative thinking to overcome some new problems’ (Aust, 2001).

This examination demonstrates that the understanding of terrorism financing was not always clear-cut and that it was shaped in relation to other ideas and interests at stake in the debates. The conventional understanding of the European fight against terrorism financing can be further destabilized by a displacement to the outside of the object by widening the perspective of combating terrorism financing to the broader security debate. Then, it becomes clear that terrorism financing was considered a marginal topic before September 2001. To be sure, beginning in the mid-1980s small groups of ‘experts’, including journalists and academics, policy makers and politicians, contributed to the framing of terrorist financing as a security issue and advocated actively the adoption of strict financial counter-terrorism measures. States affected by terrorist violence and occasionally the UN and the G7/G8 adopted measures to combat terrorism financing. However, terrorism financing was never considered as a very urgent matter until the 9/11 attacks.

Several other discourses were given more priority in the 1990s, which thwarted terrorism financing being considered a crucial issue in the EU (see figure 3.1). First, with the exception of the United Kingdom, until the mid-1980s the question of cutting off terrorists from their money was not a political or law-enforcement priority since it was still believed that the amounts of money involved in terrorism were too insignificant to justify a great deal of effort in combating terrorism financing. As a result, in 2001 a legal framework dealing terrorism financing was close to non-existent in most EU member states. Moreover, in many member states terrorism was not a crime under the penal code because arriving at a definition of terrorism was too contentious. Indirectly, the EU’s Second Anti-Money Laundering Directive, adopted in 2001, would have covered the financing of terrorism if terrorism were nationally defined as a serious organised crime. However, according to two EU officials, ‘before 2001 terrorism financing was not in the minds of the European legislators’ (interview 10).
Secondly, governments and the private sector were not very keen on introducing additional burdens on the financial sector through enhanced monitoring and control. Supported by the ideology of free markets and deregulation, the financial sector argued that this extra administrative work would too heavy be a burden on businesses and would negatively impact on the national economy due to reduced competitiveness. These economic considerations were also taken into account in the UN resolutions and G7/G8 declarations on terrorism financing. These state that to combat the financing of terrorism regulatory measures may be adopted as long as they do not impede ‘in any way the freedom of legitimate capital movements’ (UN 1999).

A third important discourse concerned civil liberties. In 1999, the US Treasury proposed strengthened Know Your Customer (KYC) regulations. These proposals faced stiff opposition in the US Congress for anti-regulatory reasons, but the main issue at stake was concerns over privacy (Eckert, 2008, p. 213, Napoleoni, 2004, p. 219). The US Treasury received more than 200,000 negative responses to its proposal from all political backgrounds objecting to the proposed requirements for banks to obtain extensive private information (Donohue, 2006, p. 359). The KYC proposal was also criticized for being a potential source of mistrust and resentment of government, particularly among immigrants and minority groups, as well as an undesirable form of generalized spying and reporting on citizens (Cato Institute, 1999).
Fourthly, the use of sanctions became an object of debate in the late 1990s. Only sparsely used during the Cold War, sanctions became a popular tool to alter the behaviour of certain states in the 1990s. Yet, the use of general trade sanctions became a controversial issue given the devastating humanitarian consequences they have on the general population. Some countries refused to respect the sanctions out of concern for human rights, while others advocated the use of targeted or ‘smart sanctions’. Moreover, many states failed effectively to enforce economic sanctions for economic reasons. Some states even benefited from the economic sanctions as they took advantage of the reduced competition with other states that respected the sanctions and froze their trade with the sanctioned state. Vetschera mentions in this respect the case of Austria, which strengthened its economic and political ties with Libya while Libyan leader Gaddafi was subjected to sanctions for supporting terrorism (1993, p. 221).

The lack of urgency concerning terrorism and its financing was enhanced by the absence of major terrorist attacks on European or American soil during the 1990s. Although combating terrorism was featured under the third pillar of the Treaty of Maastricht as well as in a number of joint declarations and recommendations issued in the 1990s, the EU never intensified the intergovernmental cooperation initiated in the mid-70s through the TREVI group. With only a few EU member states affected by terrorism domestically in the 1990s, ‘it seemed as if the issue had temporarily disappeared from the stage’ (Den Boer, 2003, p. 1). Hence, the European institutions were dedicated to the issue only on paper, treating the threat as ‘rather hypothetical’ (Tsoukala, 2004, p. 418). Moreover, the fact that prior to 9/11 the EU member states had never agreed on a common definition of terrorism or on developing a common strategy, let alone a separate policy combating terrorism financing, demonstrates the insignificance and the politically controversial nature of the topic.

Similarly, Eckert (2008) asserts that at that time the issue received little public attention in the US; only a few regulatory programmes indirectly addressed the issue and its working remained mainly of interest only to a small group of experts (p. 209). Significantly, until 9/11 no one on the White House’s National Security Committee was working full-time on countering terrorism financing. Until then, terrorism-related issues were part of a broader set of transnational threats (interview 18).

The attacks of 11 September 2001 substantially changed the urgency and importance assigned to these different debates. The relative insignificance of the amounts of money involved in terrorism, the burden on the financial sector, the civil liberties implications of strengthened regulation, and the doubts about the use of UN economic sanctions, all became
subordinate to the increased urgency of terrorism. Although the 9/11 Commission would estimate in 2004 that the total costs of the attacks was between $400,000 and 500,000 and concluded that the costs of the attacks were relatively low compared to the amounts of daily financial transactions worldwide (2004, pp. 186-189), a radically different conclusion was drawn in the immediate aftermath of the 9/11 attacks. Starving terrorists of their money had become a key objective within global governance. Likewise, financial regulation, such as Know Your Customer requirements, had been strengthened with little opposition from politicians, civil society or the financial and banking sector. Their current scope exceeds by far any previous initiative, making the contentious proposals of the 1990s look soft. Civil liberties, it was now widely accepted, had to be traded in if they constituted an opportunity for terrorists to ‘hide’.

The atmosphere of emergency and emotion after the attacks was also a very political moment. The need to take symbolic and visible action and the enormous momentum for adopting new measures led to renewed attention to the ratification and implementation of earlier initiatives and openness towards new ones. As expressed by a former civil servant of an EU member state: ‘In the days and weeks after the attacks in the US, the Minister of Finance wanted the latest news on the financing of terrorism. Every morning at 8:30 he wanted to know what he could do, which measures to take. For him this was a moment to exist, a moment of political visibility’ (interview 19). Terrorism finance did not emerge immediately as a key priority in what soon became the War on Terror. It took a few weeks for terrorism financing to become visible as a tool for combating terrorism, but the War on Terror began with ‘a strike on the financial foundation of the global terror network’ (Bush, 2001b).

Within a few weeks and months a comprehensive global framework against the financing of terrorism started to take shape. The pre-9/11 reluctance of most countries untouched by terrorism towards combating terrorism financing was abandoned for a frenetic search for policy responses immediately after the attacks. Two weeks after the attacks UN resolution 1267 (adopted in 1999) was invoked to cut off the financing of Al Qaeda and its associates. A few days later the UN adopted resolution 1373 to suppress the financing of terrorism in general. Moreover, in the months after 9/11 a ratification wave took place with regard to the Convention on the Suppression of Terrorism Financing. The number of countries that had ratified the convention went from only four on 11 September 2001 to 158 countries, including the US, by 2007 (Biersteker, 2008, p. 235). This strong commitment to implement and further elaborate existing CFT instruments reflected the profound changes caused by the 9/11 attacks.
A similar transformation can be noted with respect to other international organizations and bodies such as the G7/G8, the World Bank, and the FATF. While their involvement in the fight against terrorism financing may seem important and natural today, this was not the case before and in the first days after the 9/11 attacks. Despite the G7/G8’s continuous attention and efforts to stigmatize terrorism in the international community prior to 9/11, its initiatives remained optional and they generally faced a low level of implementation. Likewise, other international forums such as ‘the World Bank, the IMF and the FATF did not consider terrorism financing as a pressing concern nor a topic with which the organization should be dealing’ (interview 18). The designation of the FATF as a key player in the fight against terrorism financing is revealing in this context. Despite the claims of the US Treasury Secretary at that time that ‘FATF is uniquely positioned to take up the challenges of terrorist financing’ (O’Neill, 2001) and of the FATF President that its ‘mission is to strangle and cut the supply of money and assets that is the lifeline of terrorists’ (FATF, 2001), several options were on the table in the first weeks after the attacks. In France for instance there were very intense discussions as to ‘whether the FATF was the appropriate forum’ (interview 3). The Ministry of Finance strongly supported a global response through the FATF since it would strengthen the power of the Ministry of Finance. On the other hand the Ministry of Foreign Affairs was in favour of charging the UN with this responsibility, as this would simultaneously increase its own power. Another proposal was to create a new structure to deal with terrorism finance, but it was taken off the table as too ambitious to set in motion. Moreover, according to a civil servant, at that time ‘the initial reaction of the FATF, then presided by Hong Kong, was very reluctant’. ‘They didn’t want to deal with terrorism financing because it was too political. However, ‘the US, France, and the UK pushed for it to happen’. In the words of this same civil servant

I picked up my phone and called the Executive Secretary of the FATF and told him: “I think it is going to happen. The political pressure is incredibly strong so my advice is that you give a call to the FATF President and tell her that if she doesn’t want to do it, she is going to be pushed aside and completely out-maneuvered; we will do it (interview 19).

Despite these controversies and negotiations within international organizations and national bureaucracies, actors rapidly took up their new roles and their involvement in combating terrorism financing appeared to be widely accepted. Their reaction can be described as a mix between implementing and extending existing measures to combat terrorism financing, adopting measures that were already in the pipeline, and improvising new policy instruments. Parallel to and sometimes ahead of global efforts, European governments
and the EU institutions also felt a great urgency for joint action. This led to the conception of a European fight against terrorism finance.

3.5 The Birth of the European Fight against Terrorism Finance

The previous sections show that the first steps towards a European fight against terrorism financing were taken in a context in which both the understanding and the importance of terrorism (financing) had changed. Terrorism became defined in terms of war and the fight against it became the dominant discourse. From a policy perspective, the 9/11 attacks provided the political momentum to launch pre-existing initiatives that lay dormant within various national and European bureaucracies. This section discusses the birth of the European fight against terrorism financing and shows how it qualitatively differs from earlier initiatives in three ways. It became securitized, preventative, and partly privatized.

From the first days following the 9/11 attacks, statements made on behalf of the European Union explicitly included terrorism financiers in their condemnations of the attacks. In particular, representatives of the Council of the EU emphasized that ‘there will not be a safe haven for terrorists and their sponsors’ (EU Presidency, 2001, Council of the EU, 2001a, 2001b). The European Union urged member states urgently to ratify and implement pre-existing measures with regard to terrorism financing. In September 2001, only the Czech Republic, Greece, and Italy had signed the UN Convention for the Suppression of Terrorism Financing and the UK was the only member state to have ratified it. Hence, in an extraordinary meeting of the EU Justice and Home Affairs Ministers on 20 September 2001, all EU member states were invited once more ‘to ratify as soon as possible the relevant conventions to prevent and combat the financing of terrorism [. . .] and to take the implementing measures necessary” (Justice and Home Affairs Council, 2001). Within two weeks after the attacks of 11 September the European Union adopted the comprehensive EU Action Plan for Combating Terrorism. In this piece of soft law, ‘putting an end to the funding of terrorism’ featured for the first time as one of the ‘decisive aspects’ of the European fight against terrorism (Council of the EU, 2001c).

Instead of a crime with which states and the international community had to deal, terrorism financing was now mainly presented as an emergency security threat. It acquired ‘a shared critical salience [. . .] marked by the imperative of acting now’ (Balzacq, 2011, p. 32). The securitization of terrorism financing was attractive for politicians in the US and in the EU because financial measures could be adopted much more rapidly and results could be obtained
much easier and faster compared to any form of military retaliation. Financial investigators had quick successes by tracing the money trails of the 9/11 perpetrators, and by announcing the amounts of frozen terrorist assets political leaders could claim progress.

It is in this context that President Bush made the statement that money is the lifeblood of terrorism, quoted at the beginning of this chapter, and announced a first strike on the financial foundation of the global terror network with the stoke of a pen (Bush, 2001b). In what became called the ‘Rose Garden Strategy’, the Bush administration made regular announcements about the freezing of assets of suspected terrorism-related organizations and individuals. According to the New York Times, about 66 groups and individuals were blacklisted by the White House and officials claimed to have seized about $24 million in assets linked to suspected terrorists a month after the 9/11 attacks (Kahn & Miller, 2001). Five years later officials of the State Department claimed that approximately $142 million had been frozen and $65 million seized in countries around the globe since 11 September 2001 (Eckert, 2008, p. 230). The European member states also started blacklisting and freezing assets immediately after 9/11 and member states regularly communicated about the amounts of frozen assets in the media. However, figures on the amounts of frozen assets in the EU were not officially announced. Estimates vary from $2 million to $35 million between 2001 and 2004 (Bures, 2010, p. 423).

In addition to its initial focus on asset freezing, we have seen that the fight against terrorism financing was built on pre-existing anti-money laundering efforts as well as international economic sanctions. Many scholars have argued that the post-9/11 incorporation of CFT into the AML framework is problematic as these practices follow very different logics (see, inter alia, Donohue, 2006, Pieth, 2002, 2006, Roberge, 2007, Warde, 2007). Their main criticisms can be summarized as follows. Money laundering is driven by profits and the process takes place after illegal funds have been obtained. Terrorism financing, however, takes place before the crime and becomes criminal money after the transfer to an individual or group associated with terrorism. This is also called reverse money laundering or money dirtying. Contrary to money laundering, terrorism financing is considered as mainly driven by political goals. It usually involves small amounts of money and as mentioned above this money is not necessarily illegally derived. Moreover, including terrorism financing in the AML framework also assumes that terrorists use the formal financial sector to the same extent as money launderers.

Independent of the question whether the AML framework is suitable for combating terrorism financing, the detection of terrorist money through this framework also implied a
shift towards the prevention of terrorism. Although prevention was already part of the pre-9/11 follow-the-money vocabulary and practices, it must be stressed that a transformation had taken place. As rightly emphasized by Foucault, we should not assume words have kept their meaning and that ideas retained their logic (1977, p. 139). Before 9/11 anti-money laundering strategies were preventive in the sense that they were supposed to make crime less attractive as the laundered profits would be frozen or confiscated. AML regulation could not prevent the underlying crime from happening but aimed to detect the money-laundering process. After 9/11 financial regulation became preventive not only in the sense of dissuasion but rather as a precaution. The detection of terrorist monies would prevent attacks from happening and terrorists could be stopped before they could strike.

Taking a broader perspective, the measures to combat terrorism financing listed in the EU’s Action Plan can also be characterized by their preventive nature. The difficulties in agreeing on a common definition of terrorism that existed before 9/11 and that constituted an obstacle to adopting CFT legislation were rapidly resolved in the last months of 2001. In June 2002 the EU Framework Decision on Combating Terrorism was formally adopted. This Directive was strongly inspired by and built upon the preventive approach adopted in the 1999 UN Convention (Letho, 2008, p. 347). The Directive defines ‘terrorist acts’ and broadens the scope of terrorist offences by including preparatory activities that may contribute to terrorism either in or outside the EU and subjecting these offences to severe penalties (Letho, 2008, pp. 396-397).

The third significant shift is the strong involvement of the private sector in what has become a national security issue. Although the private sector was already involved in combating certain forms of crime prior to 9/11, the measures taken in name of the European fight against terrorism financing placed a different responsibility upon it. These measures not only expanded the scope of private actors involved in this fight but also required them to contribute to the security of the nation.

To conclude, the genealogical analysis in this chapter has shown that the birth of the fight against terrorism financing as an object of European governing was gradually constructed from the 1980s through international political negotiation and was subject to discussion and struggle. Active political intervention was needed to define terrorism financing as a separate crime and the activities that constitute this crime have been redefined and expanded progressively. Moreover, only after the 9/11 attacks did combating terrorism financing emerge as a dominant discourse. Before the attacks combating terrorism financing was a marginal issue restricted to small groups of experts, and other considerations such as
civil liberties and the interests of the financial sector were dominant and prevented the adoption of strict CFT legislation in most EU member states.

In the following chapters genealogical analysis is used to reconsider the modes of thought that underpin the current efforts of the EU in its fight against terrorism financing. These modes of thought are expressed in the practices of governing, as ‘practices do not exist without a certain regime of rationality’ (Foucault (1991), quoted in Heng & McDonagh, 2008, p. 561). In both case studies the practices of governing are investigated in order to understand the rationality of the fight against terrorism financing and the new forms of exercising power that have been developed in name of this fight. The following two chapters on the SWIFT affair consider the representation of the TFTP in the debates that followed its disclosure, trace the different discourses that emerged in the SWIFT affair, and bring to light the aspects of the TFTP that were absent from the debate.
Chapter 4.

Transatlantic Perspectives on the ‘SWIFT Affair’

4.1 ‘Bank Data Is Sifted by U.S. in Secret to Block Terror’

On 23 June 2006, the New York Times showed the headline “Bank Data Is Sifted by U.S. in Secret to Block Terror,” disclosing the existence of the Terrorist Financing Tracking Program (TFTP). That same day the Los Angeles Times, the Washington Post and the Wall Street Journal also published their investigations into the programme. The articles revealed a secret programme to track terrorist finances, initiated by the CIA in the weeks after the 9/11 terrorist attacks and overseen by the US Treasury Department’s Office of Foreign Asset Control (OFAC). This programme involved the analysis of millions of banking transactions worldwide through access to the financial records stored in the database of a Belgian cooperative called Society for Worldwide Interbank Financial Telecommunication (SWIFT).

Established by a group of banks in 1973, SWIFT offers its members services to facilitate the (international) transmission of financial messages worldwide through an automated standardized messaging service and interface software. The cooperative is the main financial messenger service in the world and claims to handle 80% of financial transfers worldwide.10 When the TFTP started in 2001, 7457 banks in 196 countries used the services offered by SWIFT and sent a total of 1,534 billion messages.11 The messages transferred through SWIFT’s messaging system, called ‘SWIFTNet FIN’, contain information such as the name, address, and location of the sender and the receiver as well as the amounts of money involved.

The TFTP illustrates the Bush administration’s philosophy of exploiting technological tools to prevent future terrorist attacks. It is based on a ‘proactive form of prevention in which the rationale is to “act before the other” to prevent harmful events from happening’ (Amicelle, 2011, p. 5). In this respect, the SWIFT database is particularly attractive as it constitutes the information hub of a very large part of the formal financial sector. From the perspective of intelligence services, the SWIFT database brings together very detailed information on financial transactions worldwide. While it is impossible to control all individual payment orders from any ordering customer to his or her bank somewhere on the globe, an important
part of this information can be collected in the form of standardized and encrypted SWIFT messages sent through the SWIFTNet FIN service. By analysing massive amounts of international bank transactions available in the SWIFT database, it becomes possible to trace suspected terrorists at an early stage and without issuing separate information requests to individual banks. The data contained in the SWIFT database also permit intelligence services to establish large networks of potential terrorism suspects by mapping the transactions between individuals. Moreover, the relative anonymity of SWIFT outside the financial sector was considered an advantage for using its financial data as a preventive tool in the War on Terror.

Immediately following the disclosure of the programme a vivid debate on the TFTP emerged among politicians, privacy and data protection authorities, civil liberties groups, and the media both in the EU and in the US. In what became known quickly as the ‘SWIFT affair’, questions were raised concerning the legality of the programme, the privacy aspects of financial data, the responsibility of the media, and the relationship between the US and the EU with respect to security cooperation (De Goede, 2012). Less noticed, the debate also included questions about the value of the pursuit of terrorist monies, the political effect of the deployment of risk technologies, and even the suggestion of the leader of the EP’s Civil Liberties Committee at that time that the TFTP itself should be a matter of debate (European Parliament, 2006a).

As Huysmans and Buonfino (2008) have shown, the analysis of political debates helps us to understand how political élites position themselves in parliamentary debates and how political issues are framed. Their work shows, for instance, how the nexus between terrorism and immigration has been politically sustained, the unsuccessful attempts as well as the reluctance to instrumentalise this debate for political gain, and the discontinuity of such debates.

This chapter investigates the debates on the SWIFT affair that emerged between 2006 and 2010 in the US and the EU. How was the SWIFT affair framed in the public debates in the US and the EU? Which issues were considered important once the programme became public and which issues were not discussed? How did debates change over time and how may this be understood? Or more specifically, how did the Terrorist Finance Tracking Programme become uncontroversial after the initial indignation expressed in newspapers? Answering these questions provides us with insights into the issues that became politicized through the disclosure of the SWIFT affair. It also highlights the arguments that have disappeared from the debates. Based on this analysis I argue that in the SWIFT affair power was exercised
through the ‘depoliticization’—a reduction of the political debate to technical or procedural questions—of the TFTP but also through a ‘depoliticized’ understanding of the European fight against terrorism finance in general.

Furthermore, investigating the debates emerging from the SWIFT affair shows how power is exercised and how the political process transformed a potentially wide political and societal debate into a narrow and ‘depoliticized’ understanding of the TFTP. As such it becomes visible how a new field of governing the SWIFT affair emerged and operates. In this field of governing, participants initially held differing and even contesting definitions of the problem. However, they gradually converged to a shared understanding of the issues at stake in the SWIFT affair, although they might still hold diverging opinions on the ‘resolution’ of these shared issues. The chapter also aims to make the wider political debate visible again in order to offer alternative readings and make a more comprehensive evaluation of the TFTP possible.

Although the focus of this chapter is on the EU, it is equally important to study the debates in the US. First, the TFTP was initiated by the US government and most information about the working of the programme was revealed by the American press. Secondly, the American reaction to the disclosure of the TFTP and the opinions of the Bush and Obama administrations regarding the programme are relevant for understanding the year-long transatlantic controversy and negotiations that followed between the US and the EU. Thirdly, the analysis of debates both in the US and in the EU allows for a comparison of the content of the debates and the processes of politicization and depoliticization and provides a deeper insight into how the debates in the EU mirrored or differed from the US debates.

The remainder of this chapter is structured as follows. The next section introduces the notions of politicization and depoliticization in greater detail. Subsequently, the debate on the SWIFT affair in the US will be analysed through these notions, followed by a section on the EU. This analysis is mainly based on European and American newspaper articles but also considers information obtained through interviews, official statements made by governments and SWIFT, parliamentary debates and hearings, most notably in the European Parliament and to a lesser extent in the US Congress, and reports and statements published by data protection agencies and civil liberties groups and in a few cases on internet blogs. The conclusion of the chapter advocates a ‘repoliticization’ of the SWIFT discussion in which the political and societal implications of the TFTP are discussed.
<table>
<thead>
<tr>
<th>Year</th>
<th>Month</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001</td>
<td>September</td>
<td>Attacks on the towers of the World Trade Center, the Pentagon, and a fourth unknown target.</td>
</tr>
<tr>
<td>2001</td>
<td>October</td>
<td>The UST issued its first subpoena to SWIFT.</td>
</tr>
<tr>
<td>2002</td>
<td>February</td>
<td>The National Bank of Belgium is informed about the TFTP.</td>
</tr>
<tr>
<td>2002</td>
<td>21 April</td>
<td>Central Banks of the G-10 countries are informed about the TFTP during a G-10 meeting.</td>
</tr>
<tr>
<td>2002</td>
<td>June</td>
<td>ECB is informed about the TFTP.</td>
</tr>
<tr>
<td>2003</td>
<td>8 May</td>
<td>SWIFT officials are invited for a high-level visit to the White House.</td>
</tr>
<tr>
<td>2006</td>
<td>Spring</td>
<td>Some members of US Congressional committees are informed about the TFTP.</td>
</tr>
<tr>
<td>2006</td>
<td>22 June</td>
<td>The NY Times decides to publish about the TFTP. Late that night US Under-Secretary of the Treasury Stuart Levey is interviewed to give his reaction on the programme.</td>
</tr>
<tr>
<td>2006</td>
<td>27 June</td>
<td>Privacy International files a complaint in 33 countries about the transfer of personal data from SWIFT to the US Government.</td>
</tr>
<tr>
<td>2006</td>
<td>29 June</td>
<td>US House of Representatives and Senate adopt resolutions supporting the TFTP.</td>
</tr>
<tr>
<td>2006</td>
<td>27 September</td>
<td>Belgian Privacy Commission Opinion on the transfer of personal data by SWIFT by virtue of UST subpoenas.</td>
</tr>
<tr>
<td>2006</td>
<td>4 October</td>
<td>European Parliament public hearing on the interception of bank transfer data from the SWIFT system by the US Secret Service.</td>
</tr>
<tr>
<td>2006</td>
<td>22 November</td>
<td>Art. 29 WP Opinion 10/2006 on the processing of personal data by SWIFT.</td>
</tr>
<tr>
<td>2006</td>
<td>20 December</td>
<td>Belgium Privacy Commission opinion regarding the preparation of an EU-US agreement regarding the transfer of SWIFT data.</td>
</tr>
<tr>
<td>2007</td>
<td>1 February</td>
<td>EDPS opinion on the role of the ECB in the SWIFT case.</td>
</tr>
<tr>
<td>2007</td>
<td>28 June</td>
<td>US Treasury adopts a set of unilateral commitments called “representations”.</td>
</tr>
<tr>
<td>2007</td>
<td>16 July</td>
<td>SWIFT joins the Safe Harbour Programme.</td>
</tr>
<tr>
<td>2008</td>
<td>7 March</td>
<td>Appointment of Judge Jean-Louis Bruguière as “eminent European person.”</td>
</tr>
<tr>
<td>2009</td>
<td>December</td>
<td>First Bruguière report published.</td>
</tr>
<tr>
<td>2009</td>
<td>3 September</td>
<td>European Parliament hearing on the EU-US interim agreement following the entry into force of the new SWIFT architecture.</td>
</tr>
<tr>
<td>2009</td>
<td>30 November</td>
<td>Adoption of an interim agreement between the EU and the US.</td>
</tr>
<tr>
<td>2010</td>
<td>January</td>
<td>Second Bruguière report published.</td>
</tr>
<tr>
<td>2010</td>
<td>1 February</td>
<td>The interim EU-US agreement enters into force.</td>
</tr>
<tr>
<td>2010</td>
<td>24 March</td>
<td>Reopening of the negotiations for a EU-US agreement and the Commission’s announcement of an EU equivalent to the TFTP.</td>
</tr>
<tr>
<td>2010</td>
<td>6 May</td>
<td>Biden speech before the European Parliament.</td>
</tr>
<tr>
<td>2010</td>
<td>25 July</td>
<td>EDPS opinion on the new draft EU-US agreement on financial data transfers.</td>
</tr>
<tr>
<td>2010</td>
<td>1 August</td>
<td>The TFTP continues under a new EU-US agreement.</td>
</tr>
</tbody>
</table>

Table 4.1 Detailed timeline of the SWIFT affair.
4.2 (De)politicization of the SWIFT Affair

The comparison between the European Parliament’s (EP) first debate on the SWIFT affair on 5 July 2006 and the debate in May 2010, not long before conclusion of a long-term EU-US agreement on the transfer of financial data from the SWIFT database, is marked by a sharp contrast. The first debate, and more generally the first phase of debates on the SWIFT affair on both sides of the Atlantic, was characterized by a multiplicity of political questions. In the EP’s debates of 5 July 2006, for instance, Dutch MEP Sophie in ’t Veld intervened and expressed her concerns with regard to the topic from the perspective of privacy, data protection, transparency towards citizens, the effectiveness of the programme in combating terrorism, transatlantic relations, and the US record on respecting international agreements under the Bush administration (European Parliament, 2006a). In May 2010, the debate was much more limited and was centred around a set of ‘technical’ questions. Resisting the pressure from US Secretary of State Hillary Clinton, Vice-President Joe Biden, and even President Obama, the EP’s main concern at this later date was the respect for European personal data protection rules and in particular the transfer of bank data ‘in bulk’ to the US authorities (European Parliament, 2010e).

This distinction in the kind of questions debated can be described as a distinction between questions belonging to the sphere of ‘politics’ and those belonging to the sphere of the ‘political’. Starting with the former, Jenny Edkins defines politics as the political in the narrow sense, including but not strictly confined to the doings of governments, the state apparatus, day-to-day decision-making, and technologies of governance (1999, p. 2). With regard to the SWIFT affair, the reactions of the political elite, the negotiation and conclusion of agreements between the EU and the US and, the adoption of resolutions in the European Parliament are examples of politics. The political in the broader sense sets out what ‘gets to count as “politics”’ (in the narrow sense) and what ‘defines other areas of social life as not politics’ (ibid.). In other words, the political is a process, a struggle, shaping the form of society and defining which issues are at stake. In Foucault’s terminology the political can be seen as the process of defining a ‘regime of truth’. This moment of definition is ‘marked by the articulation of a particular type of discourse and a set of practices, a discourse that on the one hand constitutes these practices as a set bound together by an intelligible connection and, on the other hand legislates and can legislate on these practices in terms of true or false’ (Foucault, 2008, p. 18).

Edkins’s understanding of politicization refers to the political in the broad sense. She
states that ‘[i]ronically what we call “politics” is an area of activity that in modern Western society is “depoliticized” or “technologized”’ (1999, p. 1). This, she continues, is not ‘an absence of the political through some sort of lapse or mistake but an express operation of depoliticization or technologization: a reduction to calculability’ (ibid.). It implies that politics consists mainly of preset procedures, norms, rules, and laws, tending to exclude the questioning of the political order itself, that is, the political. On the other hand, examining and calling into question the representation of power is in Edkins’ view the very essence of (re)politicization. This happens for instance when one social order has not yet been replaced by a new one (1999).

This instance of the political is what Žižek calls a ‘moment of openness’ (2008a, p. 188). During this ‘moment of undecidability’, ‘the turning point “when something is happening”’, a new reading of society is produced which can subsequently become legitimized (p. 189). In this moment a multiplicity of questions can be freely discussed in the absence of a dominant reading or interpretation. When decisions are taken and a new social order has been established, the moment of openness ‘becomes invisible’ and seems to be forgotten (p. 188, emphasis in original).

An alternative understanding of politicization is given by Huysmans and Buonfino (2008). Researching the argument of a nexus between immigration and terrorism in debates of the UK parliament, they consider that politicization does occur in the sphere of politics. They speak of ‘intense politicization’ when an argument is strongly defended or contested (2008, pp. 778-779). Politicization is analysed in terms of political dividing lines, the use of political terminology, and the specific renditions in political positioning and justifying measures. By creating contexts of unease, for instance, the use of smart technology can be presented as a solution to reassure citizens that they are safe and that the government is able to protect them (2008, p. 783). For Edkins this political positioning would be a form of depoliticization.

In a similar way, depoliticization can be understood as taking place in the spheres of both politics and the political. For Edkins depoliticization is linked to politics. To illustrate this she takes up two cases: the case of famines or more broadly humanitarian crises, and securitization. She argues that international actors analyse these emergency situations in technical terms, for instance in terms of food production and nutrition values and sometimes ‘social’ factors (1999, p. 10). By taking this approach, political questions or motivations that may have caused or influenced the emergency do not have to be taken into account. The exclusion of political debate is even more prominent when issues are securitized. If something is considered as an issue of national security, for instance terrorism finance, certain questions
are no longer open for debate. According to Edkins and contrary to mainstream literature in security studies, securitization is a stronger form of depoliticization. ‘When issues are “securitized”, they are even more firmly constrained within the already accepted criteria of a specific social form. And that constraint is even more firmly denied’ (1999, p. 11).

Marieke de Goede has analysed what she considers among modern society’s most depoliticized areas of activity: finance and economics (2005, p. 2). Like Edkins she highlights how financial practices and theory are technologized and presented as a matter of objective and scientific calculation through statistics, formulas, instruments, and indicators. Creating this image of a stable, natural, and objective financial system renders financial practices uncontroversial and places them beyond discussion. She also raises another important aspect of depoliticization. Taking speculation as an example, she demonstrates that it was the adoption of financial regulations after the 1929 crash that ‘made it possible to reify financial practices by erasing traces of their controversial, religious, cultural, moral, gendered and political origins’ (2005, p. 124). It is the ‘normalization’ of these practices through the adoption of a legal framework that legitimizes them.

According to Žižek not only politics is depoliticized but so is the political. In this respect, he speaks of ‘a worldwide sphere of “moderate post-politics”’ (2002, p. 135). Inspired by Rancière, Žižek means by post-politics ‘a politics that claims to leave behind old ideological struggles and instead focus on expert management and administration’ (Žižek, 2009, p. 48, see also Žižek 2008b). In Žižek’s analysis of the political this means that the currently dominant Western liberal consensus declares all realistic alternatives to capitalism impossible and reduces politics to managing capitalism and ignoring political opposition (Žižek, 2002, p. 135). More specifically, he states that the current focus of political discourses on identity has a depoliticizing effect. By first transforming ‘politics’ into ‘cultural politics’ new questions are opened up, hence politicized, but other questions about the foundations of our society are no longer asked. To illustrate this, he claims that postmodern identity politics explains economic inequality referring to racism and intolerance, implicitly abandoning questions on the nature of relationships of production and whether democracy, the state, and capitalism are the ultimate horizons of our political organisation (Hanlon, 2001, pp. 10-11). In the Foucauldian terms, one could say that postmodern identity politics offers a new ‘regime of truth’ by which certain of the previous debates become seen as irrelevant and disappear as objects of debate.

In perhaps less provocative terms, Judt describes this same intellectual shift, paraphrasing Kundera, as ‘the unbearable lightness of politics’ (2010). He argues that since
Thatcherism and Reaganism, ‘the state became reduced to that of facilitator’, ‘reducing public conversation to a debate cast in narrowly economic terms’ (2010, p. 97). Economic jargon dominates the political conversation, appreciating public services only in measurable terms of ‘productivity’, ‘efficiency’, ‘output’, and ‘impact’ instead of in terms of societal values such as providing good quality services responding to collective needs. As a consequence, political questions, for instance whether a certain measure brings about a better world and how we define a better world, are not asked and politics itself becomes insignificant.

These scholars differ sharply in their views of how to ‘repoliticize’ the depoliticized discourses they investigate. With respect to the post-political, Žižek is rather pessimistic about the possibility of repoliticization, which he calls the emergence of an act ‘that changes the very horizon in which it takes place’ (Hanlon, 2001, p. 11). He believes that ‘in politics the space for an act is closing viciously’ and that ‘politics, for some foreseeable time is no longer a domain where acts are possible’ (ibid., p. 12). On the other hand, De Goede and Edkins assert that repoliticization can take place by interrupting or disrupting the dominant discourses, ‘questioning that which is considered to be normal, natural and, most importantly scientific’ (De Goede, 2005, p. 3, emphasis in original; see also Edkins, 1999, p. 12).

The examination of political debates as processes of (de)politicization of politics and the political is a way to study the governmentality of the European fight against terrorism financing. Investigating these debates is interesting because it draws attention to the discursive framing of the SWIFT affair. It also points to the way in which power is exercised through the field of governing. Moreover, it makes visible how the field operates and how governing takes place through a reduction of the debate to expert knowledge. For instance, in a ‘field of force’ (Bigo, 2006), pressure is exercised to come to a shared—and thus depoliticized—understanding of the issues at stake in the field. Likewise, in a ‘field of domination’ the issues at stake are depoliticized as one field successfully imposes its definition of the issue upon other fields. When, contrariwise, the field is one of ‘struggle’, there is no common reading of certain issues. Participants are competing with each other and the issues at stake are part of the political.

This chapter presents an investigation of the phases of politicization and depoliticization in the American and European debates on the SWIFT affair and shows how they were rendered technical. My understanding of the various notions in this chapter is as follows. I use the expression ‘moment of openness’ as described by Žižek and Edkins’ ‘re-p politicization’ for phases in which the debates are concerned with the political. I use the notion ‘ politicization’ to refer to the issues that become problematized in the political debate
after the initial moment of openness. Hence, I follow Huysmans and Buonfino in their view that politicization takes place in the parliamentary debates but that these issues are part of politics and not of the political as Edkins suggests. With regard to the notion of depoliticization, I argue that the realms of politics—here, the political handling of the SWIFT affair by the professional field—and the political—in the sense of questioning of the assumptions on which the fight against terrorism finance is based—have both become depoliticized. I will also adopt the approach of Edkins and De Goede to repoliticize the SWIFT affair in the last section of this chapter. However, first this chapter will examine how the debate on SWIFT developed, what important moments of depoliticization took place and what political effects these moments had.

4.3 The US Debate

The New York Times article of 23 June 2006 by Lichtblau and Risen revealing the existence of TFTP is a piece of deep investigative journalism, presenting the programme from multiple perspectives. On the one hand it discloses information on the nature and the scope of the TFTP and on the other it reports on the reactions in favour of and against the programme. Two important and interrelated issues stand out in this article and these became the key political debates in the SWIFT affair: the legality of the programme, most notably with regard to privacy rights, and the decision of the newspaper to disclose the programme. However, this first New York Times publication, and other newspaper articles that appeared between Friday 23 June and the following weekend, also voice a wider range of critiques and doubts. The next section discusses this first phase of the debate as a moment of openness. Subsequently, the politicization of certain arguments in the ‘SWIFT affair’ in the US is examined as a second phase. A third phase during which these arguments became depoliticized is considered in the last two parts of this section.

4.3.1 Moment of Openness: an Emerging Debate During the Weekend

In the first publications on the subject, journalists cited a number of arguments justifying the disclosure of a secret government programme. According to the New York Times journalists and editors, their main reason for the decision in favour of publication was the belief that ‘it is a matter of public interest to be informed about the administration’s extraordinary access to the enormous quantities of financial data held by SWIFT’ (Lichtblau
& Risen, 2006). The Los Angeles Times was also concerned about the programme which it believed ‘raises privacy concerns’ and which it qualified as ‘clandestine’ (Meyer & Miller, 2006). Journalists highlighted that the TFTP obtains millions of confidential financial records through administrative subpoenas, known as national security letters, which differ sharply from the traditional individual court-approved warrants and subpoenas used to obtain financial data. Moreover, these broad subpoenas are secret and without any judicial review. The articles are also critical of the fact that this secret programme had been running for five years without Congressional approval and oversight before becoming public. During the weekend of 24 and 25 June 2006 this point was taken up by a number of Democratic and Republican politicians. Republican Senator Arlen Specter was particularly troubled to learn that the administration expanded its Congressional briefings only when it knew the New York Times would disclose the programme. He said, ‘why does it take a newspaper investigation to get them to comply with the law?’ (Stolberg & Lichtblau, 2006).

Yet concerns were not limited to privacy and legal issues. Reactions from government officials indicated that the duration of the programme was also controversial among at least some of them. One government official said, ‘I thought there was a limited shelf life and that this was going to go away’. Other officials declared that ‘what they viewed as an urgent, temporary measure had become permanent nearly five years later without specific Congressional approval or formal authorization’. A former official is quoted saying that ‘there was always concern about this programme’. Equally, SWIFT executives seemed to have doubts, as expressed by the question of one of them, who wondered ‘how long can this go on?’ (quoted in Lichtblau & Risen, 2006).

The first articles written about the programme also reported on its lack of results. A former administration official questioned its efficiency, saying, ‘We were turning on every spigot we could find and seeing what water would come out. [. . . ] Sometimes there were hits, but a lot of times there weren’t’ (Lichtblau & Risen, 2006). In the LA Times, current and former US officials also expressed their scepticism about the results of the programme, saying ‘the effort has been only marginally successful against Al Qaida’ (Meyer & Miller, 2006). Similarly The Washington Post reported that

[o]fficials said far more information was collected early on, often on people who had nothing to do with Al Qaeda but whose Muslim names or businesses were similar to those used by suspected members of Al Qaeda. That method flooded the intelligence community with reams of material that was laborious to go through and repeatedly misled investigators (Gellman et al., 2006).
Furthermore, newspapers reported on concerns about the potential problems of the collection of huge sets of financial data. Regarding this issue a former official raised the question, ‘how do you separate the wheat from the chaff? And what do you do with the chaff?’ (Meyer & Miller, 2006). On this same topic a then-current government official highlighted that ‘the potential for abuse is enormous’ (Lichtblau & Risen, 2006). These quotes show that the premises and the effectiveness of the TFTP were not self-evident. They questioned the value of a risk-based approach to the War on Terror, and officials involved in the TFTP indicated that it is a labour-intensive method that produces very little useful information and many false positives.

These first days after the disclosure of the TFTP can be understood as a moment of openness in which the SWIFT affair was part of ‘the political’. There was no political positioning around this issue yet and when the US Treasury learned about the decision of the New York Times to publish the article in the evening of Thursday 22 June 2006 and the next morning, their initial reaction was rather mild. They were unhappy with the situation, but informally they congratulated the journalists with their scoop (interview 13). There was also no established reading of the TFTP. During these first hours and days, newspapers, privacy and civil liberties groups, and politicians addressed a range of issues in relation to the disclosed programme and including fundamental questions concerning the legality and the effectiveness of the programme and the value of trawling though large amounts of financial data. The moment of openness or first phase of the SWIFT affair ended quickly when during the weekend the public debate started to swell.

4.3.2 Politicization: Privacy and Legal Concerns

Attempting to limit the impact of the publication of the TFTP, government officials defended the programme during rapidly convened meetings with the press, assuring the public that it was crucial for US security and entirely legal. Furthermore, the Bush administration, members of the Republican Party and some newspapers and TV stations strongly condemned the New York Times for publishing the article. Focussing their response exclusively on privacy and legality issues on the one hand and the decision to disclose the TFTP on the other, the scope of issues that were debated became reduced. At this moment a second phase started in which a distinction became apparent between issues that were considered legitimate subjects for political debate and others that seemed to be forgotten. The political disappeared in favour of politics.
The response by President Bush, Vice-President Cheney, and officials from the US Treasury to the allegations about the illegality of the TFTP, can be summarized as an aggressive defence of the programme, avoiding much detail and attempting to reassure citizens. On Monday 27 June President Bush asserted that ‘what we did was fully authorized under the law’ and ‘what we were doing was the right thing’ (quoted in Baker, 2006). During the previous weekend and on the day of disclosure, Cheney said ‘the fact of the matter is that these are good, solid, sound programs’ and ‘they are conducted in accordance with the laws of the land’ (quoted in Stolberg & Lichtblau, 2006).

During press conferences and on TV, Treasury Secretary John Snow and Under-Secretary Stuart Levey provided a little more detail on the workings of the programme. They explained that following international transactions makes it possible to map terrorist networks and to locate terrorist financiers worldwide (Snow, 2006a). It provides concrete leads such as names, addresses, and account numbers (Levey, 2006) However, they avoided responding to specific critiques raised by journalists, for instance on the extensive use of large and uncontrolled administrative subpoenas. Snow declared that the TFTP ‘is entirely consistent with democratic values, with our best legal traditions’ (quoted in USA Today, 2006a). ‘It is responsible government. It is effective government’ (quoted in Miller & Meyer, 2006). Levey immediately asserted that the programme was ‘without doubt a legal and proper use of our authorities’, ‘grounded in the president’s emergency economic powers’ (quoted in Lichtblau & Risen, 2006). He continued to say that the programme was ‘hyper legal’ and ‘on rock solid legal ground’. In particular, he said that it was based on the International Emergency Economic Powers Act (IEEPA) that ‘specifically gives us the authority to conduct this type of investigation if there is an emergency declared by the president’ (Gellman et al., 2006). These rather vague and general answers to the legal concerns raised by the media, politicians, and civil liberties groups helped to depoliticize these issues, giving the impression that the program was entirely ‘legal’ and therefore no object for concern, debate, or political struggle. Moreover, this reduced the TFTP to a legal issue, excluding questions about the societal desirability of the programme.

To be more precise, the Bush administration found a legal justification for the programme in a new interpretation of the broadly-worded International Emergency Economic Powers Act, enacted in 1977 ironically to limit and control the emergency powers of the president. According to the IEEPA an emergency is ‘any unusual or extraordinary threat [to the national security, foreign policy or economy of the United States], which has its source in whole or substantial part outside the United States’ (IEEPA, section 1701a). If the president
has declared such an emergency, as Bush did by means of Executive Order 13224, the IEEPA authorizes the president to ‘investigate, regulate or prohibit [. . . ] money transactions and other property of any person subject to the jurisdiction of the US’ (IEEPA, section 1702aA). Generally speaking, it seemed that the TFTP would fit in this legal framework. One official said ‘the program arguably complies with the letter of the law if not the spirit’ (Lichtblau & Risen, 2006).

However, it can be debated whether the scale on which the searches into financial records took place, the duration of the programme, and the targeted suspects still fell within the scope of the IEEPA. That they did not was voiced for example by Pam Dixon of the World Privacy Forum. She said, ‘We need firm lines drawn on how we use emergency powers in crisis situations’ (Miller & Meyer, 2006). Likewise, Democratic Representative and Member of the House Financial Services Committee Carolyn Maloney stated, ‘The administration is basing its actions on a 1970’s law that never envisioned a state of perpetual emergency. It wasn't meant to become the status quo’ (Shane, 2006a). More fundamentally, the unusual or extraordinary threat of terrorism financing which is required for invoking the IEEPA was not irrefutably established.

Another legal issue concerned the role played by SWIFT in transferring its database to the CIA. The New York Times wrote that SWIFT was seen as a ‘willing partner’ (Lichtblau & Risen, 2006), and ‘very resolute in its commitment to the programme’ (Stolberg & Lichtblau, 2006), yet constantly concerned about its legal liability. After the disclosure of the programme, the company’s officials always emphasized their reluctance to cooperate with the US authorities and underlined that the data transfers were compulsory under US law (SWIFT, 2006a). US Treasury and SWIFT officials debated whether SWIFT could be held liable for breaching banking laws such as the Right to Financial Privacy Act. US Treasury officials asserted that SWIFT is not a bank but a banking consortium and concluded that banking laws did not apply. The company itself also examined the legality of the data transfer and concluded that while operating in the US it had to comply with the subpoenas, as this was compulsory under US law (Belgian Privacy Commission, 2006a).

Journalists and European data protection authorities considered the situation to be much more complex. They highlighted that SWIFT’s mirror database is located in the US but the company’s headquarters are located in Belgium, which means that not only American but also European privacy laws could apply to the company. According to several newspapers, the cooperation with SWIFT exploited a ‘grey area’ in the national and international laws regulating banking, which were considered to be ‘complex and rather murky’ (Lichtblau &
Risen, 2006). In reaction to the affair, SWIFT provided a written statement in which it insisted that executives ‘have done their utmost to get the right balance in fulfilling their obligations to the authorities in a manner protective of the interests of the company and its members’ (SWIFT, 2006a). SWIFT said it had complied with all applicable laws on the one hand and that it had negotiated protections and assurances as to the use of the data and had narrowed down the scope of the data that were transferred on the other. Since potential breaches concerned EU law, there was no further debate on the role of SWIFT and its legal breaches in the US.

In addition to the issues involving the legal foundations of the programme, potential privacy breaches also became a matter of great concern. On the day the TFTP became public, the American Civil Liberties Union (ACLU) issued a statement in which it ‘condemned the US government for gaining access to vast troves of international financial data with no judicial or Congressional oversight nor definition of how the information is being used’ (ACLU, 2006a). Anthony Romero, Executive Director of the ACLU, declared that ‘the revelation of the CIA’s financial spying program is another example of the Bush administration’s abuse of power. The invasion of our personal financial information, without notification or judicial review, is contrary to the fundamental American value of privacy and must be stopped now’ (ACLU, 2006a).

The allegations of privacy violations were countered by the Bush administration with three arguments. First, it insisted that the TFTP did not involve national transactions within the US. For this reason, it was argued, the privacy of American citizens was not infringed upon. Yet, the New York Times reported that while the program was mainly concerned with international wire transfers, it also included financial transfers between Americans within the US (Lichtblau & Risen, 2006). Moreover, it must be noted that Americans who make international wire transfers are certainly concerned. In addition, other US Treasury officials stated that the database and the searches did look into the financial information of American citizens but that ‘privacy laws don’t protect individuals believed to be acting as a “foreign terrorist agent”’ (Meyer & Miller, 2006).

Secondly, it was stressed that the TFTP was controlled tightly and that it was targeted rather than involving an examination of all the records. In the words of Treasury Secretary John Snow, ‘It is not a fishing expedition but rather a sharp harpoon aimed at the heart of terrorist activity’ (Snow, 2006a). Moreover, it was revealed that an outside auditing firm had verified that the data searches were based on intelligence leads and that only terrorism-related searches were allowed, excluding for instance tax fraud, drug trafficking, or other inquiries
(Lichtblau & Risen, 2006). This ‘control argument’ was a way of depoliticizing privacy concerns with respect to the TFTP. It suggests that there is nothing to be debated since privacy rights are respected through the introduction of technology, procedures and institutions.

A third argument is that privacy concerns are not relevant with respect to the TFTP. Two variations on this argument can be distinguished. It was argued, for instance by Treasury officials, that the Right to Financial Privacy Act (RFPA), which requires the respect of certain procedures for searching bank records, does not apply since SWIFT is mainly to be considered as a messaging service and is not a bank or financial institution (Lichtblau & Risen, 2006). It would follow from this that government access to SWIFT’s database is not restricted. Under-Secretary Levey went a step further and stated that ‘people have no privacy interest in their international wire transactions’ (Lichtblau & Risen, 2006).

It is interesting to note that in these debates the privacy of non-American citizens inside and outside the US has not been a matter of concern. But more importantly it needs to be emphasized that the three arguments given by the Bush administration are not fully consistent. If indeed international wire transfer data are not of a private nature, the arguments that the programme does not concern the financial data of American citizens and that the searches are very specific and tightly controlled should not be relevant. In addition, behind the scenes, privacy concerns did seem important. Anonymous US government officials declared that ‘the access to large amounts of confidential data was highly unusual’ and that because of privacy concerns and fear of abuse, the government had put some restrictions on the use of the SWIFT data (Lichtblau & Risen 2006).

4.3.3 Depoliticization: Shoot the Messenger!

After the weekend following the disclosure of the TFTP, the Bush administration’s first reaction of defending the necessity and legality of the programme was exchanged for a more aggressive approach. In this third phase, the SWIFT debate became consciously and successfully reframed around the question whether journalists should report on secret programmes concerning national security. First, Dick Cheney, Vice-President at that time, severely condemned the disclosure of the TFTP in the media and declared he was offended by it. He said, ‘What I find most disturbing about these stories is the fact that some of the news media take it upon themselves to disclose vital national security programs, thereby making it more difficult for us to prevent future attacks against the American people’ (quoted in
Stolberg & Lichtblau, 2006). On the following Monday, President George W. Bush harshly added to the critique condemning the disclosure of the TFTP, qualifying the publication by *The New York Times* and other media outlets as ‘disgraceful’ (quoted in Stolberg, 2006).

That same day President Bush defended the programme in terms very similar to those used immediately after the 9/11 attacks, presenting it as ‘a legal and effective tool for hunting down terrorists’. ‘We are at war with a bunch of people who want to hurt the United States of America, and for people to leak that program, and for a newspaper to publish it, does great harm to the United States of America’ (quoted in Baker, 2006). Such statements contributed to the ‘securitization’ or depoliticization of the TFTP, rendering it more difficult to question the legitimacy and effectiveness of the programme.

Although newspapers continued reporting on privacy and legal aspects of the SWIFT affair, the debates were increasingly centred on the newspapers that published the story and the officials who leaked it to the press. Democratic Congressman Ed Markey summarized the situation:

Bush, Cheney and other Republicans have adopted a shoot-the-messenger strategy by attacking the newspaper that revealed the existence of the secret bank surveillance program rather than answering the disturbing questions that those reports raise about possible violations of the US Constitution and US privacy laws. (quoted in Baker, 2006)

Republican critiques of the media were voiced to various degrees. In a letter to *The New York Times*, US Treasury Snow wrote that he was ‘deeply disappointed’ in the newspaper (Snow, 2006b). Others, for instance Senator Jim Bunning, also condemned the revelation of sensitive information (quoted in Bender, 2006). Senator Pat Roberts requested an assessment of whether the reports had damaged anti-terrorism operations (quoted in Bender, 2006), to which the Director of National Intelligence, John D. Negroponte, answered in the affirmative (Shane, 2006b). A number of Republican congressmen and senators were even more virulently opposed to the revelation of classified information that they claimed could harm national security. Some argued for criminal prosecution of the journalists. For instance, Congressman and Chairman of the House Homeland Security Committee, Peter King, said ‘I am asking the Attorney General to begin an investigation and prosecution of *The New York Times*, the reporters, the editors and the publisher’. ‘We're at war and for the Times to release information about secret operations and methods, is treasonous’ (quoted in Burkeman, 2006). He also said that the officials who leaked the classified information could be prosecuted for violation of the Espionage Act (Fox News, 2006). Other politicians (and
media outlets) accused those media that decided on publication of sensationalism and of letting commercial interests prevail over national security concerns.

In addition, certain media and Internet blogs also attacked the New York Times. This newspaper attracted the most attention because it was the first to disclose the programme, because of its (then) recent publications on the National Security Agency’s (NSA) eavesdropping programme and probably also for opportunistie electoral reasons (interview 13). In an editorial, The Wall Street Journal assailed the publication by The New York Times, reminding the newspaper that ‘not everything is fit to print’ and explaining that its own decision to publish on the SWIFT affair was based on different considerations (2006). A more simplistic and sensational attack came from former federal prosecutor Arthur McCarthy. He wrote that ‘the media’s war against the War continues’: ‘Yet again, the New York Times was presented with a simple choice: help protect American national security or help Al Qaeda. Yet, again, it sided with Al Qaeda’ (McCarthy, 2006). In the New York Post, a controversial cartoonist compared the New York Times reporting on the SWIFT affair to revealing George Washington’s surprise attack of crossing the Delaware River on 25 December 1776 during the American Revolutionary War, leading to the defeat of the forces of the British Empire in Trenton. The cartoon shows a British soldier reading about the planned surprise attack in the New York Times, suggesting that the disclosure of the SWIFT affair was an act of treason, informing terrorists of the secret attacks that were taking place on them (see figure 4.1).

Figure 4.1 If the New York Times had covered the Revolutionary War, Sean Delonas, New York Post, 28 June 2006.
While *The New York Times* and *The Los Angeles Times* discussed their plans for disclosing the secret programme with administration officials prior to the publication and explained their reasons for publication in their first articles, they felt forced by readers and the attacks of the Bush administration to respond to the criticism in public. In addition to the explanation already given in *The New York Times*’ first publication on the SWIFT affair, a number of letters by the executive editor of the newspaper, Bill Keller, followed in the weeks after the disclosure of the TFTP. Accused of being unpatriotic, unwise, and exposing the US to danger, Keller defended the publication as proof of an independent and critical press and as a ‘protective measure against the abuse of power in a democracy and an essential ingredient for self-government’ (Keller, 2006a). In his view, the more citizens know about the news, the better they are able to make decisions and make their views known to their elected officials (*ibid.*). ‘Our job, especially in times like these, is to bring our readers information that will enable them to judge how well their elected leaders are fighting on their behalf, and at what price’ (Baquet & Keller, 2006).

Keller further insisted that the decision to publish was not taken lightly, which was also attested by one of the journalists responsible for *The New York Times*’ publications. Not long after their publication on the NSA eavesdropping programme in December 2005, Risen and Lichtblau discovered that something was going on in relation to SWIFT. After discovering the first leads to the programme in 2005, it took the journalists one more year to obtain sufficient confirmation of the facts to publish the story. In his joint letter with Dean Baquet, editor of *The Los Angeles Times*, Keller explained the thorough consideration required before an article is published (Baquet & Keller, 2006). In addition, months before actually deciding to publish the SWIFT story, there had been several lengthy meetings with the US Treasury to exchange arguments (in favour and) against disclosure of the programme (Lichtblau, 2009, p. 250). Moreover, before publishing there was an extensive discussion within the editorial board of *The New York Times* on the question whether the public’s interest in unveiling the programme outweighed the potential threat to national security (*ibid.*, p. 251, Keller, 2006a). The newspapers tried to strengthen this argument by highlighting that they do not publish all information they receive on secret counter-terrorism programmes and missions (Baquet & Keller, 2006, Keller, 2006a, Lichtblau, 2009, p. 251).

Moreover, Keller, Lichtblau and others countered the argument that the publication of the SWIFT affair could help terrorists and lead them to change their tactics. They argued that the US government itself had already made reference to the existence of these kinds of programmes and actively sought to render some of its efforts public. ‘Treasury Secretary John
Snow himself had led reporters from major media organizations on a six-day tour to trumpet the administration’s supposed success in tracking terrorist financing and going after their dirty money’ (Lichtblau, 2009, p. 252). ‘The secretary’s team discussed many sensitive details of their monitoring efforts, hoping they would appear in print and demonstrate the administration’s relentlessness against the terrorist threat’ (Baquet & Keller, 2006). Keller and Lichtblau also stated that terrorism financiers already knew that their financial behaviour was being observed by governments. A former US diplomat involved in the UN efforts to combat terrorism financing states, ‘unless they were pretty dumb, they had to assume their transactions were being monitored’; ‘We have spent the last four years bragging how effective we have been in terrorist financing’ (quoted in Bender, 2006). Former US officials even argued that there had been explicit public references to SWIFT before in public sources, among them a 2002 report for the UN Security Council (Bender, 2006).

4.3.4 Swift Depoliticization

Quite surprisingly, none of the legal and privacy issues brought up by the journalists, politicians, and civil liberties groups led to heated political debates or further investigations in the US. Since the US does not have a centralized data protection authority, civil rights organizations such as the American Civil Liberties Union and certain politicians asked the US Congress to investigate the alleged privacy breaches (see ACLU, 2006b). However, the House of Representatives and the Senate decided not to open investigations into the TFTP. Within only a few days a political consensus appeared considering the legal basis of the TFTP and the privacy safeguards introduced to be sufficient. Once the congressional intelligence committees were briefed, they were, according to a senior congressional aide, ‘generally supportive of [the efforts to track terrorist financing]’ and ‘everybody thought they had appropriate controls’ (Miller & Meyer, 2006). Likewise, the open letter of Privacy International (2006d), requesting from SWIFT’s CEO a clarification about the company’s cooperation with public authorities, remained unanswered and did not stir any further debate.

On the juridical level, the potential privacy breaches of the TFTP were addressed in two separate lawsuits. Immediately after the disclosure of the programme on 23 June 2006, plaintiffs Ian Walker and Stephen Kruse filed a lawsuit against SWIFT in the US District Court in Chicago (Walker Kruse v. SWIFT SCRL). They claimed to have made at least one international transaction since 11 September 2001 and accused SWIFT of violating the First and Fourth Amendments of the US Constitution and the privacy rights of Americans by
disclosing private financial information to the government. The suit seeks statutory, compensatory, and punitive damages on behalf of every American who made a domestic or international financial transaction after 11 September 2001 (US District Court for the Northern District of Illinois Eastern Division, 2007a, De Young, 2006). A second lawsuit against SWIFT and a number of the highest government officials was filed exactly two years later on 23 June 2008 by a company called Amidax Trading Group on behalf of itself and all those similarly situated within the jurisdiction of the District Court of the Southern District of New York (Amidax Trading Group v. SWIFT SCRL et al.). This company also accuses SWIFT and the US government of violating the First and the Fourth Amendments of the Constitution as well as the federal Right to Financial Privacy Act, as it made Amidax’s financial information available to the US government by responding to the subpoenas issued by the US Treasury.

These lawsuits may be read as an attempt to ‘repoliticize’ the privacy questions surrounding the TFTP through a judgement on the question whether the programme violates privacy rights. However, these cases did not provoke much debate nor did they lead to any sustained attention to the alleged privacy breaches of the TFTP. After an initial attempt by the Department of Justice to have the case of Walker and Kruse dismissed on the basis of the state secrets privilege, the case was accepted but, at the request of SWIFT, it was transferred from Chicago to a federal court in Virginia (Lichtblau, 2007). The court ruled that the plaintiffs’ allegations were unconvincing as they could not provide evidence that their personal data were directly targeted by the TFTP (US District Court for the Northern District of Illinois, 2007b). Very similar arguments were used in the court case and the appeal filed by Amidax. The District Court and the Court of Appeals stated that the Amidax case failed to have standing because the plaintiff ‘did not allege facts giving rise to a plausible inference that its information had been disclosed as part of the TFTP, and therefore that it had suffered any injury-in-fact’ (United States Court of Appeals, 2010, pp. 1-2). Moreover, the Court of Appeals added among other issues that federal law immunizes SWIFT from liability for compliance with the subpoenas of the US Treasury (ibid., p. 37). The threat to shut down lawsuits concerning the TFTP on national security grounds, the impossibility for plaintiffs to prove that their financial data have been used in this secret programme, and the immunity of SWIFT with regard to the transfer of financial data make further attempts to sue SWIFT or US government officials for privacy violations very unlikely.

The criticism that was not entirely swept away in this moment of depoliticization was the lack of congressional oversight. Although the Bush administration had argued that
Congress was sufficiently informed and had been ‘on board with this all along’ (Miller & Meyer, 2006), several members of Congress had openly complained to the press that they had been left in the dark about the existence of the programme. An editorial piece in *USA Today* sketched the new ‘regime of truth’ in a few phrases. ‘It’s hard to imagine any American would not want the administration to go after terrorist financing’, and ‘it is improbable that Congress would have blocked the program’ (USA Today, 2006b). According to this article the Bush administration could have avoided any problems with the TFTP if it had ‘accepted the simple bargain’ of getting congressional approval. Hence, the problem with the TFTP was reduced to a failure to follow the procedures of democratic oversight, rendering the TFTP and the war on terrorist financing uncontroversial.

This reading of the SWIFT affair is further confirmed by the rapid adoption of the resolutions of the House of Representatives and the Senate. Both very strongly support the TFTP and condemn the disclosure of the programme by various media in the strongest words. The resolution of the House of Representatives even denies the critique raised by *USA Today*, stating on the contrary that ‘Congress has been appropriately informed and consulted for the duration of the Program and will continue its oversight of the Program’ (United States House of Representatives, 2006). The adoption of these two resolutions marked to a large extent the end of the SWIFT controversy, just one week after its disclosure.

The relatively limited concern raised by the disclosure of the programme can be attributed to the skilful handling of the affair by the Bush administration. On the one hand, it continually defended the programme in very forceful and personal terms. Before the House Financial Services Subcommittee on Oversight and Investigation Levey, for instance, stated, ‘I am very proud of this programme’: ‘For two years I have been reviewing the output [of the TFTP] every morning. I cannot remember a day when that briefing did not include at least one terrorism lead from this program’ (US Department of Treasury, 2006a). On the other hand, the Bush administration successfully changed the focus of the discussion in the US. Instead of discussing the content and implications of the TFTP, the media’s decision to disclose the secret programme became central to the debate.

In addition, it is also important to take into account the broader context in which the SWIFT affair took place. Six months earlier the *New York Times* had revealed a very sensitive eavesdropping programme run by the National Security Agency. This secret programme consisted of monitoring (international) phone calls and e-mail messages to and from American citizens and residents with the help of the biggest telecommunication companies and had provoked an enormous outcry amongst politicians and the population. Many
politicians and many citizens who were aware of the TFTP programme considered it to be on a firmer legal ground compared to the NSA eavesdropping programme. Moreover, they esteemed the collection of financial data much less controversial than wiretapping telephone calls and e-mail messages (interview 12). Representative Arlen Specter, for instance, declared on a TV show that ‘there is not the privacy interest in bank records that there is in a telephone conversation’ (quoted in Kornblut, 2006).

Furthermore, unlike the NSA programme that monitored communications of US citizens, the emphasis in the SWIFT affair was on international wire transfers. Hence, there was a strong belief among Americans that the programme only concerned foreign transactions and that their financial data were not subject to investigation. In short, SWIFT remained overshadowed by the NSA eavesdropping programme (interview 13) and was considered as ‘yet another spying programme’ (interview 12). In fact, the NSA scandal constituted an important lesson for the Bush administration on how to deal with criticism in reaction to the publication of a secret counter-terrorism programme. The Washington Post reported that this time, ‘far from giving ground, the administration mounted a muscular defence of the program [. . .]’ (De Young, 2006).

Finally, the newspapers’ own public discussions, in which they explained that the decision to publish the SWIFT story was difficult also contributed to depoliticizing the TFTP and strengthening the government’s security argument. In later publications, the public editor Byron Calame of The New York Times even stated that although he initially strongly supported the decision for publication (2006a), he later ‘altered [his] conclusion’, considering that he ‘was off base’ (Calame, 2006b), and even spoke in terms of a ‘mea culpa’ (Calame 2006b, 2006c). The long-term implications of this mea culpa became visible two years later in the context of ‘The Free Flow of Information Act of 2007’. The objective of the proposal for this act was to maintain the free flow of information to the public by providing conditions for the federally compelled disclosure of information by certain persons connected with the news media. In a response to the proposal, US Secretary of the Treasury Henry M. Paulson wrote that the Department was strongly opposed to providing a ‘journalist privilege’ for unauthorized disclosure of government programmes. To strengthen his argument, he discussed the disclosure of the TFTP at length as an example of media coverage that had damaged national security and he emphasized the fact that even the newspapers that had published on the programme now acknowledged their error (Paulson, 2008).

In short, after a short political moment, three questions became politicized in the US debate about the TFTP. These were the constitutionality of the programme, the respect for
privacy, and the newspapers’ decision to publish information about the programme. Framing the debate around questions of legality, national security, and, (connected to this) morality helped quickly and successfully to depoliticize the programme with arguments that were difficult to refute. By ascertaining that the programme was entirely legal, the Bush administration, the US Congress, and later the US courts normalized and legitimized the TFTP. Likewise, the Bush administration, Republican politicians, and certain media organizations defended the programme on the basis of their personal convictions and values and with an appeal to national security, while they accused the newspapers that decided to publish the SWIFT story of a lack of patriotism and professional integrity. The invocation of the argument of national security made it very difficult to challenge the arguments of the Bush administration and to ask questions belonging to the sphere of the political.

4.4 The EU Debate

After the clandestine flights, the abduction of European citizens rightly or wrongly under suspicion and the illegal transfers of prisoners using aircraft landing on European soil, we now learn that, friend of ours though it may be, a power in alliance with ourselves has been rooting around in our bank accounts. When will the blood samples start to be taken? When shall we start having to submit details of births and so forth? Emphatically, enough is enough. Parliament really does need to put a stop to this type of thing.16

—Jean-Marie Cavada, European Parliament, 2006

[In response to the adoption of the US–EU SWIFT agreement:] The true problem remains the incapability of the European Union to equip itself with a computer analysis tool for the analysis of data exchanges similar to that of the United States.17

—Jean-Marie Cavada, press statement, 2010

For more than four years the European Parliament was closely involved in the political handling of the ‘SWIFT affair’ in Europe. The two quotes above illustrate the strong contrast between the broad critique raised in the first reactions to the disclosure of the TFTP in 2006, and the understanding of the issues at stake when an agreement between the US and the EU on this matter was reached in 2010. They not only reflect the evolution in the ideas of the liberal French Member of the European Parliament (MEP) Jean-Marie Cavada (Alliance of Liberals and Democrats for Europe (ALDE)), who presided over the European Parliament’s civil liberties committee (LIBE) from 2004 to 2009, but also represent a shift that took place more broadly in the European Parliament and in EU member states. This section analyses the
political and societal debates in the EU in reaction to the disclosure of the TFTP and distinguishes four different phases in these debates. These phases, it must be emphasized, do not exactly mirror the debates in the US with regard to their duration or their content (see table 4.2). A moment of openness following the publications in American newspapers during which the ‘SWIFT affair’ was hotly debated constitutes a first phase. Contrary to the US situation, in the EU the moment of openness in the debate lasted for several weeks. A second phase consisted of the politicization of certain aspects of the SWIFT affair. During this period, roughly from July until December 2006, newspaper articles on the SWIFT affair continued to appear regularly. Between 2007 and 2009, a third phase of slow depoliticization took place. Finally, a fourth phase of re-politicization can be distinguished, lasting from the last months of 2009 until August 2010.

4.4.1 Moment of Openness: the Mobilization of the European Parliament

Immediately after its disclosure by the press in the US, media across Europe became interested in the SWIFT affair. While the European press initially only reported on the revelations and the debate in the American media, a distinct European debate emerged after a few days. The period that followed can be seen as a moment of openness, during which a range of representatives from public and private authorities – such as the European institutions, national ministries, central banks, NGOs, SWIFT, and banks – reacted freely on the various aspects of the disclosed security programme.

The London-based civil rights group Privacy International rapidly started a campaign to put a halt to the transfer of SWIFT data (Privacy International, 2006c). Four days after the revelation of the secret programme the organization filed complaints with data protection regulators in over 30 countries, including all of the EU member states (Privacy International, 2006a). In its complaints it called for ‘an immediate halt of the [financial data] transfers until essential questions regarding due process and privacy protections can be answered adequately’ (Privacy International, 2006b).

In the European newspapers, one of the first issues that emerged consisted of determining the role of the public and private authorities in this affair on both the European and national levels. While many governments and banks were indeed not informed about the secret programme, those who were informed tried to minimize their responsibility in the affair. The Dutch National Bank, which had known about the data transfers since 2002, distanced itself from the SWIFT affair, qualifying it as an ‘American issue for SWIFT’
(Tamminga, 2006). The National Bank of Belgium, also aware of the programme since 2002, stated that the data transfers to the US were ‘beyond its control’ (Bilefsky, 2006). According to the Belgian central bank, the central banks of the Group of Ten countries (G-10)\(^{18}\), called the Oversight Group, monitors SWIFT’s activities but only ‘insofar as they are relevant to the maintenance of financial stability’. Since the US Treasury subpoenas did not affect financial stability they were considered ‘outside the purview of central bank oversight’ (National Bank of Belgium, 2006). SWIFT itself stressed that it had to comply with all applicable laws in the US and had no choice but to transfer its database to the US Treasury (SWIFT, 2006a).

The European Commission also denied any responsibility in this affair. A spokesperson for the European Commission declared that ‘the Commission had no powers to investigate the decision by SWIFT to supply the US government with information about bank transfers’ (quoted in, \textit{inter alia}, Bilefsky, 2006). Moreover, it was argued that there was no European legal framework regarding security-related data transfers since the existing privacy directive only targeted data transfers for commercial purposes (Quatremer, 2006). Another spokesperson stated that the Commission judged that no European laws had been violated with respect to this case (EuroNews, 2006). Hence, Commission officials suggested that member states should open up investigations on a national level.

Similarly, the Finnish President of the Council declared that the Council ‘cannot confirm […] or comment’ on the revelation of the TFTP and that ‘the national authorities are responsible for this sort of enquiry’. Furthermore, the Council ‘assumes that the cooperation between private companies like SWIFT and the US authorities will be in accordance with applicable law and in compliance with fundamental rights’ (European Parliament, 2006a).

Despite the rapid conclusion of the European Commission and the Council that the matter primarily concerned the individual member states, the European Parliament took a major and persisting interest in the SWIFT case. A first plenary session on the issue was held on 5 July 2006 and can be understood as a moment of openness in the European debate. During this session, various criticisms of the revelations were voiced and the SWIFT affair was debated from multiple perspectives.

The vast majority of MEPs who intervened declared themselves to be highly concerned about privacy breaches and the respect for data protection norms. For instance, Dutch MEP Sophie in ’t Veld (ALDE) stated that
European citizens have never been told about the details of their bank accounts being monitored, and I regard it as a precondition that they should be. I wonder how we would react if it were not the United States, but another country, that was checking our bank accounts, and whether we would be equally tolerant of that’ (European Parliament, 2006a).

Similarly, Italian MEP Giovanni Claudio Fava (Party of European Socialists (PES)) argued:

[. . .] the Union is an area that is bound by the rules and principles of the rule of law and that, therefore, personal data, all personal data, including our current account data, must not be given to third countries, except in the cases provided for under national laws and now under European directives; there are no exceptions, not even in the name of the fight against terrorism. Anything that goes beyond this constitutes an arbitrary act and an abuse of the system (European Parliament, 2006a).

Aside from the data protection and privacy concerns, the SWIFT affair was also put in a broader economic and international relations context. MEPs were concerned about the possibility for the US ‘to detect not only transfers linked to illegal activities, but also information on the economic activities of the individuals and countries concerned, and could thus be misused for large-scale forms of economic and industrial espionage’ (European Parliament, 2006b). Sophie in ’t Veld also argued that ‘we expect from an allied nation that they inform [the EU] about these kinds of operations’ (quoted in Van der Kris, 2006).

Several MEPs also expressed their concern with respect to the wider societal implications of the SWIFT affair. In response to the various authorities that declined to bear any responsibility, Cavada passionately argued: ‘we must not forget that the members of the Commission and the Council are our government; if they have no means to act against this scandal and do something, it doesn’t prevent you from showing moral virtue and demonstrating and stating what you think about it’ (European Parliament, 2006b). Italian MEP Giusto Catania (Group of the European United Left/Nordic Green Left (GUE/NGL)) stated that ‘for the future of Europe we have to stop the CIA dictating law in Europe’ (European Parliament, 2006b).

MEPs also argued that the SWIFT affair should not be seen in isolation. They drew attention to the similarities with other once-hidden programmes in the US War on Terror such as the secret CIA rendition flights and the secret prisons. According to Dutch MEP Jan Marinus Wiersma (PES), ‘the SWIFT affair is part of the broader discussion on the balance between liberty and security’ (European Parliament, 2006b). He stated that ‘the SWIFT case is not an isolated one, but an example of the way in which the Americans, in particular, hope to fight terrorism’, and that a thorough discussion on the nature of the War on Terror was indispensable (European Parliament, 2006a). Connections were also made with counter-
terrorism programmes that make use of massive datasets. Greek MEP Stavros Labrinidis (PES) stated, ‘PNR [Passenger Name Records], SWIFT, [telecommunications] data retention: in all these cases private individuals are collating data and the police are using them on the pretext of terrorism’ (European Parliament, 2006a). In Catania’s view, these programmes lead to a Big Brother Society as described in Orwell’s 1984 (European Parliament, 2006a).

The day after the plenary session, the European Parliament adopted a resolution on the SWIFT affair. In this resolution the EP also referred to the complaints filed by Privacy International and it demanded that the European Commission, the Council, and the European Central Bank (ECB) explain the extent of their awareness of the secret agreement between SWIFT and the US government, and asked the European Data Protection Supervisor to establish whether the ECB had violated Regulation 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. The resolution also stressed the urgent need for the adoption of a regulation covering data protection in the EU’s ‘third pillar’ (this is the framework of police and judicial cooperation in criminal matters) (European Parliament, 2006c).

Although the EP’s resolution ‘requests that the Commission undertake an evaluation of all EU anti-terrorist legislation that has been adopted from the point of view of efficiency, necessity, proportionality and respect for fundamental rights’ (European Parliament, 2006c), the SWIFT debate was somewhat narrowed down rather than being opened up to these broader issues. Within a month after disclosure, the moment of openness disappeared and the discussion about the SWIFT affair became focussed on two main issues: privacy and the Data Protection Agency’s investigations into potential violations of privacy laws on the one hand, and the negotiation of an agreement with the US Treasury to legalize the transfer of SWIFT’s financial records on the other. The next section discusses the politicization of these two issues.

4.4.2 Politicization: Privacy and the Data Protection Law

At the request of the European Parliament and civil rights groups and on their own initiative, data protection agencies opened investigations into the allegedly illegal transfer of financial data from SWIFT to the US Treasury. The main objective of these investigations was to check if any European or national privacy and data protection laws had been violated. Since SWIFT is a cooperative under Belgian law, the Belgian Privacy Commission
The Belgian Privacy Commission issued three reports concerning SWIFT. The first two reports were published in 2006, opinion 37 on 27 September and opinion 47 on 20 December, and a final decision was published on 9 December 2008. The main objective of the first investigation was to determine if (Belgian) data protection law is applicable to SWIFT and whether the reported data transfers to the US Treasury constituted a violation of the law. These reports mainly discussed the applicability and interpretation of national and European privacy law. One of the key questions for the Belgian Privacy Commission was to determine whether SWIFT is a ‘processor of data’ or a ‘controller of data’. This is an important legal distinction introducing different levels of responsibility with respect to privacy safeguards. SWIFT CEO Lazaro Campos asserted, ‘SWIFT has always maintained that it is a “processor of data” and not a “controller of data”’ (SWIFT, 2007, p. 17), while the Belgian Privacy Commission qualified SWIFT as a controller of data (Belgian Privacy Commission, 2006a, p. 11). The investigation of the Belgian Privacy Commission also focussed on the transfer of data to American authorities (the US Treasury’s Office of Foreign Assets Control and the CIA) via the SWIFTNet FIN service.

The Belgian Privacy Commission was very critical of SWIFT and expressed great concern about the lack of transparency surrounding the arrangements it had made with the US Treasury. In its first report it stated that ‘SWIFT [. . .] should have realized that the exceptions under American law could hardly justify a secret, systematic and large scale violation of the basic European principles of data protection which went on for years’ (2006a, p. 21). It regrets SWIFT’s decision to ‘comply with American law and searching solutions via secret negotiations’ instead of opting for alternative systems that would respect European data protection laws and consulting European data protection authorities (ibid., p. 22). The Belgian Privacy Commission was also negative about the nature of the subpoenas, which, it argued, could be qualified as ‘non-individualised mass requests’ (2006a). In addition, it accused SWIFT of serious misjudgements and shortcomings in light of European privacy and data protection law.

The Belgian government requested a second report from the Belgian Privacy Commission that would investigate the solutions for the lack of an equivalent level of data protection between the EU and the US and indicate the possible frameworks for an EU-US agreement on the transfer of SWIFT data to the US Treasury. This second report (opinion 47
of 20 December 2006) was still critical of SWIFT but extended its critique to the role of American and European authorities in the TFTP. It emphasized that there was still no proof of the vital interest of the SWIFT information for combating terrorism and that contestation over the secret initiation of the TFTP by Belgian and European authorities was appropriate (2006b, p. 2). In its recommendations, the Belgian Privacy Commission also emphasized that ‘the conclusion of a specific agreement with the US is not the only manner to solve the lack of equivalent protection between the EU and the US’ (ibid., p. 11). They suggested alternatives to such an agreement, drawing attention to existing procedures for exchanging financial data. Furthermore the BPC stated that the minimum requirements for an agreement must be Belgian and European privacy and data protection laws and these existing laws would need to be sharpened to avoid any legal voids.

On a European level, the Article 29 Working Party, in which the national data protection agencies in the European Union cooperate, as did the European Data Protection Supervisor (EDPS), issued opinions on aspects of the transfer of financial data from SWIFT to the US authorities. The investigation of the Article 29 Working Party published on 22 November 2006 was the most comprehensive. Supporting the critical conclusions of the Belgian Privacy Commission’s report, it also established that the existing EC directive 95/46 on data protection applied to SWIFT’s data transfers. Moreover, this report took into account the role of the financial institutions using SWIFT’s network and central banks. The Working Party disagreed with the argument made by banks and central banks that they had no responsibility or competency with respect to upholding privacy and data protection safeguards. In its view, ‘SWIFT and the financial institutions in the EU have failed to respect the provisions of the Directive [95/46]’ (Article 29 Working Party, 2006, p. 26). Furthermore, the working group required a number of immediate actions to be taken to improve the current situation. These immediate actions included a cessation of the infringements, an immediate return to lawful data processing, and a clarification of central banks’ oversight of SWIFT.

The competencies of the EDPS for investigation are limited to data protection issues concerning European institutions and agencies and in this case the EDPS analysed the responsibility of the ECB in the SWIFT affair. In the opinion issued on 1 February 2007, the EDPS addressed the position of the ECB as an overseer of SWIFT, as a user of the SWIFTNetFin service, and as a central policy maker (EDPS, 2007). Contrary to the ECB’s own judgement, the EDPS found that the transfer of SWIFT’s data to the US concerned the ECB in its role as overseer. The EDPS argued for instance that ‘the lack of compliance with data protection legislation may hamper the financial stability of the payment system’ because
‘it could seriously affect consumers’ trust in their banks’ and ‘because it might lead European data protection authorities [. . .] to use their enforcement powers to block the processing of personal data which are not in compliance with data protection law’ (p. 8). On the role of the ECB as a user of the SWIFTNet Fin service, the EDPS concluded that the ECB must also be considered a ‘data controller’ and therefore it has strict responsibilities with regard to the processing of data (pp. 8-10). Finally, the EDPS stated that failed compliance with European data protection rules was a breach of EU citizens’ fundamental rights and potentially exposed European companies to economic espionage. Therefore, the ECB as a policy-maker needed to ensure that European payment systems were fully compliant with European data protection law (p. 12).

The European Parliament Committees on Civil Liberties (LIBE) and on Economic Affairs (ECON) also held a hearing aimed at gathering more information about the respect for data protection laws in the TFTP and whether changes in European law were needed. They invited and questioned a representative from SWIFT, the presidents of the ECB and the EDPS, the president of the Article 29 Working Party, and the head of the European Commission’s Data Protection Unit. In their reactions, the MEPs asked for more detailed information such as the memorandum of understanding between SWIFT and the US, the audit reports on the American data searches, and the legal basis for the institutional set-up of the SWIFT databases. At this point it was said that ‘the wider issue was whether the United States in general provided adequate levels of data protection to comply with the EU requirements for European companies to store or process data there’ (European Parliament, 2006d, p. 2).

From these initiatives, it becomes clear that the political response to the SWIFT affair in Europe was to set in motion investigations led by data protection agencies. The European Parliament was very mobilized in debating the TFTP but until 2010 it had limited legal powers with regard to international security matters. Consequently, the debate became mainly framed as a privacy and data protection issue and other questions that officially fell outside the competencies of the European Parliament and the data protection agencies were pushed to the background. Next, despite the critique expressed by data protection agencies, their reports did not lead to an immediate halt or suspension of the data transfers. The Belgian Privacy Commission’s second opinion, for instance, served the preparation of a first agreement with the US on the transfer of personal data by SWIFT to the US Department of the Treasury. As such, the reports were used to legitimize the continuation of the TFTP by remodelling the programme within the limits of European data protection law.
4.4.3 A Series of Ad Hoc Solutions Depoliticizing the ‘SWIFT Affair’

While the SWIFT affair remained a highly politicized issue for several months, the disclosure of the SWIFT affair was immediately followed by attempts to depoliticize the situation and by efforts to maintain the existing power relations. This is illustrated by the attempts of private and public authorities to minimize their responsibility in this affair and by the focus on the technical and legal aspects of data transfers. Independently from each other, EU member states took steps to ‘solve’ the SWIFT affair. In cooperation with the Dutch Privacy Commission (College Bescherming Persoonsgegevens (CBP)), the Dutch Banking Association (Nederlandse Vereniging van Banken (NVB)) and Dutch banks, for instance, decided to publish an advertisement on their webpages and in national newspapers informing their customers about the fact that their financial data might be stored and become part of counter-terrorism investigations in foreign countries. Commenting on this issue, the Dutch Ministers of Justice and of Finance stated that there was no possibility for customers to avoid the transfer of their financial data when an international payment is made through the SWIFT system (Ministerie van Financiën, 2007, p. 4). Thus, customers of Dutch banks could not prevent their data from being transferred to the US but now they were at least informed about it.

On a European level the SWIFT affair was further depoliticized by the decision not to prosecute SWIFT and to start negotiations with the US instead. Despite the conclusions of the Belgian Privacy Commission and the Article 29 Working Group that European privacy laws had been breached, the Belgian Courts investigating the allegations against SWIFT reached the conclusion on 13 December 2006 that the European privacy framework did not apply to the SWIFT case (Notte, 2009, p. 48). The decision not to take any legal action was also attributed to a work overload (Fuster et al., 2008). Belgian Prime Minister Guy Verhofstadt was also not in favour of prosecuting SWIFT. He concluded from the reports of the privacy commissions that the EU and the US should negotiate about a ‘clear legal framework’ for transferring financial data (Deweerdt, 2007, p. 314). In 2011, in response to allegations that he had actively tried to circumvent the prosecution of SWIFT made on the basis of Wikileaks documents, Verhofstadt declared that at that time ‘the intention was to find a proactive solution in order to avoid the problem’ of having to prosecute SWIFT (De Standaard, 2011).

In the second half of December 2006, European Commissioner for Justice Freedom and Security, Franco Frattini announced that ‘he plans to initiate discussions in early January, 2007, with the US Government to address matters surrounding the SWIFT case’ (SWIFT,
2006b). From early 2007 onwards, three important initiatives were undertaken by SWIFT, the US Treasury, and the EU to find new grounds for continuing the TFTP.

First, in attempting to fit into existing legal frameworks and to comply with privacy safeguards in the US and in Europe, SWIFT decided to adopt the Safe Harbour privacy principles in April 2007. The seven Safe Harbour principles had been adopted by the European Commission in 2000 in order to facilitate the transfer of personal data from the European Community to the US, ensuring an adequate level of data protection according to European privacy and data protection laws (European Commission, 2000). The principles were initially designed for American companies, which could choose to adhere to these principles, as for instance Microsoft had done (De Hert & De Schutter, 2008, p. 315). However, as Fuster et al. rightly point out, SWIFT is a European company with branches in the US. Having its headquarters in Belgium, SWIFT should in the first place comply with Belgian laws on privacy and data protection, which provide a higher standard of protection than the Safe Harbour principles (2008, p. 197).

Secondly, the European Commission and the Council Presidency negotiated a set of unilateral commitments, the so called ‘representations’ of the US Treasury, in response to the critical reactions voiced by European governments and the European Parliament. These representations were made public on 28 June 2007 (European Union, 2007). Aiming to reassure Europeans, this document on the one hand summarizes the inception, the general procedures and the (international) legal grounds of the TFTP, and on the other hand describes the controls and safeguards integrated into the TFTP. The representations emphasize the legality of the programme, the restricted and targeted use of the data obtained, and the extraordinary value of the intelligence extracted from SWIFT’s database. The safeguards explicitly mentioned in the representations are the restriction to use the data exclusively for counter-terrorism purposes, adoption of technical and organizational measures to control access and ensure the security of the computer system, the internal and external oversight of the TFTP, dissemination and information-sharing procedures, the (limited) possibilities for redress, and the period during which the data records are retained. In addition, in the document the TFTP is placed in a framework of well-established international initiatives for combating terrorism financing such as the 1999 UN International Convention for the Suppression of the Financing of Terrorism, numerous UN resolutions on this issue, and the recommendations of the FATF (European Union, 2007, pp. 19-20). The document highlights that the TFTP not only protects America’s citizens and national security but also other persons around the world and other countries’ national security. Both arguments aim to render
the TFTP more acceptable to Europeans and contribute to forgetting the highly secret and dubious background of the programme.

It must be emphasized that the representations reflect to a large extent the controls and safeguards that had already been informally negotiated by SWIFT with the US Treasury in spring 2003, when SWIFT realized that the TFTP was not a short-term operation. Increasingly worried about SWIFT’s potential liability, a delegation from SWIFT was invited to the White House where it was given ‘red-carpet treatment’ (Lichtblau, 2009, p. 323). Top officials and key figures including National Security Advisor Condoleezza Rice, FBI director Bob Mueller, and Federal Reserve Chairman Alan Greenspan, all attempted to convince the company of their continued cooperation (ibid.). While the company had been heavily criticized after the disclosure of the programme, the perception of the role played by SWIFT changed in the course of 2007. The critique of the role of the company in the SWIFT affair faded and instead the company’s manner of continuing the TFTP under sharpened conditions was now accepted.

This shift also becomes clear from the third and final report on the SWIFT affair of the Belgian Privacy Commission published on 9 December 2008. The critique of SWIFT has largely disappeared and the report praises the company instead. It states that ‘nothing confirms the suspicions that SWIFT has seriously and repeatedly violated the law. The company acted with such caution that the data requested from SWIFT/USA by the American authorities were duly protected’ (Belgian Privacy Commission, 2008a). Moreover, the Belgian Privacy Commission stressed that SWIFT had meaningfully cooperated in improving privacy safeguards and accepting the Commission’s decisions. In fact, according to the Belgian Privacy Commission, the lesson to be learned was that ‘private companies are unable to combat the risks alone when data they have legitimately acquired are confiscated and unfairly exploited by certain states, nor are they capable of bearing all the consequences’ (2008b). The shift in the consideration of SWIFT from accomplice to almost a victim took place not only in the Belgian Privacy Commission’s reports, but also among members of the European Parliament (interview 6).

A third initiative aimed at rendering the TFTP less controversial was the designation of an ‘eminent European person’ reviewing the procedures governing the handling, use, and dissemination of the SWIFT data subpoenaed by the United States Department of the Treasury. This initiative was part of the representations announced by the Treasury Department. On 7 March 2008, the European Commission appointed the French counter-terrorism judge and active member of President Sarkozy’s party UMP, Jean-Louis Bruguière
for this function. According to EU Justice Commissioner Franco Frattini, ‘Jean-Louis Bruguière is a prominent and highly regarded figure in counter-terrorism circles both in Europe and the United States’ (European Commission, 2008). However, instead of reassuring the European Parliament, the appointment of Mr. Bruguière and the publication of his reports in December 2008 and January 2010 led to heated discussions.

The appointment of Mr. Bruguière was controversial in the view of some MEPs. According to them, he was not neutral because of his 30-year career in prosecuting terrorists in France and his very close relations with the American law-enforcement community. Moreover, Jean-Louis Bruguière had no record of defending privacy and data protection rights, which made him an ‘unconvincing’ candidate for this job (in ’t Veld, 2008). Moreover, according to some MEPs, ‘while discussing his first report Mr. Bruguière made a very big mistake. He made political comments defending why the programme is so important’ (interview 11), while the European Parliament had demanded an objective report presenting the facts.

After the publication of the Bruguière reports of December 2008 and January 2009 MEPs were briefed via in camera sessions about the confidential aspects of the TFTP and they had the right to consult the Bruguière reports under certain conditions. They complained repeatedly about the lack of evidence provided by either the US authorities or the Council of the EU to justify the need for the programme. One MEP declared,

I do not understand why those reports are classified. They are very general and they do not contain the many details that we were looking for. It says what is good about the programme and what could be improved. It is claimed that the programme provides many intelligence leads to the Europeans, it is completely unclear, however, if these leads have led to any indictments (interview 11).

Likewise, Portuguese MEP Tavares (GUE/NLG) stated that to justify the TFTP ‘the repeated references to the Bruguière Report, a secret report, are [. . .] unacceptable. This is hardly convincing as anyone who had read the Bruguière Report knows that it contains almost no empirical data’ (European Parliament, 2010a).

Some were also critical of the fact that the second Bruguière report stresses the importance of the TFTP by referring twice to the foiled terrorist attack on 25 December 2009 on a flight from Amsterdam to Detroit. They felt that linking this attempted terrorist attack, which took place on Christmas Day and just before the publication of the Bruguière report in January 2010, with the TFTP was one of the attempts to convince MEPs of the great value of the programme. Yet, in the words of one MEP, ‘SWIFT [data] had nothing to do with the Christmas attack as it was one of the passengers who stopped the terrorist’ (interview 11).
Although highly confidential, a summary of the first Bruguière report and a complete version of the second report are in fact available on the Internet. The seven-page summary is very general. It repeats the content of the representations, describes the designation and mandate of the ‘eminent European person’ and summarizes the three missions to Washington that Bruguière had undertaken to ‘ensure a proper understanding of the TFTP and the various data protection safeguards surrounding it’ (Bruguière, 2008, p. 4). However, none of his findings, except for his conclusion ‘that the Programme has made a real contribution to counterterrorism efforts’ and the announcement of ‘a series of detailed and specific recommendations regarding the operation of the Programme’, are included in the summary (Bruguière, 2008, p. 6).

The first five pages of the twelve-page second Bruguière report are rather general too. They contain an executive summary, a background section on the TFTP, a reminder of the principal controls and safeguards surrounding the TFTP, and a description of the evolution of the TFTP. The last seven pages cover the investigation of Judge Bruguière on the implementation of the TFTP. The focus of his analysis is threefold. First, it describes and assesses the measures taken by the Treasury in response to Bruguière’s recommendations set out in the December 2008 report. Second, the report considers the compliance with the data protection safeguards set out in the TFTP Representations. Third, it looks at whether the TFTP has contributed to provide a high level of added value to the fight against terrorism, notably in Europe (Bruguière, 2010). Throughout the report, it is emphasized that ‘the TFTP must be seen as an important and highly valuable source of reliable information which has provided police and other services with significant intelligence for the fight against terrorism’ (Bruguière, 2010, p. 12).

In sum, the Safe Harbor Agreement, the US representations, and the appointment of the eminent European person assured the continuation of the TFTP. Despite their improvised and ad hoc nature, outside conventional frameworks of international cooperation, these initiatives normalized and legitimized the surveillance programme, providing it with an alternative legal framework and a certain degree of oversight. In addition to these initiatives, there have been continuous negotiations between the US and the EU in order to establish a more comprehensive agreement. However, before such an agreement was finally adopted in August 2010, SWIFT’s decision to change its processing architecture, withdrawing its mirror database from American soil, and the expiration of the existing interim arrangements between the EU and the US Treasury caused a new period of politicization.
4.4.4 Repoliticizing the TFTP

The SWIFT affair became front-page news again from the end of 2009 through the first half of 2010. The renewed politicization of the SWIFT affair resulted from SWIFT’s decision to review its global messaging system. In order to ‘cope with future capacity increases’, SWIFT adopted a ‘new policy to enhance flexibility and efficiency through a regionalisation of [SWIFT’s] data processing centres’ (SWIFT, 2007, p. 17). This new regional architecture can also be seen as a direct response to the complaints following the TFTP since it would ‘improve our commercial appeal in some jurisdictions’, allowing for different data privacy arrangements (ibid.). More specifically, it implied that from December 2009 European financial data records would only be held in Europe—in the existing datacentre in Zoeterwoude in the Netherlands and in a new mirror datacentre in Diessenhofen, located in non-EU member state Switzerland. Through the changed architecture, European data would cease to be automatically available in bulk to the US. In order to assure continued access of the US to all SWIFT data after the expiration of the existing agreement on 31 January 2010, a new EU-US agreement had to be adopted before the end of 2009.

The adoption of this new agreement led to a serious power struggle between the US and the EU as well as among the European institutions. With respect to the latter, the Commission and the Council had started negotiations with the US in July 2009, involving the ECB and the EDPS but without informing the European Parliament. They considered that because the EU-US agreement was negotiated as a third pillar issue, according to which the European Parliament had no formal decision-making powers, there was no role for the European Parliament. Moreover, the Commission and the Council aimed to have the agreement in place before the Lisbon Treaty entered into force as they believed that the involvement of the Parliament could take at least six additional months of negotiation (Taylor, 2009). In turn, the European Parliament learned about the negotiations for an agreement from the press but it considered that although the powers of the Parliament are limited, the treaty prescribed the right of Parliament to be consulted by the Council before an act is adopted. In September 2009, the EP reacted to the envisaged international agreement by organizing hearings and adopting a resolution in which the Parliament expressed its critique of the envisaged agreement and repeated its concerns about data protection and privacy breaches as well as economic espionage (European Parliament, 2009a, 2009b).

In the negotiations between the EU member states and the US, Austria, Germany, Greece, and Hungary were very reluctant to normalize the TFTP programme. They continued
to have concerns that the interim agreement would not include sufficient guarantees on data protection (Monar, 2010, p. 146, Taylor, 2009). The debate on the interim agreement was particularly vivid in Germany where the German Bundesrat, the German Federal Crime Office (BKA), German MEPs, and German members of the Council such as the Minister of Justice, Sabine Leutheusser-Schnarrenberger, were very critical of the TFTP while Chancellor Angela Merkel, and the Minister of the Interior, Thomas de Maisière, defended the agreement (Dretzka & Mildner 2010, Monar, 2010). In order to obtain the consent of Germany, Austria, Greece, and Hungary, the highest US officials, including US Treasury Secretary Timothy Geithner and Secretary of State Hillary Clinton, tried to put them under pressure. This is confirmed in one of the Wikileaks cables in which the US Embassy in Berlin reports that ‘Germany relents following intense pressure’ and that the ‘German vote [which allowed the agreement to pass] comes with costs for the coalition [the US]’ (Embassy of the US in Berlin, 2009). By obtaining one of the revisions it demanded—a reduction of the duration of the interim agreement from one year initially to nine months—Germany was willing to stop blocking the agreement. Finally, all four countries decided to abstain from voting when the interim agreement was adopted on 30 November 2009.

The European Parliament was very disappointed and angry about the adoption of an interim agreement just one day before the Lisbon Treaty was to enter into force. It stressed that the timing of the adoption of this interim agreement was significant since under the Treaty of Nice the EP had no formal competencies to control or to be otherwise involved in the decision-making process concerning third pillar issues. The Treaty of Lisbon, on the contrary, would make it possible for the EP to debate and alter the agreement as it was given co-decision power.

Nevertheless, in the end the members of the European Parliament had the opportunity to influence the adoption of the EU-US agreement. According to the formal procedures, ‘there are three stages to the signature of an agreement: complete, adopt, and conclude. On 30 November the agreement was completed but not yet concluded before the Treaty of Lisbon entered into force’ (interview 11). Practically this meant that the EP could not change the text of the agreement anymore but it would gain the right to endorse or reject the negotiated text.

Many MEPs were annoyed by the initial decision of the Council and the US authorities to sign the agreement just before the European Parliament was to acquire new powers. The dissatisfaction of the EP with the Council and the Commission grew as the MEPs found that they did not receive the relevant documents in time and they were put under pressure to give their consent to the agreement quickly. In reaction to this situation, German
MEP Manfred Weber (European People’s Party (EPP)) stated during the parliamentary debates about the interim agreement reached in February,

This whole debate was, of course, initially coloured by the frustration and irritation that many people in the European Parliament felt because we had the impression that, once again, things were being rushed through in the Council before the entry into force of the Treaty of Lisbon (European Parliament 2010a).

Other MEPs complained about the ‘undue haste’ or ‘breakneck speed’ of the procedures. They were critical of the fact that they had received important documents only a few days before the vote of the Parliament was scheduled. The second Bruguière report was made available to the EP just a few days before the vote. MEPs protested that they were never informed about the preparation and publication of this report, and considered that the timing of the report made it impossible to take it into account before the vote. In addition, the text of the agreement was not provided to the EP before 25 January because of delays in translating the document. MEPs called this argument into question and qualified it as ‘unacceptable’, ‘something that cannot be taken seriously’, and they reminded the Council that ‘parliamentary consent must not be a retrospective tool’ (European Parliament, 2010a).

The relations between the majority of the EP on the one hand and the Commission and the Council on the other further deteriorated as the latter sought to persuade the MEPs to vote in favour of the agreement. Proponents of the agreement—the Council but also members of the EPP—referred to a ‘security gap’ that would arise in case of a rejection of the agreement (EurActiv, 2010, Pop, 2010a). They meant that when data transfers to the US authorities ended, ongoing and new investigations into terrorist networks on the basis of SWIFT data would be frustrated, which would pose an unacceptable security risk. It may be noted however, that when the agreement was rejected, SWIFT decided to increase the storage time of its data beyond the regular period of 124 days. This would allow the US authorities to request the missing data when a new agreement would be negotiated. Moreover, as argued by several MEPs, the US could still obtain financial data through traditional channels of international judicial aid and existing legal frameworks of police cooperation.

Furthermore, proponents of the agreement argued that the EP used the agreement for its own political purposes and that a rejection of the agreement would put lives at risk. An EU diplomat for instance warned against ‘playing politics with the security of our citizens’ (quoted in Pop, 2010a). US Secretary of State Hillary Clinton also personally called Jerzy Buzek, the President of the European Parliament, to convince EU lawmakers not to reject the agreement and Stuart Levey, the Under-Secretary for Terrorism and Financial Intelligence, wrote an article in Europolitics warning against the “tragic mistake” of scrapping the deal.
Representatives from the Council even accused the European Parliament of using the SWIFT case to show its increasing powers. According to one highly placed European official, the European Parliament was not so much opposed to the agreement but was interested in a power play (interview 20).

In the debates of 20 January 2010 held in the European Parliament to prepare for the vote on the US-EU interim agreement, the TFTP was again considered from a wide range of perspectives. In addition to their attention to data protection safeguards, MEPs questioned the effectiveness of the programme and the desirability of international cooperation in this field. They asked the Ministers of the Interior to ‘convince Parliament that these methods that are now being proposed in this agreement really are necessary for the fight against terror’ and to ‘explain to us where the added value of the SWIFT agreement is’. Others were opposed to the idea of transferring the private data of Europeans to the US because of a lack of trust. In the words of German MEP Franz Obermayer (a Non-Attached Member (NA)) ‘high-ranking politicians and criminal experts doubt that, in the US, the data will be used solely for combating terrorist activities’. Similarly Portuguese MEP Rui Tavares (European United Left/Nordic Green Left (GUE/NGL)) stated ‘it is unacceptable to say that this is a provisional report, when the data collected over the next nine months will be in the hands of the US administration within five years, and it might be a Sarah Palin administration rather than the Obama administration’ (European Parliament, 2010a).

On 4 February 2010, the EP’s LIBE Committee debated and accepted a report written by Dutch MEP Janine Hennis-Plasschaert that recommended the rejection of the EU–US agreement on the processing and transfer of financial messaging data from the European Union to the United States for purposes of the TFTP (A7-0013/2010). In this report three issues were highlighted. First, the rapporteur partially reframed what was perceived to be at stake in the professional field by emphasizing that the EU should take up a more active role and become ‘a true counterpart to the US’, ‘working shoulder to shoulder’ (European Parliament, 2010b, p. 7). She argued that with the proposed agreement ‘it cannot be denied that the EU continues to outsource its financial intelligence service to the US’. Therefore, she stated:

the current debate is not about SWIFT as such but about how Europe could cooperate with the US for counter-terrorism purposes and how financial messaging data providers are requested to contribute to this fight, or indeed more generally the law enforcement use of data collected for commercial purposes (ibid., p. 8).

Secondly, she offered a list of legal shortcomings of the proposed agreement. These include, for instance, the continued violation of the proportionality and necessity principles of data
protection laws that cannot be respected by SWIFT due to the structure of its database and the absence of indications on the retention period of the data, the conditions for sharing information with third countries, and the public control and oversight of the authorities’ access to SWIFT data. In short, she concluded that the agreement ‘does not guarantee European citizens and companies the same rights and guarantees under US law as they would enjoy in the territory of the EU’ (p. 9). Thirdly, the rapporteur criticized the Commission and the Council for failing to respect the duty to inform the European Parliament ‘fully and immediately at all stages of the procedure’ and asked these institutions to make all relevant information available for the deliberations in Parliament (p. 10).

On 11 February 2010, the European Parliament voted on the interim agreement that the Council had concluded on 30 November 2009. During the parliamentary debate the previous day and in line with the Hennis-Plasschaert report, MEPs criticized the data protection safeguards adopted in the agreement, which they qualified as ‘unacceptable’ and a ‘flagrant breach of citizens’ rights’. More generally, many MEPs considered the agreement as a ‘bad agreement’ (European Parliament, 2010c). They also condemned the attitude of the Council which, it was widely agreed, ‘did not act properly with the European Parliament’, and had ‘a really amateurish approach’, as well as the American diplomats, who in the words of German MEP Martin Schulz (PES) behaved like Jonathan Swift’s Gulliver and ‘believes that it can treat the European Parliament as if it were an organization of little people’ (European Parliament, 2010c).

In addition, during the plenary debate doubts about the effectiveness of the TFTP were raised again. Swedish MEP Carl Schlyter (Greens/European Free Alliance) called into question the TFTP’s effectiveness in preventing terrorism, stating that ‘no terrorist attack will be stopped by this proposal. None of the four attacks mentioned by the Council Presidency would have been stopped, although perhaps the subsequent investigations would have been made easier’ (ibid.). British MEP Sajjad Karim (European Conservatives and Reformists (ECR)) emphasized that the ‘instances where SWIFT has failed or let us down’ must also be taken into account. He continued,

There have been many failed or bad investigations in the European Union. In my constituency alone, 12 innocent people were detained and were not able to be charged. At the time they were detained, they were informed that financial transactions were part of the substantial evidence against them (ibid.).

Yet, the broadening of the debate did not last long as the concerns of Schlyter and Karim were not actively defended by many other MEPs. It is important to stress that at this stage the opposition of the European Parliament fundamentally differed from its critique just
after the disclosure of the TFTP. While MEPs remained very critical in 2010, ‘nobody in the European Parliament is against the use of SWIFT data in the fight against terrorism’ (interview 11). Although the interim agreement was massively rejected by an EP resolution (378 in favour, 196 against, 31 abstentions), the Parliament requested that the European Commission and the Council work on ‘a long-term agreement with the United States’ (European Parliament, 2010d). A few weeks later, on 24 March, new negotiations for an agreement between the EU and the US were opened (European Commission, 2010).

After the rejection of the agreement, the Commission and the Council demonstrated a new spirit of cooperation. Home Affairs Commissioner Cecilia Malmström commented that “[t]he interim agreement was not perfect, we’ll come up with something better,” and pledged that she would ‘keep the parliament informed from the very beginning and throughout the whole process’ (Pop, 2010b). Subsequently, the Commission immediately informed the European Parliament about their recommendations to the Council to open negotiations with the US that would start on 10 May. Reacting to these recommendations in its resolution of 5 May 2010, the EP indicated the main obstacles to accepting the EU-US agreement. The most important for the EP were its opposition to bulk transfers of data, the need to appoint an independent person to monitor the TFTP, improved access to documents that would demonstrate the necessity of an agreement, and its desire that Europeans have the same rights as Americans in case of abuse of data, including the right to go to court (European Parliament, 2010e). Concerning this last safeguard it is important to stress, however, that the rights obtained would not be very significant. Previous lawsuits in the US against SWIFT and the authorities involved in the TFTP have been unsuccessful and it continues to be problematic for Europeans to prove that their data have been secretly targeted.

In addition to these privacy and data protection-related issues, sovereignty remerged as another important aspect of the TFTP. The EP did not want to ‘free ride’ on the American security programmes, and was opposed to outsourcing Europe’s security policy to the US. This means that the EP was asking for reciprocity with regard to American financial records and the development of a European capability to analyse financial data. It might be called quite surprising that the idea of an EU version of the TFTP had much success with MEPs. If one had suggested such a programme in 2006 this would probably have led to a severe condemnation and massive outcry. However, by 2010 this was seen as a good solution by fractions of the EU institutions. Initially developed by the Council Secretariat and strongly supported by the EU Counter-Terrorism Coordinator, Mr. Gilles de Kerchove, the EU equivalent of the programme was considered as a way to avoid the transfer of data to the US.
authorities and to strengthen the EU’s capabilities with respect to combating terrorism financing. This last argument is somewhat puzzling, taking into account the critique by the same MEPs of the lack of results and effectiveness of the TFTP.

Meanwhile the pressure of the Obama administration continued. On 6 May 2010, Vice-President Joe Biden delivered a speech to the European Parliament in which he tried to convince MEPs about the necessity for the transfer of financial data to US authorities for the purpose of combating terrorism. In what was qualified as ‘sweet talks’ by the European online newspaper *EUObserver* (Pop, 2010c), Biden complimented and supported the work of the European Parliament and the European Union and he insisted that he, his government, and his President ‘are back in the business of listening—listening to our allies’ (Biden, 2010). He also went into great lengths to explain the importance of, and his personal commitment to, the protection of privacy, but added that ‘no less than privacy, physical safety is also an inalienable right’ (*ibid*). Biden emphasized that the ‘Terrorist Finance Tracking Programme is essential to our security as well as yours’ and that ‘as leaders, we share a responsibility to do everything we can within the law to protect the 800 million people we collectively serve’ (*ibid*). From the reactions of the MEPs who had been fiercely opposed to the previous agreement, Biden’s speech succeeded in gaining quite some sympathy. According to Hennis-Plasschaert, for example, “the No-vote was a wake-up call for the Obama administration, they suddenly realised we can block things. They’ve since shown willingness to co-operate” (quoted in Pop, 2010c).

Negotiations between the EU and the US authorities continued and on 28 June 2010 the European Union and the United States signed an EU-US agreement on the processing of financial data for the purposes of the TFTP (Council of the European Union, 2010b). Following an earlier threat that the European Parliament would reject the agreement for a second time (Pop, 2010e), many of the European Parliament’s demands were addressed in the new version of the agreement. The agreement acknowledges, for instance, the demand for an EU equivalent to the TFTP in the EP’s resolution of 5 May, a supervisory role and a right to examine data requests for Europol, and the restriction of search tools to terrorism-related requests only.

However, despite the large majority who voted in favour of this agreement (484 in favour, 109 against and 12 abstentions) on 7 July 2010, MEPs were not entirely satisfied about the content. In fact, they felt that their main objection, the transfer of personal data in bulk from the SWIFT database to the US authorities, remained unresolved in the new text. According to MEP Sophie in ’t Veld, “the US has the capacity to filter, so it can be done. We
need to get the technology and do it here in the EU” (quoted in Pop, 2010e). Nevertheless, many MEPs considered that the new agreement was a “step forward” (quoted in Pop, 2010d) compared to the earlier agreement and stated that “it is better to have an insufficient agreement than no agreement at all” (interview 11).

The European Parliament’s consent to the conclusion of the EU-US agreement marked an end of the ‘SWIFT affair’, and the TFTP restarted on 1 August 2010 for a period of at least five years. During the four-year EU debate two phases can be seen as political, the weeks after the revelation of the TFTP, and the debates and the vote on the EU-US interim agreement of early 2010. In these moments the TFTP was discussed from the perspective of privacy and data protection rights, economic and international relations with the US, its effectiveness, and (but only in phase one) the societal desirability of the programme. On the basis of these issues, the privacy and data protection law became most politicized. Like the debate in the US, framing the TFTP around a legal issue and its technical aspects helped to depoliticize the programme. By developing a legal framework and making the financial data transfers compatible with all technical aspects of European privacy law, the TFTP became normalized. Hence, through the involvement and the incorporation of some recommendations of data protection agencies and the conclusion of international agreements on the programme, the TFTP gained legitimacy. From the entry into force of the EU-US agreement in August 2010, the SWIFT affair can be considered as depoliticized. However, occasional media reports indicate that the SWIFT affair is not to be considered as a completely closed case yet. New controversies, such as the seemingly difficult development of the EU Terrorist Finance Tracking System, the revelation that Europol violated the data protection rules set out in the agreement (Pop, 2011a, 2011b), and the court ruling with respect to the disclosure of secret documents concerning the TFTP (Volkskrant, 2012, in t Veld, 2012) continue to appear in the media and the political debate.
4.5 Conclusion

A comparison of the debates on the SWIFT affair in the US and the EU shows significant differences in duration, topical emphasis, contextualization, and political follow-up. The debate on the TFTP lasted approximately two weeks in the US and four years in the EU. In the US the legality of the programme, its respect for privacy, and media organizations’ decision to disclose the programme became politicized, while in the EU privacy and data protection were considered crucial. Furthermore, in the US the SWIFT programme was placed in the broader context of the NSA eavesdropping scandal while in the EU it was most often considered in relation to the American demand for travel data (PNR records) and illegal secret programmes in the War on Terror. Finally, the conclusions from the public debate on the disclosure of the TFTP were radically different, as in the US the TFTP was considered legal and much less controversial compared to the NSA programme, while in the EU a tough and long transatlantic, intra-European, and inter-institutional battle followed (see table 4.2).

<table>
<thead>
<tr>
<th>Phase</th>
<th>US</th>
<th>EU</th>
</tr>
</thead>
<tbody>
<tr>
<td>0. Depoliticization</td>
<td>September 2001–23 June 2006: from its inception after 9/11 until its disclosure the TFTP is completely depoliticized because it is kept secret from the public.</td>
<td>June–July 2006: the TFTP is debated from the perspective of: privacy rights, data protection laws, legal competence, the possibility of economic espionage, transatlantic relations, the desirability of the programme, and the wider context of the War on Terror.</td>
</tr>
<tr>
<td>2. Politicization</td>
<td>26–29 June 2006: the issues discussed are the legality and privacy aspects of the TFTP on the one hand and the decision to disclose the programme on the other.</td>
<td>January 2007–November 2009: three initiatives are taken to render the TFTP acceptable: SWIFT joins the Safe Harbour Principles, the UST Representations, and an ‘eminent European person’ is appointed to review the TFTP.</td>
</tr>
<tr>
<td>3. Depoliticization</td>
<td>From July 2006: the debate mainly focusses on the media’s decision to disclose the TFTP. Congress supports the TFTP and does not start investigations into the programme.</td>
<td>December 2009–August 2010: critical debates and rejection of the EU-US agreement by the EP. This is followed by new negotiations taking into account the demands of the EP and Biden’s speech before the EP. Eventually, the EP gives its consent to the new agreement entering into force by August.</td>
</tr>
<tr>
<td>4. Re-politicization</td>
<td>--</td>
<td></td>
</tr>
</tbody>
</table>

Table 4.2. Phases of politicization and depoliticization in the SWIFT affair.

However, there are also important similarities in the (de)politicization of the SWIFT affair. On both sides of the Atlantic, the disclosure of the TFTP was followed by a moment of openness during which many questions were raised. These included questions about the
‘political’, calling into question the TFTP and even the assumptions underpinning the War on Terror. Subsequently, certain aspects of the programme became politicized and can be seen as part of ‘politics’. In a third phase attempts were made to depoliticize the programme. In this phase, debates continued as a part of politics, with a shared understanding of the problem developing around questions of administration (what are the legal competencies of institutions and which legal procedures must be followed?) and detailed technical questions (how can privacy safeguards be integrated into the analytical software used by the US authorities? And how can datasets become more targeted?). In this phase the programme was rendered uncontroversial and the focus was on ‘solving’ specific matters. Making this process visible demonstrates that societal and political questions that call into question the political order can emerge in the ‘moment of openness’ and when an issue becomes repoliticized. Only in these instances is there room for ‘the political’.

Comparing the questions of the political raised in the moments of openness in the US and the EU shows another similarity. In both debates two subjects were raised but never became debated. First, the philosophy of the War on Terror that also shaped the TFTP was not part of the SWIFT debates. At the core of this philosophy, like Laplace’s demon, is the desire to see into the future with the help of science and technology to prevent terrorism from happening. More practically this means that the assumptions of the War on Terror were based on the idea that terrorists can be caught before they strike through the analysis of massive sets of personal data by ‘smart software’. This belief in complex risk- and link-based calculations and the timely connection of data dots for detecting terrorists preventively was at the core of the Bush administration’s counter-terrorism policy, and continues to be important today. However, despite the connections that were made between the TFTP and other secret and controversial programmes, and more general remarks about the need for reflection on the War on Terror, the debates in the US and the EU did not deal with the philosophy underpinning the War on Terror.

A second issue that was raised but never discussed thoroughly in the American and European debates on the SWIFT affair was the effectiveness of the TFTP. Despite the hints about the lack of results, potential abuse, and false positives in the first newspaper articles, and the repeated questions from MEPs on the effectiveness and the added value of the programme, the working and the tangible results of combating terrorism through SWIFT data have remained piecemeal or vague. It is important to highlight the absence of these vital elements of the debate on the TFTP as it shows how the ‘political’ was occulted and how the questioning of the political order and the *raison d’être* of the TFTP was avoided.
Analysing the kind of questions that were raised or avoided in the SWIFT debate as well as the shifts that took place during the debate also leads to the question why none of the participants in the field objected to the depoliticization of the affair. While a reduction of the debate to politics and calculable questions might be understandable from the perspective of those in power, it is interesting to see that other participants, such as the entities responsible for monitoring or controlling the authorities, civil liberties groups, national data protection agencies, the parliamentary opposition, and the media, also restricted their contributions to a few specific and technical issues.

From the perspective of governmentality and field theory, two explanations can be found to explain the abandonment of the political. After a first reaction of strong protest, the European Parliament was most interested in solving the issue. In this case it is important to stress that unlike national parliaments the EP is not organised into a governing majority and an opposition. To maximise its influence on European decision-making it is of great importance to find a compromise that is supported by a majority of the MEPs. The Belgian Privacy Commission, and privacy commissions in general, explained that their task was to establish whether privacy or data protection laws had been violated. They did not examine ethical questions (interview 9). Journalists in turn might claim that their job is to report different opinions and facts but not to take an ethical or political position. In other words, it seems as if nobody owns the questions concerning the societal desirability of the TFTP and more broadly the philosophy on which the War on Terror is based. This underscores Judt’s and Žižek’s point that both politics and the political are depoliticized in favour of a bureaucratic technique of governance.

Secondly, the analysis of the debates in the US and the EU shows how a field of governing emerged in relation to the SWIFT affair and which issues were at stake in this field. In both debates a shared understanding of the TFTP emerges. Within two weeks an agreement was reached in the American debate that the programme was a ‘vital tool’, representing ‘government at its best’, providing a ‘unique and powerful window into the operations of terrorist networks’, and saving lives (inter alia, Lichtblau & Risen, 2006). Likewise, despite the lengthy debates in Europe, a consensus that an international agreement with the US had to be concluded to legalize the transfer of European data to the US already existed in September 2006. The central question raised in the European Parliament, and this is very clear in the debates of early 2010, was how to continue the TFTP with respect for European (data protection) law. Both fields can be seen as fields of domination or fields of force in which power was exercised by framing the TFTP as an issue of national security and
around legal arguments. Proponents of the TFTP exercised pressure by highlighting the importance and the necessity of the programme for national security, which was difficult to challenge. Furthermore, the focus on establishing and complying with the law helps to end the debate, as it implies that the societal, and political questions and debates that preceded or destabilized the law can be avoided. In short, the structuring of the field facilitates the depoliticization of the TFTP and the avoidance of questions of the political.

Finally, in the European debate on the SWIFT affair, the European Parliament played a small but important role in generating public attention for the EU-US agreement on the transfer of bank data, and showed its commitment and powers as a defender of European citizens’ fundamental rights. However, the demands and concerns of the European Parliament must be considered as mainly part of politics. They ‘revolve around day-to-day decision making and ideological partisanship’ (Edkins, 1999, p. 2). Despite the attempts of some MEPs, the European Parliament did not succeed in debating adequately the questions of the political raised by the SWIFT affair. The following chapter attempts to re-politicize the SWIFT affair by addressing the questions of the political that were avoided in the debates in the US and the EU. It aims to investigate how the TFTP works opening the black box of SWIFT, and to consider the TFTP from the perspectives of effectiveness and the broader War on Terror philosophy.
Chapter 5.

SWIFT: Opening the “Black Box”

There is no doubt that America and our allies in the war on terror are safer today because of this program.
—TFTP fact sheet, US Department of Treasury, 2010

The Terrorist Finance Tracking Program (TFTP), which is based on the SWIFT network, is a very precious instrument in Europe too. It is of benefit to our member states.
— Gilles de Kerchove, EU Counter-Terrorism Coordinator, 2009

5.1 Introduction

As discussed in the previous chapter, the revelation of the Terrorist Finance Tracking Program led to the politicization of certain aspects of the programme. The political controversies concentrated in particular on the public’s interest to know about the transfer of their financial data versus the need to prevent disclosure of information that supposedly could put lives at risk, and the respect for certain norms and legal principles, most notably data protection and privacy. The precise workings of the TFTP and the alleged successes of the programme have received far less attention in the public debate. Claims of American and European political leaders that the programme is a “very precious instrument” in the fight against terrorism, and that “there is no doubt that it makes America and its allies safer” seem to have been taken for granted or were gradually accepted by most politicians and much of the wider public. In the proposal for a European equivalent of the TFTP, the effectiveness of the programme is even regarded as “proven” (European Commission, 2010). In addition, investigations made by journalists and data protection and privacy agencies raised relatively few questions about the operational aspects and the tangible results of the TFTP. As such, the debates on the TFTP often ignored or only partly examined these questions: How exactly are the SWIFT data analysed? What is the actionable intelligence resulting from the analysis? How valuable is the intelligence retrieved from SWIFT? Where is the evidence that it makes “us” safer? What is the value of financial data in security practice?

In this chapter the operational aspects of the TFTP are analysed. In fact, it is of key importance to study the processes, procedures and also the analytical software that shape the
TFTP in detail since they are a critical part of the way in which the field of governing works. Rather than being mere technicalities of the SWIFT programme, the operational aspects represent an account of power reflecting political choices, negotiations, and practical considerations. Investigating which data are transferred to the US authorities and how these data are analysed helps in bringing back the political into the depoliticized workings of the TFTP.

For the purpose of this analysis, I use the analogy of the black box as described by Donald MacKenzie. He states that ‘black boxes are devices, practices, or organizations that are opaque to outsiders because their contents are regarded as “technical”’ (2005, p. 555). In a literal sense the TFTP is a black box with regard to its analytical software and datasets. In fact, the dataset transferred from SWIFT’s American database to the US Treasury was actually called ‘the black box’. It is an appropriate name as neither SWIFT nor the US Treasury would be able to tell how many records and whose data are contained in the black box. Hence, its content is unknown to outsiders and even to insiders. The TFTP is also metaphorically a black box because the practices and expertise involved in the daily workings of the programme and the way in which the programme produces actionable data remain invisible to a wider public.

Instead of disregarding the internal structure of the black box, MacKenzie argues that it is important to open the black boxes of finance. Examining black boxes shows how they structure their contexts and how the contexts of black boxes shape their contents (2005, p. 558). Opening the black box of the TFTP thus helps develop an understanding of how the intelligence from the programme affects individuals or society and also how political preferences and assumptions influence the workings of the programme. Moreover, it becomes possible to name and discuss an arcane world of scientific devices and the (perhaps unintended) implications for society of the use of these technological solutions of the War on Terror.

As far as possible within the limitations of the continuing secrecy surrounding the TFTP, the opening of the black box reveals how the SWIFT data were used. It makes the context and the content of the programme more visible by ‘reassembling’ (Latour, 2005) the processes, procedures, and analytical software tools of the TFTP. This means tracing the connections between the participants or things that are involved in the programme and showing what kind of power relations and security decisions this produces. Finally, the opening of the black box brings back the prominence of certain ethical, political, and societal questions. Are, for instance, some individuals or groups more exposed to inclusion in the
black box and in the data selected for analysis? What do established links between individuals on terrorist network maps mean? What are the implications for individuals that appear on these maps? How is the line drawn to determine which financial transactions are considered ‘risky’ and whose data are suspicious? What are the consequences of ‘outsourcing’ European security decisions on the basis of (commercial) financial data to the US authorities? How proportional is the collection of massive sets of financial data in the fight against terrorism finance?

What it means to ‘open the black box’, and more generally how technology can be taken into account as an actant in the War on Terrorism financing, will be discussed in the section ‘opening the black box’. Subsequently, the TFTP will be discussed, with a focus on the technicalities and the questions that these may raise, in four steps: first, the transfer of information from SWIFT to the US Treasury; secondly, the inclusion of safeguards to the programme; thirdly, the analysis of data by the CIA; and finally, the announced results of the TFTP. To conclude, this reading of the TFTP is discussed in the light of the expected European equivalent of the TFTP, the so-called Terrorism Finance Tracking System (TFTS). However, in the next section I first analyse why the black box has not been opened yet.

5.2 We Cannot Know, We Should Not Know, We Do Not Want to Know

The continued obscurity of the operational aspects of the Terrorism Finance Tracking Programme can be explained by three partly intertwined arguments. An apparently compelling reason why the public lacks in-depth knowledge about the working of the TFTP is the fact that it is a top-secret programme considered of key importance to the national security of the US. This implies that only a very restricted number of persons was informed about the programme even within the organisations directly involved and that they were held to strict confidentiality. As discussed in the previous chapter, the secrecy and disclosure of the programme was one of the highly politicized topics emerging from the SWIFT affair. In short, the Bush administration argued that the TFTP should have remained secret in order to protect Americans and combat terrorists efficiently while other observers said that it was not a secret that the US authorities tracked the financial trails of alleged terrorists and that the administration sometimes invited the press, hoping that they would draw attention to its relentless efforts in the war on terrorist financing (Bacquet & Keller, 2006). Yet, this debate largely overshadowed questions about who knew and who could or should have known about it. In other words, how secret was the programme really and how was this secrecy justified?
Newspaper articles reporting on the SWIFT affair indicate that many actors that should have been informed about the programme according to democratic, legal, or diplomatic norms were not. Virtually all of the 7800 banks submitting their clients’ data to the SWIFT system were unaware of the potential communication of this confidential information to the US Treasury. Moreover, only a few selected members of US Congressional and Senate committees on security and intelligence were informed about the TFTP in 2002 and some others were informed in spring 2006 when the *New York Times* indicated that it would publish the story (Lichtblau, 2009, p. 254). Relevant representatives such as the Chairwoman of the House Banking Subcommittee, Sue Kelly, the Chairman of the Senate Judiciary Committee, Arlen Specter, and a member of the House Financial Services Subcommittee in charge of international monetary policy and technology complained in various newspapers that they had not been informed about the programme (see, *inter alia*, Stolberg & Lichtblau, 2006, DeYoung, 2006).

In Europe most governments were unaware of the TFTP. The UK Home Office declared that it had been directly informed by the US government (Guha, 2006). The German Ministry of Finance became aware of the programme one day before the story was published in the media via an e-mail from Stuart Levey (Atkins et al., 2006). The Belgian and Dutch governments declared they were neither informed by the US nor by their national central banks. Equally, the European Parliament, national parliaments, and data protection agencies were completely ignorant about the transfer of SWIFT data to the US authorities. Hence, before the disclosure of the TFTP many relevant actors were indeed unaware of the programme. Even if they had wanted to, they could not open the metaphorical black box of the TFTP since they were not even aware that it existed.

Nevertheless, if one establishes a list of those people who were informed, one must admit that dozens of people spread over at least seventeen countries were aware of the programme. Within SWIFT, the highest echelons such as the CEO, Leonard Schrank, and some of the 25 members of the Board of Directors, constituted of top bankers of the biggest international banks, were informed about the transfer of data from their database to the US authorities (interview 13). On the receiving side, the US Treasury Office for Foreign Assets Control (OFAC) and the data analysts and data consumers at the CIA and the FBI were involved in the TFTP, while the National Security Agency (NSA) provided technical assistance. Information about SWIFT was of course also available for those politically responsible for the programme at that time, including President G. W. Bush, Vice-President Dick Cheney, National Security Advisor Condoleezza Rice, Treasury Secretary John Snow,
and their most senior advisors (among them Stuart Levey, a senior counter-terrorism official for the Department of Justice until 2004, and between July 2004 and March 2011 the Under-Secretary for Terrorism and Financial Intelligence at the US Treasury). Furthermore, as mentioned above, some members of the US Congress and Senate were briefed about the programme. In addition to the US authorities, the Central Banks belonging to the G10 and the members of the Oversight Group that monitors SWIFT’s activities were informed about the programme by the Federal Reserve Board (the US central bank) in 2002. Some of these central banks informed parts of their governments. In the Netherlands, for instance, the Dutch Central Bank informed the Minister of Finance, who in turn briefed the Dutch Ministries of Justice and of the Interior (Ministerie van Financiën, 2007, p. 6). Interestingly, most of those informed apparently valued the respect for secrecy about the American programme over democratic oversight, and chose not to inform their governments and data protection agencies.

When, four years after its initiation, the strict confidentiality surrounding the programme was broken, this did not lead to opening the metaphorical, or the literal, black box of data collection and analysis. As highlighted in chapter 4, members of the European Parliament have often complained about the continuing secrecy surrounding the programme. They stated that that they could not make a good judgement since the Council withheld information about procedures and the effectiveness of the SWIFT programme and refused them sufficient access to relevant documents. Moreover, the findings of the Bruguière report, meant to enhance democratic oversight on the TFTP, remained officially confidential, and instead of opening the black box, they only examined procedural safeguards (interview 6).

The operational and technical aspects of the TFTP are also little known because national data protection agencies, as well as the European Data Protection Supervisor, have limited competencies to examine these questions. They do not have the power to investigate a case and hear people beyond the territory for which they are competent. For this reason, even the Belgian Privacy Commission, which had taken the lead in investigating the transfer of SWIFT data, was not able to monitor the data transfers and analysis in the US (interview 9). Moreover, the revelations and explanations made in their reports depend fully on the willingness of the parties involved to participate in hearings and to voluntarily submit information, and on publicly available information. Furthermore, data protection agencies that investigated the SWIFT case primarily took a purely legalistic approach in line with their official competency. An officer from a national privacy commission described it as follows. ‘We look at two matters, privacy laws and data protection laws and we check [the SWIFT case] on the basis of principles in these laws’ (interview 9). More generally, the investigation
of the SWIFT case by national data protection agencies in Europe consisted of contrasting the information they received about the SWIFT case with national laws implementing Directive 95/46/EC concerning the protection of personal data. Although it is certainly important to establish whether privacy and data protection laws have been violated, this is a limited interpretation of responsibilities. It implies that the technical modalities—for instance, whether it is a push or a pull system, or the duration of the data storage—of the TFTP are considered relevant from a privacy or data protection perspective but there is no need fully to understand the programme and analyse it with regard to broader ethical or societal implications.

In addition to the arguments explaining why we still cannot know the technical and operational aspects of the TFTP, the black box also remains closed because according to some we should not know. After the story broke, the editors of the New York Times and the Los Angeles Times explained in a joint contribution that it involved a conscious choice not to ‘dwell on the operational or technical aspects of the program, but on its sweep, the questions about its legal basis and the issues of oversight’ (Bacquet & Keller, 2006). According to the editors, the technical details of the programme were not suitable for publication as they could potentially harm national security and were not essential for American readers. However, in their attempt to combine the duty of the free press to inform their readers about government action in the War on Terror with the ethical value of not divulging potentially sensitive information, they willingly restricted the ‘right to know’ to only those facts they believed were essential, and they consciously framed the story around more acceptable debates.

Finally, some argue that inquiring about the practices of the TFTP in detail is irrelevant as long as it ‘works’ and generates useful leads and security action. From this perspective, the operational part of the programme becomes regarded as mere ‘technicalities’, a black box of which the content may remain opaque. As an official from the European Commission has put it with respect to DNA, ‘it’s like a TV, you don’t need to know how it is built; you just want to watch your favourite shows’ (CEPS, 2008). From this point of view, there is no need for questioning the political dimensions to science and technology, being only the output, and the watching of the show is relevant. This view seems to be even stronger with respect to risk management and risk criteria. Not only do few people know how risk calculations work, but according to officials from the European Commission, ‘we shouldn’t know [how it works]’, ‘because once you actually make these criteria transparent you deem them useless’ (interview 8). The assumption on which the use of risk analysis for security purposes is based is that terrorists and other criminals show different behaviour compared to
normal citizens. Opening the black box by revealing the criteria of the risk analysis would help them to hide by adopting less suspicious travel or banking habits.

These reasons for public ignorance about the operational and technical workings of the TFTP can be summarized as: we cannot know, we should not know, or we do not want to know. Although these may seem (and are to a certain extent) legitimate reasons, they do also tell us something about, and have an impact on, society. They draw an image in which the decision to disclose or withhold information about the programme becomes unconnected to any laws or conventions. Within the US this introduces a hierarchy between certain selected privileged US representatives who were briefed about the programme and others, sometimes belonging to the same Congressional committees, who knew nothing. From an international perspective it reshaped and dispersed sovereignty, not only affecting the relation between public and private authorities (De Goede, 2008, p. 100) but equally altering the relations among public authorities. Until the TFTP became public, most EU governments remained uninformed about the cooperation between a Belgian company and the US government while certain major central banks in these same countries, apparently feeling no urge to inform their government and possessing no competency or willingness to assess the implications of the TFTP for their citizens, became the preferred interlocutors of the US government. Moreover, some participants in the field seemed to prefer not to examine the consequences of the TFTP for citizens and society. Journalists consciously avoid certain axes of research in order not to touch upon questions considered too sensitive. In sum, there seems to be no public authority that was authorized or claimed the power to assess properly what happened with the SWIFT data.

5.3 Opening the Black Box

A number of academics, most notably Bruno Latour through his actor-network theory (ANT), have highlighted how certain objects influence human behaviour and interaction by the role they are assigned or the way in which they are used. Latour asserts that human behaviour is affected by objects in the sense that they ‘might authorize, allow, afford, encourage, permit, suggest, influence, block, render possible, forbid and so on’ (Latour, 2005, p. 72). He illustrates this by explaining how the invention of the TV remote control made it possible to become a couch potato in front of the TV, surfing from channel to channel (2005, p. 77). In this chapter, the equivalent of Latour’s remote control consists of the datasets SWIFT transferred to the US Treasury, the so-called ‘black box’, and the analytical software
that produces the suspected terrorist networks. It is important to examine these objects as participants in the context of the TFTP because their design and functioning shape the possible outcomes of the programme. For example, the design of the search options included in the software renders possible and authorizes certain results while others are blocked or technically impossible. Likewise, the kind of transactions and data fields included in the datasets of SWIFT allows for certain forms of analysis and outcomes differing for instance from national financial transaction services.

In addition to making objects part of the analysis, opening the black box entails highlighting the assumptions and political choices that structure the object of investigation. In his article, MacKenzie (2005) opens two black boxes in the world of global finance: option pricing theory and arbitrage. He recommends the (further) opening of two other black boxes, which are ‘ethnoaccounting’ and regulation. He explains that in order to price options the Black, Scholes and Merton equation is commonly used. This theoretical model is derived from the heat or diffusion equation used in physics. It is based on a number of assumptions partly for mathematical convenience but it also reflects powerful theoretical beliefs of how markets work and how they should work. When the use of the model became more widespread, it transformed the market by providing legitimacy to certain financial practices and it implicitly imposed ideas of an ideal market (pp. 559-562).

The second case discussed by MacKenzie is the use of arbitrage to exploit price discrepancies. Arbitragers are supposed to contribute to efficient markets and separate economic matters from ‘irrational’ sociological and psychological logics. Opening this black box, MacKenzie demonstrates how investment banks and hedge funds actually operate very much on the basis of sociological and psychological behaviour, for instance copying arbitrage strategies of their successful competitors. This in turn undermines a number of the assumptions on which arbitrage is based, for instance that it does not require capital, that it involves no risk, and that the capacity to close price discrepancies is unlimited (2005, pp. 562-565). Both cases show that political, social, and psychological decisions are present in what are believed to be purely technical economic tools.

With respect to the TFTP, the consideration of objects as actants as proposed by Latour and MacKenzie helps us to understand how datasets and technology have contributed to shaping the field of governing and the outcomes of the TFTP. It draws attention to the fact that the availability of SWIFT data for security purposes led to new methods for investigation and intelligence-gathering, which in turn led to new ways of exercising power. This point is also brought forward by a former senior counter-terrorism official who stated, ‘the capability
here [of the TFTP] is awesome or, depending where you’re sitting, troubling’ (Lichtblau & Risen, 2006). The introduction of the TFTP silently allowed radical changes regarding a number of democratic principles and judicial safeguards. These changes and their implications can be made visible by focussing on the ‘details’, or the ‘small’ to understand how it structures the ‘big’ (MacKenzie, 2005, p. 558). It implies examining the TFTP by reassembling the social and technological processes, procedures, and practices, bringing back the context and content to this ‘black box’. In the next sections, I attempt to provide this context and content to the technicalities of the TFTP, starting with the transfer of data from the SWIFT database to the US Treasury.

5.3.1 Obtaining ‘the Rosetta Stone for Financial Data’

The particular interest of intelligence and law-enforcement agencies in the data held by SWIFT did not arise after the 9/11 attacks. Already in the early 1990s, under the administration of George Bush senior, the US government tried to obtain information from SWIFT via traditional subpoenas issued by the OFAC. However, these were not complied with either because the data was older than 124 days and already erased from the system, or because SWIFT convinced The Treasury that the data could be obtained more easily through the sending or receiving bank, or because the demand implied a name search, which is impossible in the SWIFT system (Belgian Privacy Commission, 2006a, p. 5). Throughout the 1990s, pressure was put on the company by the US Justice Department to include more elements of financial data in their messaging system and to make deciphering of SWIFT’s encrypted data easier. The Justice Department also asked for access to broader sets of information to support criminal investigations. The purposes for which SWIFT data were intended to be used, at that time, included uncovering money-laundering schemes, mapping international money flows of Colombian drug cartels, and more generally combating organised crime (Lichtblau, 2009, p. 242). In those years, but also just after 9/11, the CIA even considered secretly entering the SWIFTNet FIN service (Lichtblau, 2009, p. 243).

After the 9/11 attacks, SWIFT’s attitude towards cooperation quickly changed. Prior to the attacks SWIFT presented itself as a loyal partner towards law-enforcement agencies and it responded to their requests for information. However, at that time the cooperative as well as certain government officials had serious reservations about secretly becoming a partner of the U.S. government. Reminded of SWIFT’s database being ‘the mother lode’, ‘the Rosetta stone for financial data’ by a Wall Street executive (Lichtblau & Risen, 2006), the Bush
administration decided to approach SWIFT again. This time, SWIFT’s American CEO Leonard Schrank, who felt very much affected by the 9/11 attacks, was keen to cooperate.

However, the design of SWIFT’s messenger service SWIFTNet FIN is such that it could not directly deliver the data elements requested by the CIA (Belgian Privacy Commission, 2006a, p. 5, 10). The messages transferred through the system consist of an ‘envelope’ containing information on the sender (for instance Barclays Bank), its BIC (Bank Identifier Code), the identification of the receiving bank, and the date and time of the message. The actual message or ‘the letter’ is encrypted and contains information that is entered via standardised fields by the sending institution. The system proposes standardised forms for nine different types of transfers among which a bank’s customer payment is one. These standardised forms contain at least the following information: the amount of the transaction, the currency, the value, the date, the beneficiary’s name, the beneficiary’s financial institution’s details on the customer requesting the financial transaction, and the financial institution of the customer requesting the transaction. Additional information such as reference numbers for payments and ‘unstructured text’ can also be added to payment-related messages (ibid., p. 4). Since the SWIFT messenger service only passes along the millions of encrypted envelopes, its software does not have a research tool in its operating centre for queries concerning names or other personal data. Thus, because SWIFT itself was unable to search its database for names of terrorist suspects, the company proposed to hand over the datasets from the SWIFTNet FIN service to the OFAC (Lichtblau, 2009, p. 244).

The transfer of SWIFT’s financial data to the US Treasury started within two weeks after 9/11. Due to the architecture of SWIFT’s data centres when the TFTP was initiated in 2001, this data transfer could take place entirely on American soil. At that time, SWIFT operated one database at the site of its Belgian headquarters near Brussels and another mirror database was held on American territory, in Langley, Virginia. To make matching with the CIA lists of suspected terrorist financiers and operatives and the SWIFT data possible, datasets from SWIFT’s mirror database were compressed in a so-called “black box” and made available to the US Treasury. In turn, the US Treasury designed search software to decrypt and consult the messages in the black box on the basis of specific searches by name.

Several accounts exist with regard to the amounts of data made available by the American operation centre. US Treasury Under-Secretary Snow is quoted as saying that SWIFT initially proposed that it would give all its data to the US (Lichtblau, 2009, p. 244), while according to statements made by SWIFT, the data transfers were limited and the US Treasury and the CIA were never given a full copy of the SWIFTNet Fin database (SWIFT,
It is also unknown how many messages the black box contained exactly. The Belgian Privacy Commission deduced from its investigations that the ‘number of subpoenaed messages must be enormously high’, given the daily message traffic via SWIFTNet FIN of approximately 6.9 million messages per day in 2005 and 11 million messages per day in 2006 (Belgian Privacy Commission, 2006a, pp. 5-6).

From October 2001, monthly administrative subpoenas were issued by the US Treasury to SWIFT’s American operation centre in order to obtain the black box and give SWIFT an element of proof that it had no choice but to cooperate with the US authorities. Between autumn 2001 and June 2006 SWIFT received a total number of 64 subpoenas from the US Treasury (Belgian Privacy Commission, 2006a, p. 5). The subpoenas specified the datasets that had to be included in the black box. For instance, they might cover all transactions within and outside the US to certain countries and jurisdictions, on a specific date or in a specific period of time, usually one month. The CIA analysts selected more than thirty countries involved in terrorism financing, including, not surprisingly, Saudi Arabia, Pakistan, and the United Arab Emirates (Lichtblau, 2009, p. 244). The use of these administrative subpoenas, also known as National Security Letters, was controversial because of their extraordinary scope and their administrative character. Contrary to court-approved warrants for instance, they were administrative subpoenas that took the form of a letter with only limited judicial review. This new governing practice made it possible for the CIA to investigate millions of financial transactions without opening an official criminal investigation and without the interference of the judicial system to test the probable cause standard typically required in criminal subpoenas. It would have been possible, and according to the Belgian Privacy Commission desirable, to challenge the subpoenas, as SWIFT had done before 9/11, but this time they chose not to.

Despite the compulsory character of the subpoenas, this silent and close cooperation between the US government and SWIFT was not without risks. Although the secret selection of data from SWIFT’s messaging system and the transfer to the US Treasury did not alter the money flows or the workings of the financial sector, revealing this cooperation with the US authorities was potentially very damaging for SWIFT. The aim of SWIFT’s services is to provide a highly secure and confidential money transfer service to the financial sector. Cooperation with the US harmed the image of confidentiality of the service since the envelopes were opened by the CIA. It would also potentially damage the trust in the level of security of the provided service by transferring customers’ data without notice. Attempting to reduce the risks to its reputation, SWIFT negotiated what it called ‘unique and unprecedented
protections from the US Treasury’ (SWIFT, 2007, p. 18; see also Belgian Privacy Commission, 2006a, 2008a, Lichtblau, 2009, SWIFT, 2006a, 2006b).

5.3.2 Safeguards Saving the TFTP

When it became clear that the programme would not be a temporary tool to search for hits between the 9/11 hijackers and the data in SWIFT’s black box, but a long-term arrangement in the War on Terror, SWIFT started demanding extra safeguards to be built into the programme. In addition to those that SWIFT had gradually obtained—limiting access to only the black box instead of the entire SWIFT system, the issuance of monthly compulsory administrative subpoenas, permission only for searches connected to terrorism investigations, and measures restricting the possibility to search freely into the transferred data—SWIFT negotiated more safeguards and tougher limitations on the use of their financial records.

Although in later stages of the debate it was argued that the searches within the TFTP have always been strictly limited to terrorism suspects, and to small percentages of the total amount of data contained in the black box, different statements were made just after the *New York Times* published the story. Some government officials are quoted as saying that ‘the programme is limited to tracing transactions of people suspected of having ties to Al Qaeda’. Others said ‘the government sought the data only for terrorism investigations and prohibited its use for tax fraud, drug trafficking or other inquiries’ (Lichtblau & Risen, 2006). Yet, Stuart Levey states that ‘when information appeared that indicated a non-terrorist crime, such as money-laundering or drug trafficking the source of the information was “sanitized” before it was passed to other law-enforcement agencies’ (DeYoung, 2006). This suggests that at least at some stage information from the TFTP produced leads unconnected to terrorism and that these were shared with agencies beyond the CIA.

On the demand of SWIFT, the access and scope of the searches were restricted by asking for more information to justify the requests for financial records in the black box. Investigators were only allowed to search financial data on the basis of targeted investigation files concerning alleged terrorist activities (Belgian Privacy Commission, 2006a, p. 7, SWIFT, 2006c). This means that the data that are searched in the black box, for instance names of individuals and companies, must appear in documents, intercepted communications and other evidence gathered by intelligence agencies around the world. ‘The programme works for names already in the intelligence system, collected elsewhere and identified as being part of an open investigation’ (Lichtblau & Risen, 2006) Although this new requirement supposedly restricted the searches in the SWIFT system, the Belgian Privacy Commission
stated that the ‘the US Treasury departs from a broad definition of “terrorism”’ which applies to the 9/11 attacks and to ‘global terrorist cells that pose a threat’ to the US but also to any terrorist act committed anywhere in the world (2006a, p. 5).

In addition, two SWIFT employees referred to as ‘the scrutineers’ or ‘scrutinizers’ received a security clearance to monitor the extraction of data from the black box and to verify if the searches in the system were according to the rules. Initially they verified the legitimacy of the requests to the system in real-time, first via statistical sampling and later through a complete verification of the requests. The scrutinizers had permanent access to the black box and, if needed, they could block search orders at any time (Belgian Privacy Commission, 2006a, p. 7). It is unknown whether searches have ever been blocked. Moreover we may question whether two scrutinizers are sufficient to oversee the programme and what their impact is if they only report to SWIFT’s management in relation to the compliance with the extraction principles but not on the details of specific extractions.27

Furthermore, SWIFT insisted on enhanced audit procedures by an external firm to supplement the internal audit procedures. From mid-2002 an outside defence and intelligence consulting firm, Booz Allen Hamilton, Inc., was hired to monitor the TFTP to make sure that the data transferred by SWIFT could not be abused by the US government (Belgian Privacy Commission, 2006a, p. 7). In practice it meant that this firm reviewed the search records to verify if the searches made by CIA analyst were based on a legitimate reason to believe that the transaction might be connected to terrorism (ACLU & PI, 2006, p. 1, Lichtblau, 2009, p. 245). Furthermore, Booz Allen Hamilton did audits of the system designed by the US Treasury to provide SWIFT with an additional assurance that the system was secure and they verified that the scrutinizers had access to everything the analysts were inquiring about (Belgian Privacy Commission, 2006a, p. 7).

However, it remains unclear what the exact role of this consulting firm was. For instance, Lichtblau says that it did occasional checks into the system (2009, p. 245) while the Belgian Privacy Commission speaks of continuous monitoring (2006a, p. 7). Moreover, the ACLU and Privacy International (PI) issued a very critical report for the EU’s Article 29 Working Party, stating that the auditing firm Booz Allen Hamilton was not an independent or objective outsider to check on the TFTP. They argued that the company has a very close relationship with the US government and in particular the Pentagon and the intelligence services. This is illustrated by the fact that many staff members of Booz Allen Hamilton used to work for the military and intelligence agencies. Among the vice-presidents of the company are former directors and top-level officers of the National Security Agency (NSA), the CIA,
the FBI, and the Department of Defence. Furthermore, the consulting company has many contracts with the US government of which a majority, worth 932 million dollars, are related to defence IT. More important is the fact that the company is not known for being very critical. They describe themselves as committed to the client’s mission and success and they received a special recognition from the Department of Defence for the good relations, the ‘cooperative partnership’, between the Department and Booz Allen Hamilton. In addition, the company was involved in and actively supported some of the George W. Bush administration’s most controversial surveillance programmes such as the Total Information Awareness programme, and a law that allowed government eavesdropping via telecommunication companies (ACLU & PI, 2006).

This section shows that private companies play an important role in shaping the governing practices of the War on Terror. SWIFT facilitated the development of the TFTP by granting access to vast troves of personal data. By negotiating additional safeguards for the TFTP in order to protect itself against reputational damage, it was not the law or the European Parliament but SWIFT that imposed the limits of the programme. In the role of external auditors, Booz Allen Hamilton authorized and legitimized the new security practices through (secret) audit procedures and reports. Meanwhile, these private companies were not subjected to principles of transparency and accountability. While they contribute to security decisions that are being taken and which have real consequences for those who are targeted through the TFTP, these private companies have no obligations to parliaments and the wider public to reveal and justify what they do.

5.3.3 Analysing Six Degrees of Separation . . .

One of the most intriguing questions concerns the actual analysis and intelligence production. Although the precise working of the TFTP remains classified, it is possible to reconstruct broadly the way in which the CIA analyses the SWIFT data, the literal black box. According to declarations of US government officials, among them Stuart Levey, the data retrieved from the SWIFT database were used for link analysis or social network analysis (see, inter alia, Miller & Meyer, 2006). Link analysis uses large collections of data to find links between a subject—a suspect, an address, or other piece of relevant information—and other people, places, or things (DeRosa, 2004, p. iv). In the case of the SWIFT data, the connections with terrorism investigations may be established on the basis of real names, addresses, phone numbers, and bank accounts. The data of interest are usually presented in the form of nodes in a network connected by links (see Figure 5.1). By combining and linking
the pieces of data with other sources, layers can be added to improve the understanding of the behaviour that the data represent (US Department of Treasury, 2006, p. 10). Subsequently characteristics of the nodes and connections between them, can be analysed, for instance, the centrality of a person or entity, its closeness to others and the thickness of the connections between the nodes.

Figure 5.1 An example of a social network analysis of the 9/11 hijackers. Source: Valdis Krebs, 2001.

The first investigations of the TFTP departed from the names of the 9/11 hijackers in search for unknown connections with still hidden terrorists. Subsequently these searches were extended to larger numbers of suspected terrorists and their financiers. This implies that the analysts were looking for matches between the various terrorist lists or tips from intelligence reports and the data held in the black box delivered by SWIFT. Presumably these lists included the official UN and US lists of suspected terrorists established by UNSC resolutions 1267 and 1773. On these lists Al Qaeda-related individuals and entities are mentioned but so are other suspected terrorists and terrorist organisations.
However, at least in theory, there should be no or very few hits between the official terrorist lists and the names in the SWIFT database since it is legally forbidden to make a bank transfer or provide any other financial service to people and entities on these official lists and assets of these people should be frozen. Therefore, it is very probable that broader watch lists have been flushed through the system. Like other intelligence services, the CIA has access to the Terrorist Identities Datamart Environment (TIDE) containing data on known or suspected international terrorists. According to the American Civil Liberties Union (ACLU), this watch list of terrorism suspects had over a million records corresponding to approximately 400,000 people in 2008 (Reuters UK, 2008) and it is continuously expanding.\textsuperscript{28} The TIDE records also include separate entries with aliases, (fake) passport numbers and (fake) birth dates. The vast majority of the listed persons (95\%) are not U.S. citizen or residents (\textit{The Washington Post}, 2007).\textsuperscript{29} Furthermore, ‘it is also widely assumed by people in the US that all charities that have been publicly linked by the US as having possible terrorist ties, for instance the Holy Land Foundation, Al Haramain, and the Global Relief Foundation, are subject to the subpoena, and we know for fact that some of them are’ (interview 13).

In the first five years of the programme tens of thousands, maybe hundreds of thousands of financial transactions have been examined (DeYoung, 2006). When a hit occurs between the data held on the watch lists or in intelligence documents and the SWIFT data, analysts try to map all those from whom the person received money and to whom he or she sent money. This might for instance be a wire transfer. Although the details on the methods used to produce intelligence from SWIFT data remain secret, it is known that the FBI conducts link analyses up to three or four links removed from the initial suspect, and that the CIA even goes up to five or six links (interview 13).

From these findings it can be deduced that the SWIFT data have been used for at least two different purposes. Firstly, it has helped to gather or verify practical information about terrorist suspects and their potential financiers in the context of ongoing terrorism investigations. For instance, the data that pass through the SWIFT system indicate when and where a wire transfer has been made, which allows locating the person at a certain moment in time. Through the data held in the black box it is also possible to search for a link between a certain bank account number and one or several names that may provide information about the identities of the sender or the receiver. Furthermore, SWIFT information may reveal something about the activities of the suspect through the amounts of money concerned and the senders and receivers. Again, according to Levey, ‘the way SWIFT data works, you would
have all kinds of concrete information—addresses, phone numbers, real names, account numbers, a lot of stuff we can really work with, the kind of actionable information that government officials can really follow up on’ (quoted in Gellman et al., 2006).

Second, SWIFT data has ‘clearly’ been used for ‘a modest version of data mining’, establishing the degree of connection between different transactions, i.e., link analysis (interview 13). This form of analysis ‘is perceived to be an imaginative and innovative risk technique in the War on Terror that enables the pre-emptive identification and disruption of potential suspects’ (De Goede, 2008, pp. 105-106). SWIFT data allows one to ‘connect the dots’ between banking transfers worldwide and make the social network of a ‘suspicious’ person visible. It can produce investigative leads to other suspected terrorists and potential terrorism financiers before a terrorist act takes place. As such, TFTP is supposed to enhance American and third countries’ ability to identify financiers of terrorism at an early stage, and to help map terrorist networks by creating a window into their operations.

Government officials have always insisted that the SWIFT information has never been used for data mining and have stated that ‘we are not turning on a vacuum cleaner and sucking in all the information we can’ (Lichtblau & Risen, 2006). To clarify this statement, it is important to emphasize that data mining can be defined as the discovery of useful, previously unknown knowledge by analysing large and complex data sets through the use of algorithms that search for predictive patterns (De Rosa, 2004, p. 3). However, link analysis is not considered data mining as it is not based on predictive algorithms but on subject-based queries, as in the case of the TFTP, or pattern-based queries. In case of the latter, the patterns may be obtained through data mining (DeRosa, 2004, p. 4).

There are, however multiple understandings of data mining and there are important similarities between link analysis and data mining. It is important to stress that like data mining, link analysis may also involve enormous amounts of data. First, the black box retrieved from the SWIFT database contains millions of data items. Secondly, the lists with terrorism suspects contain thousands of names. Thirdly, the searches of up to six links separated from the initial suspect are exponential in character, leading to overwhelming volumes of data. This aspect is crucial for understanding some of the problematic aspects of this method. (Automated) link analysis is justified and deemed acceptable because it is believed to be extremely targeted—the CIA is not searching through the whole database, but does specific searches on the basis of a name from the watch list. Yet, departing from one name, the software searches transactions to or from other persons contained in the black box. Subsequently these persons are linked to all those persons from or to whom they receive and
send money, and so on. This implies that the investigations do not cover the only 400,000 suspected terrorists, but a potentially much greater number of persons.

Moreover, although in the context of the TFTP the link analysis departs from one subject, this method is in the end not targeted. By tracing links between one name and all those people to whom money transfers are made, many false positives occur as the suspected terrorist will not make only terrorism-related expenses. Especially when networks are mapped up to six links from the initial subject, it can be assumed that a lot of people become part of the network analysis and most have nothing to do with the initial subject. In intelligence and law-enforcement circles these are sometimes called ‘Pizza Hut leads’, referring to investigations that look at ‘someone who has called someone, who called the pizza delivery guy, who in turn doesn’t know [the initial terrorist suspect] but only came to deliver a pizza’ (interview 13). Hence, as with data mining and risk analysis, great amounts of data on individuals who are completely unconnected to terrorism are included in a link analysis. Furthermore, it might be added that the reality of the searches into the black box might have been messier than appears in the description above. According to one official, ‘this was creative stuff, nothing was clear cut, because we had never gone after information this way before’ (Lichtblau & Risen, 2006).

Finally, if perhaps the TFTP is not a matter of switching on the vacuum cleaner, sucking in and analysing all the information out of SWIFT’s black box, it is also unlike the sharp harpoon Levey referred to (see chapter 4), targeting and eliminating one specific prey. Once an individual is targeted it rather works as a cluster bomb, designed for targets not precisely identified and indiscriminately hitting anyone surrounding the initial target up to four or six links removed. Hence, like cluster bombs, link analyses or social network analyses have a wide area of effect through which they may ‘hit the target’ and be able to reveal financial relations between terrorists, but they also produce a lot of ‘collateral damage’ in the form of false positives and useless links. Moreover, defining whether the connection between the dots is actionable, and constitutes a hit, depends on the ability of financial investigators to (re)construct or imagine a posteriori the context and relevance of a financial transfer (Wesseling et al., 2012).
5.4 Results and “Successes”

It is fascinating that there has been little publicity about the “success stories” of a programme that ran 24/7 and is continually described as a vital tool with ‘tremendous possibilities’ (Meyer & Miller, 2006). The press articles revealing the SWIFT affair in June 2006 mentioned only one high-profile case in which SWIFT data has played a role. This was the case of Riduan Isamuddin, alias Hambali, the Indonesian leader of Jemaah Islamiyah (JI), a terrorist organisation linked to Al Qaeda, and alleged to be the mastermind of the 2002 bombing of a Bali nightclub and of the 2003 attacks on the Jakarta Marriott hotel. According to the New York Times, ‘the SWIFT data identified a previously unknown figure in Southeast Asia who had financial dealings with a person suspected of being a member of Al Qaeda; that link helped locate Hambali in Thailand in 2003’ (Lichtblau & Risen, 2006). In this country Hambali was arrested by the CIA and subsequently brought to a secret prison (Human Rights Watch, 2004). Later that year he was transferred to Guantanamo Bay, where he is currently being held without charge. He is considered as one of the sixteen high-value detainees.

Press articles highlighted two other ‘success’ cases in which the SWIFT data are said to have played a role, the case of Uzair Paracha and the case of the so-called ‘liquid bombers’. Paracha, a Pakistani national living in Brooklyn, was convicted in 2005 and given a thirty-year prison sentence for offences that included receiving $200,000 in exchange for assisting a Pakistani Al Qaeda operative planning to commit a terrorist attack in the US (US Department of Justice, 2006). The US Department of Justice considered this case as an example of effectively combating terrorism through ‘proactive investigation’ and ‘aggressive prosecution’ (ibid.). Later, it became public that the wire transfer from a Karachi bank to Paracha was made using SWIFT’s messaging service. However, few media organizations have reported the fact that his father, Saifullah Paracha, was also suspected of the same offences. He was arrested in Bangkok in July 2003 and was first detained in the CIA prison in Bagram, and from September 2004 he has been held as an enemy combatant at Guantanamo Bay without any official charges against him (Amnesty International, 2007).

SWIFT information is also said to have played a role in the investigation and the convictions in connection to a disrupted terrorist plot in the UK. In August 2006, 25 British individuals, some of whom have a Pakistani background, were arrested for planning attacks on at least 10 flights from the UK to the US and Canada by detonating liquid explosives. Eventually, eight men were prosecuted and three of them were found guilty of conspiracy to murder involving liquid bombs. The discovery of this plot led to the prohibition of liquids in
carry-on luggage on airplanes. It is unclear how exactly information from the TFTP contributed to the investigation and indictment in this case, but it is known that the British authorities ‘monitored the spending’ of the suspects prior to their arrest (Sherwood & Fidler, 2006), and searched for clues as to whether the plot was ‘planned, financed or supported in Pakistan and whether there is a connection to remnants of Al-Qaeda’ (Van Natta et al., 2006).

Interestingly, some more figures were mentioned in the press when the last EU-US agreement was signed in 30 November 2009, when the European Parliament was about to vote on this agreement at the beginning of February 2010, and before its final vote on 8 July that same year. In connection to the last vote, Stuart Levey revealed that information from the TFTP was used to track down three Al-Qaeda suspects planning a bomb plot in Norway (Pop, 2010f). Earlier that year, the Dutch newspaper De Volkskrant stated that the US had passed 2250 leads to other countries on basis of analysis of the SWIFT database (2010), and Het Parool stated that the searches led to 1450 leads for European governments and 700 for the Americans (Laan, 2009). In a speech, US Treasury Department Assistant Secretary for Terrorism and Financial Intelligence David Cohen mentioned that over 1550 leads were shared with countries in the EU (Cohen, 2010), citing some of the concrete examples that are also mentioned in the Bruguière report. However, it is unclear what precisely the meaning of a ‘terrorism lead’ is. On the basis of informal conversations with law-enforcement officers, it seems that a lead might simply imply passing on a name or other data elements without further information, but just the advice to look into the case. It is also important to add that law-enforcement agencies beyond the CIA may not know that the leads they receive originate from the TFTP ‘due to the fact that […] it is usually provided to third parties without indication where the information came from (European Commission, 2011, p. 5).

Finally, the confidential Bruguière report of 2010 offers a list of cases in which the TFTP has provided added value (see table 5.1). Unfortunately, it is impossible to examine all these cases in detail here but the 2005 investigation following the terrorist attack on Theo van Gogh can be taken for illustration. This attack was carried out on 2 November 2004 by the Dutch Muslim, Mohammed Bouyeri, who first shot the film artist and newspaper columnist Van Gogh, then tried to decapitate him with a knife, and implanted a letter threatening Western society with another knife in his chest. In this case the information of the TFTP is said to have ‘revealed that the attacker had connections to individuals with global terrorism connections’ during the investigation of (thus not prior to) the attack (Bruguière, 2010, p. 12).
However, press articles, reports drafted on basis of intelligence from the AIVD, the Dutch General Intelligence and Security Service (Ministerie van Binnenlandse Zaken en Koningsrijksrelaties, 2006, Commissie van Toezicht betreffende de Inlichtingen en Veiligheidsdiensten, 2008), and the court ruling in Bouyeri’s case did not find any indications of alleged international contacts. The Dutch internal intelligence service, AIVD, reported that Bouyeri had no international contacts prior or after to the attack on Van Gogh (Bessems, 2004, Ministerie van Binnenlandse Zaken en Koningsrijksrelaties, 2006, p. 5). Likewise, the court ruling states that there are indications that Bouyeri cooperated with and probably received financial support from members of the Dutch terrorist network called the ‘Hofstadgroep’, of which Bouyeri was considered to be the leader after the attack had taken place, but that this evidence was insufficient to be taken into account (Rechtbank Amsterdam, 2005). Although the AIVD and the Dutch judges considered that Bouyeri had no international contacts, with the help of telephone taps and fingerprints the AIVD found that some other members of the Hofstadgroep did. These international contacts included among others a Moroccan man suspected of involvement in the 2003 terrorist attacks in Casablanca, and with the group of Mohammed Achraf suspected of planning of the attacks in Madrid. This Spanish group also sent money to individuals who were in contact with Mohammed Bouyeri (Bessems, 2004, Kranenberg & Genovesi, 2004).

The analysis of the publicly available information on the Van Gogh murder does not reveal how and when the TFTP made a connection between Bouyeri and international terrorists or what kind of and how much SWIFT data were involved. However, the analysis does put the claim of the Bruguière report in a different perspective. First, the AIVD and the Dutch court dealing with the Van Gogh murder stated explicitly that they could not establish any contacts with international terrorists. This means that they either did not possess the information from the TFTP or they did not consider this information trustworthy or significant enough. Secondly, based on public information, the only connection that could be made between Bouyeri and international terrorist groups was indirect, via the members of the Hofstadgroep. These findings suggest that the claim made in the Bruguière report is disputable, and call into question what the added value of the TFTP information was if it did not play any role in preventing the murder of Van Gogh nor in the prosecution of Bouyeri.

Despite these examples, it remains to be debated whether these cases and recent figures justify the often repeated claims such as those made by the European Commission or the US Treasury that because of SWIFT, lives have been saved (Biden 2010, Gellman et al., 2006, Malmström, 2010, US Department of Treasury, 2010). In the words of a Member of the
European Parliament, ‘It is a fairly bold claim and if it is true then it is an important fact but we would like to see it black on white’; ‘I want proof, you know, we are decision makers, when we will be asked to take a decision on this I want all the facts and figures’; ‘[Evidence has not been forthcoming] because in some cases it is simply not there’ (interview 6). Indeed

Historical TFTP Value Examples

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

**November 2008 Mumbai Attack**
Following the attack the US Government provided information about members of the attack.

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

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

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

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

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

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

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

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

Table 5.1 Historical TFTP value examples. Source: Bruguière, 2010.
the examples above have shown that the evidence supporting the vital role of the programme in saving lives is rather thin so far. Half of the cases highlighted by Bruguière do not concern preventive action in order to avoid a terrorist attack from happening but investigations after an attack has taken place (Bruguière, 2010). Moreover, information from the TFTP has not (yet) played a crucial role in the sentencing of terrorist suspects. Hambali is currently being held without charge. In the court cases against Bouyeri and Paracha the information from the TFTP seemed to have played respectively no or only a marginal role in establishing their culpability. In addition, the ‘liquid bombers’ were initially released because of insufficient evidence. They had for instance not yet bought any airplane tickets and some of them did not possess a passport. It is not clear if and how TFTP information, as was asserted in the Bruguière report (see table 5.1), helped to convict the individuals responsible for this foiled plot.

5.5 Conclusion

This chapter has shed light on the daily practices and the analytic tools underlying the TFTP. Putting the pieces of the puzzle together—press articles, official reports and statements, academic work, and interviews—it is possible to open the black box of the TFTP to some extent. It shows that the CIA carries out subject-based queries, which means matching intelligence from terrorism investigations against the datasets requested from SWIFT through administrative subpoenas. The TFTP is also used to make link analysis of the social network of a terrorism suspect. Hence, the TFTP allows for the discovery or verification of identifying information, for instance, indications on the location of a certain individual, and for the identification of broader networks of suspected terrorists by establishing links between financial transactions. Subsequently, the obtained intelligence is passed on within the CIA, to other intelligence or law-enforcement agencies in the US or to third countries such as the EU member states, which may undertake further action.

The investigation of the technicalities and the daily practices developed in the name of the TFTP shows how the small structures the big, and raises important societal, ethical and political questions. The investigation of the design and initiation of the TFTP shows how the technicalities of the TFTP have changed the respect for certain legal safeguards and democratic principles. A first example is the use of administrative subpoenas. When the TFTP was disclosed, the use of administrative subpoenas to obtain the data from SWIFT was heavily criticized. It meant that existing frameworks of judicial oversight and international
judicial cooperation based on limited data requests were side-lined, and millions of records containing sensitive personal information could be disclosed without review and approval from a court. Although the European Parliament has attempted to limit the transfer of personal data in bulk, the practice of issuing administrative subpoenas continues under the EU-US agreement that entered into force in August 2010. Instead of an independent court, Europol is now responsible for reviewing the US Treasury’s requests and according to the review of Europol’s Joint Supervisory Body, the European police agency is ‘merely rubber-stamping’ the requests made by the US authorities (European Parliament Committee for Civil Liberties, 2011a).

In addition, the analysis of the question why the black box has not been opened and of the establishment of the programme shows significant shifts in the way in which information regarding national security circulates, and the way in which overview and authorization of national security programmes is organised. Before its exposure the existence of the TFTP was shared with a small group of selected representatives in the public and private sectors but not in a way that made democratic oversight or (confidential) discussion of the programme possible. In fact, from the initiation of the programme power was exercised through new alliances between public and private authorities, and a close partnership between the US Treasury, the CIA, and SWIFT, and later Booz Allen Hamilton. This partnership led to circumventing some certain key principles of democratic governance. Most notably, it lacked some degree of transparency about what happens with the personal data included in SWIFT’s black box, and also a form of accountability to public institutions and third countries. Despite the gradual improvements requested by SWIFT and later the European Parliament, the TFTP continues to have serious shortcomings in this respect.

The opening of the black box shows that the analyses made by the TFTP are problematic. Searches made on the basis of the matching of SWIFT data and terrorism-related information appear to be biased, as certain assumptions and political choices regarding terrorism (financing) underpin the design of the programme. The data requested in the subpoenas target certain countries, especially it seems Muslim countries, and therefore individuals and businesses that make money transfers to these countries have more chance of being associated with terrorism and included in an investigation. It also targets specific Muslim charities that are accused of terrorism ties. In addition, if the SWIFT data are indeed matched against watch lists such as TIDE, the vast majority of the listed persons consists of non-Americans and it is known that the allegations against people on this list are not always very strong. Moreover, in the previous chapter it was mentioned that people with Muslim
names and businesses with names similar to suspected members of Al Qaeda members have been targeted. As the requests in the subpoenas and the data from watch lists structure the possible outcomes, it seems that the TFTP is not politically neutral, and even discriminating, since it seems to target primarily non-American citizens or residents, people with Islamic names or people maintaining private or professional relations with these countries.

The use of link analysis for mapping terrorist networks also seems problematic. Establishing connections up to six links removed from the initial suspect leads to many false positives and useless links. According to Lichtblau ‘the searches led to inevitable dead ends’, ‘there was smoke but no fire, and Americans’ private banking records had been examined by the CIA based on suspicions that often proved unfounded (2009, p. 245). It also leads to questioning what the definition of a network is. This question has been discussed by legal experts with regard to the prosecution of terrorism networks, for instance in the court cases against the Hofstadgroep, but received little attention with respect to the use of link analysis for preventing terrorism. Connected to this, it can be questioned what the meaning is of the leads produced by the TFTP. What importance must be given to these leads?

The investigation of the results of the programme equally raises some questions. Considering the effectiveness of the programme, about fifteen cases have been made public, seven in Europe, in which information from the TFTP has played a role. Examining the examples from the Bruguière report (see table 5.1), in six cases information of the TFTP was used after an attack had taken place and in three cases to prevent future attacks from happening. In addition, since 2001 ‘more than 1550 TFTP-generated reports have been passed to European governments’ in total, and ‘over 100 of those TFTP reports have been provided in 2009’ (Bruguière, 2010). On average, this means approximately 170 leads relevant to the European countries per year. At the same time, the analysis in this chapter has also shown that the link analysis of SWIFT data is not a targeted form of analysis, it generates many false positives, and it cannot explain or discriminate between the connections it establishes. Instead of the sharp harpoon it is claimed to be, the functioning of the TFTP is more accurately described by the metaphor of the cluster bomb. These findings are important to formulating an informed opinion on the claim that the TFTP makes us safer and on the proportionality of the collection of millions of financial records made possible beyond the rhetoric of the War on Terror.

In addition, to the effectiveness of the programme in terms of numbers, it can also be questioned in terms of method. The opening of the black box and the investigation of the successes of the TFTP show only limited evidence for the claim that SWIFT data helps
‘identify, track and pursue those who provide financial support for terrorist activity’ (US Treasury, 2006). Despite its promises of prevention, link analysis cannot look into the future as the context and meaning of the financial transactions cannot be retrieved from the messages sent through the SWIFT system, and financial investigators can only speculate about the connections the software establishes. This calls into question an important assumption on which the War on Terror is based—the prevention of terrorism by using technology and large sets of personal data—and prompts us to consider the effectiveness of the methods of the TFTP and whether the programme is acceptable and desirable if its contribution to preventing terrorism is uncertain.

Furthermore, the claim that the TFTP is a soft or non-violent way to fight terrorism is questionable since investigation and prosecution on the basis of the SWIFT data and the TFTP programme directly led to one of the “success cases”, and to one other individual connected to a second case being detained and possibly tortured in secret prisons, and subsequently Guantanamo Bay. Being mapped or targeted through SWIFT data may thus have very serious implications. More importantly, this little-known connection between the sophisticated and clean way of fighting terrorism and the dark side of the War on Terror raises questions about the consistency of the European position of supporting the TFTP on the one hand and disapproving detention at Guantanamo Bay on the other.

Finally, the opening of the black box may contribute to a critical debate around the development of a European Terrorism Finance Tracking System (TFTS). The European Parliament insisted on a European version of the TFTP to avoid the outsourcing of European security decisions to the US, and make an end to the systematic and daily transfer of great amounts of European banking data to the US (Nielsen, 2012). Instead searches into the SWIFT data would be carried out by European intelligence officers and more targeted data would be provided to the US authorities. In 2011, the European Commission proposed three available options and designed a roadmap for establishing a TFTS (2011a, 2011b). However the expected date of adoption in the first quarter of 2012 was delayed and no further developments have been announced so far. In the light of these developments and following the findings of this chapter, a (renewed) discussion on TFTP taking into account the problems of the design, the methodology, and the results of the programme seems justified.
Chapter 6.

Theatre of Compliance: the Third AML/CFT Directive in Practice

There is no evidence that the Third Directive is essential or cost-effective in the fight against terrorism financing.
—Interview at the European Commission, 2009

There is a clear difference between being compliant with the Third Directive and combating terrorism financing.
—Interview a compliance officer, 2010

6.1 Introduction

The Third Directive on the prevention of the Use of the Financial System for the Purpose of Money Laundering Terrorist Financing (2005/60/EEC) (henceforth, the Third Directive) is the European Union’s most important and comprehensive instrument for fighting terrorism financing. Adopted in 2005, it requires businesses in the banking and financial services sectors to store and monitor their clients’ data and to make risk assessments to detect suspicious transactions. The Directive is a ‘preventive effort’ to combat terrorism via the financial system and has three proclaimed objectives (EU, 2005, p. 15). In Foucauldian terms these can be called ‘ideal functions’, the functions we expect the Directive to perform (Foucault, 2007, pp. 117-118, see also chapter 3).

First, the Third Directive requires regulated entities to identify their clients and to monitor their transaction data in order to detect terrorists and their associates. Due diligence procedures, meaning the detailed identification of the customer and assessment of his financial behaviour, are considered of ‘crucial importance’ for the prevention of terrorism financing (EU, 2005, p. 16). Likewise, the analysis of ‘risky’ transactions, for instance those involving large cash payments, is thought able to uncover terrorist intentions and should be reported.

A second objective of the Directive is to disrupt terrorist plots by denying terrorists access to their funding and thereby cutting off their ‘lifeblood’. This means that banks should refuse any service to entities blacklisted as terrorism suspects. Similarly, they have to report
suspicious transactions pertaining to terrorism financing to the national Financial Intelligence Unit (FIU) and, if requested by the FIU, furnish all necessary information (ibid., p. 27).

Third, according to the Directive, the transfer of legally or illegally obtained money for terrorist purposes through the financial system can jeopardize the stability and the reputation of, and confidence in, the financial system. The Directive intends to protect ‘the soundness, integrity and stability of credit and financial institutions and confidence in the financial system as a whole’ by establishing European norms integrating international FATF recommendations (EU, 2005, p. 15).

So far, the Third Directive has been studied primarily by legal scholars, and by a few political scientists and economists. A significant portion of this work consists of detailed assessments of the content of the law and analyses of the Directive in relation to the broader legal context. Mitsilegas and Gilmore (2007), for instance, examined the evolution of the EU’s three AML Directives and addressed the challenges they pose to the EU’s legislative and constitutional framework. They raised questions with regard to the legitimacy of EU action in this field – does the EC/EU have the legal competence to adopt global standards – and the compatibility of the Directive with the protection of civil liberties and certain fundamental rights, in particular the confidentiality of the lawyer-client relationship. Taking a more descriptive approach, Handoll (2006) devoted a chapter to the Third Directive. He offered a detailed legal analysis, discussing the legal basis, objectives, structure, key definitions, requirements and obligations of the Directive. A comparative analysis between the legal requirements of the FATF and those of the EU’s anti-money laundering framework has been undertaken by Van den Broek (2011b). She highlighted that despite the fact that the Third Directive aims to transpose FATF recommendations, there is a certain amount of discrepancy between the norms as defined by the EU and those of the FATF.

A few other academic works have focussed on implementation of the Third Directive. Bergström et al. (2011) studied the Third Directive as an example in which for-profit actors are given a role in assuring national security, and how this new role could jeopardize democratic accountability. They concentrated especially on differences in implementation of the Directive between the UK and Sweden. An early-stage assessment of the implementation of the Third Directive in Italy was offered by Costa (2008). Taking only the anti-money laundering aspects of the Third Directive into account, he concluded that the Directive improves the definition of money laundering in Italian legislation as well as the organizational structure for combating money laundering.
Building on these two strands of existing academic work, this chapter offers a micro-level analysis of the daily practices and modes of governing developed to comply with the Third Directive’s objectives and examines its power implications. Although literature on the Directive is growing, the detailed workings of the regulatory framework remain more or less unknown. This chapter examines the new professional field that has emerged from the requirements of the Third Directive. It considers how public and private authorities ‘co-produce’ intelligence to fight terrorism (Favarel-Garrigues et al., 2009), and how the exercise of power is dispersed across numerous places and people. It also specifically investigates new practices of governing that have been established in response to the Directive. How are accounts monitored continuously? How are customers qualified as risky? Which transactions are considered suspicious? Furthermore, questions are raised concerning the implications of fighting terrorism financing through the private sector. What are the societal and political implications of this cooperation in the case of the Third Directive, for instance, with regard to democratic accountability and transparency?

An examination of banks’ daily practices for combating terrorism is all the more important in the light of the thin results yielded by the Directive’s requirements, as highlighted in the impact assessment reports of consultancy firms and national auditing agencies. In reports for the European Commission, consultancy firms conclude that compliance with the Directive is sufficient but that the effectiveness of the Directive is difficult to measure because of a ‘lack of quantitative and limited qualitative information’ (Deloitte, 2011, p. 293). Moreover, they argue that it is difficult to measure success because the preventive effect of the recommendations can hardly be measured at all (John Howell, 2007, p. 26). The Dutch National Audit Office states that the results of the AML/CFT legislation have been disappointing. It ‘insufficiently prevents against terrorism financing’ and, ‘the chances of terrorism financing being discovered and punished are small’ (Algemene Rekenkamer, 2008, p. 15). Similarly, during fieldwork interviews, civil servants at the European Commission stated that ‘there is no evidence that the Directive is essential or cost-effective’ (interview 10) with respect to combating terrorism financing. This finding raises the question of what precisely the purpose of the Directive is, if not efficiency in the sense of amounts of assets frozen and successfully prosecuted terrorist financiers. In this chapter I argue that although the objective of the Third Directive is to inhibit the financing of terrorism, it sets in motion an apparatus of compliance in which compliance itself has become the main objective.
In order to investigate the field of governing and the governing practices emerging from the implementation of the Third Directive in detail, I shall use the metaphor of a ‘theatre of compliance’. In this chapter, the theatre is the field of governing emerging from the implementation of the Third Directive. It is ‘the autonomous microcosm set within the social macrososm’ (Bourdieu, 2000). The main objective of the field has become compliance with AML/CFT legislation. The advantages of examining the field of governing through the theatre metaphor are threefold and relate to the terminology of the theatre, the understanding of the theatre as a productive space, and the theatrical effects of the implementation of the Directive.

The terminology of the theatre is helpful because it facilitates a detailed analysis of the way in which the professional field works. Sketching the stage of the theatre helps to explain in which settings the ‘play’ (i.e. compliance) takes place and how the play is organised. The image of the stage helps to describe the (geographic) locations on which compliance is enforced and which departments within the bank are involved. It allows for assessing which actors (the participants in the field) are relevant for implementation of the Third Directive, and for describing their role. Analysing the script of the theatre play helps us to understand the governing practices through which compliance is organised. This entails a meticulous description of how AML/CFT policies create measurements on the basis of risk modelling, how scenarios operate and how transactions are deemed suspicious. Finally, the performance can be understood as the staging and representation of the results generated by the implementation of the Third Directive. Analysis of the performance also raises the question of who the audience is in this theatre.

The theatre metaphor can also be used to illustrate ‘the production of a space in which “appearance” of a particular kind becomes possible’ (Nield, 2006, p. 64). This reference to the theatre emphasizes that compliance with the Third Directive is not only a technical issue but also a social activity created by human beings. Although the legal text of the Directive might seem clear cut, the implementation appears to be far from self-evident, and can be downright messy. In fact, the Third Directive does not exactly prescribe how banks must comply, but imposes a risk-based approach. This means that in order to be compliant, banks produce their own risk categories, CFT policies and procedures against which they assess the risks posed by customers and their transactions. In turn, these procedures call into being certain performances (behaviours) by customers.

Considering the Third Directive as a productive space by looking at the professional field and its governing practices is a way of investigating the Directive from a
governmentality perspective. Examining the implementation of the Directive in terms of the stage, the script and the performance of the theatre of compliance is ‘to be sensitive to the complex geographies of power beyond pre-established scales’ (Larner & Walters, 2004, p. 14). This metaphor allows a consideration of practices of governing that affect all banking clients, and it emphasizes the dispersion of power and responsibility across an infinite number of actors in the theatre.

Finally, the discrepancy between the intended and actual results can be called the theatrical effect of the implementation of the Third Directive. As one bank employee states, ‘there is a clear difference between compliance with AML/CFT legislation and combating terrorism financing’ (interview 14).

As described in chapter 3, international measures to fight terrorism financing have often been grafted on to pre-existing anti-money-laundering frameworks. This is also true for the European Union, where the CFT dimension has been added to existing AML legislation and resulted in the Third AML/CFT Directive. To provide more context to on how the ‘theatre of compliance’ came into being during the 1990s and the first years of the new millennium, it is necessary first to give a short description of the legal scope and the political decisions upon which the Third Directive is built. Next, the choice of the theatre metaphor for analysing the governance practices of the fight against terrorism (financing) is discussed. The subsequent sections examine the stage, the scripts and scenarios and the performance of the theatre of compliance that are set in motion through the Third Directive.

6.2 The Development of the EU’s Anti-Money-Laundering Directives

6.2.1 The First Anti-Money Laundering Directive

In the 1980s, the US War on Drugs galvanized international concern regarding profits from drug trade. European states and the European Community actively supported the development and adoption of international measures aimed at combating money laundering (Gilmore, 2004, Mitislegas & Gilmore, 2007). In these years, the European Parliament demanded Community action with respect to the illegal drug trade. The financial aspects of the drug trade and money-laundering practices were first mentioned in an EP Resolution, and in the European Council Conclusions of 1986. Subsequently, the European Commission became involved in negotiating the 1988 United Nations Convention against the Illicit Traffic
in Narcotic Drugs and Psychotropic Substances, and the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime. These two conventions defined, for instance, what money laundering is, and sought to criminalise money laundering through international law. Parallel to these initiatives, international standards and coordination aimed at preventing money laundering were enhanced by the establishment of a Financial Action Task Force and the adoption of its 40 Recommendations in 1989.

In 1990, the European Community undertook formal discussions regarding the adoption of European anti-money laundering legislation. This resulted in a Council Directive on the Prevention of Use of the Financial System for the Purpose of Money Laundering (91/308/EEC), (henceforth, the First Directive). The justification for a European initiative in addition to pre-existing international ones followed a ‘two-fold threat rationale’, combining a threat to the financial system and financial institutions and a threat to society in terms of health, life and the social fabric (Mitsilegas, 2003, p. 55). Other justifications for adopting the Directive were the need to protect the European Single Market from criminal money, and demonstrating to the outside world (in particular to the US) that the EC was acting in a united manner and going beyond existing international legislation by adopting preventive and legally binding instruments (Bergström, 2011, pp. 105-106, Gilmore, 2004, pp. 194-195, Mitsilegas, 2003, pp. 55-56). In addition, adoption of the Directive was also presented as ‘one of the most effective means of opposing this form of criminal activity’ (European Communities, 1991).

The final text of the Directive was adopted in 1991 and brought money laundering under Community law. It adopts not only the criminalization approach of the UN and the Council of Europe instruments prohibiting and penalizing money laundering, but also a preventive approach based on the 40 FATF recommendations in the form of imposing duties on credit and financial institutions in order to stop money laundering. The adoption of the Directive is remarkable for two reasons. It indirectly gives the European Community competence in the sphere of criminal law, which it formally does not have (Bergström, 2011, p. 105, Mitsilegas, 2003, p. 58), and it extends the fight against money laundering to the private sector, recognizing that ‘the financial system can play a highly effective role’ (European Communities, 1991).

More specifically, the First Directive required credit and financial institutions to establish customers’ identity and keep records of their transactions, the ‘Know Your Customer’ or KYC principle. Moreover, credit and financial institutions are obliged to actively report any suspicious transaction to the authorities responsible for combating money laundering, and have a passive duty to provide all necessary information at the request of
these authorities. A corollary of the duty to report suspicious transactions is the obligation to
demonstrate due diligence in monitoring transactions. Hence, credit and financial institutions
have to examine whether any transaction is likely to be related to money laundering, in
particular complex, unusual, large transactions or sequences of transactions following strange
patterns, or those involving countries that comply insufficiently with the FATF
recommendations. Furthermore, credit and financial institutions have the duty to refrain from
transactions of which they suspect any relation with money laundering until they have further
instructions from the authorities combating money laundering. The obligation of
nondisclosure to the customers concerned and third persons the information transmitted to the
authorities (no tipping off) is another duty provided for in the Directive.

The first decade following the adoption of the First Directive must be seen as a
‘pioneer phase’ in which practices and procedures for the transfer of suspicious transaction
data from the private sector to competent authorities and the follow-up on this information
were shaped (Vedder & van Nunen, 2003, p. 72). During the 1990s, banks did not consider
reporting suspicious transactions a priority, and their AML policies remained rather limited
(interview 15). The main responsibility for crime prevention rested with public actors, and the
dichotomy between the public and the private sector was not challenged by private actors
(Bergström et al., 2011, p. 1049). It also took some time to organize the information-receiving
side. There was no agreement on an internationally accepted model for the functions of a FIU
(Financial Intelligence Unit) in the early 1990s (IMF, 2004, p. 9), since each country
preferred a model best fitting its own objectives and institutional architecture. Moreover,
within states, various agencies competed over the responsibilities emerging from the
Directive, attempting to strengthen their own position in the field (see for instance Vedder &
van Nunen, 2003).

The First Directive is nevertheless important because it introduced a preventive
approach to money laundering in which the private sector has to report suspicious transactions
to competent national authorities, later qualified as Financial Intelligence Units. This rationale
and reporting structure has been maintained, extended and enhanced, in subsequent AML
Directives (see table 6.1).
Successive inclusion and extension of reporting entities

| First AML Directive (1991) | - Credit institutions as defined in Directive 77/78/EEC  
- Financial institutions carrying out operations as defined in Directive 79/267/EEC  
- Insurance companies |
|---------------------------|---------------------------------------------------------|
| Second AML Directive (2001) | Extension of the definition of financial institutions to include investment firms and collective investment undertakings  
Inclusion of:  
- auditors, external accountants and tax advisors  
- real estate agents  
- some operations of notaries and independent legal professionals  
- dealers in high value goods such as precious stones or metals or works of art  
- casinos |
| Third AML/CFT Directive (2005) | Extension of the definition of dealers in high-value goods to natural or legal persons trading in goods worth € 15,000 or more and paid cash.  
Inclusion of: Trust or company service providers |

Table 6.1 Successive inclusion and extension of reporting entities.

6.2.2 The Second Anti-Money Laundering Directive

Throughout the 1990s, a number of arguments were raised to revise the First Directive. Firstly, the European Council emphasized the link between money laundering and organised crime (see for instance European Council, 1999). Although the text of the First Directive related not only to drug trafficking offences but also to the broader notion of criminal activity, there was a perceived need to explicitly extend the predicate offences listed in the Directive. Secondly, it was argued that money launderers had circumvented AML legislation by making use of sectors outside the realm of the Directive (Mitsilegas, 2003, p. 86). Therefore, the scope of professions concerned by AML legislation needed to be widened ‘outside the classical financial sector’ (European Council, 1996). Thirdly, it was argued that not only had money launderers changed their modus operandi, but also the banking sector had changed during the 1990s. Developments in technology made some parts of the Directive outdated, and new developments, such as possibilities resulting from generalized access to the Internet had to be included (Gilmore, 2004, p. 201). A fourth aspect that needed to be addressed was the improvement of information exchanges between FIUs. The European Council stated that ‘regardless of secrecy provisions applicable to banking and other commercial activity, judicial authorities as well as FIUs must be entitled, subject to judicial
control, to receive information when such information is necessary to investigate money laundering’ (European Council, 1999). A fifth argument concerned the need to transpose new international legislation and guidelines into European legislation. These consisted most notably of the updated FATF recommendations of 1996.

Taking into account all these issues, the European Commission scheduled a proposal for a Second Anti-Money Laundering Directive in 1999. Yet, it took over two years of debate to adopt a new text. The main issues of contention were the definition of the predicate offences and the decision on the range of professions covered by the Directive (Gilmore, 2004, Mitsilegas, 2003). Following the revised FATF Recommendations, the Second Directive referred to money laundering in relation to organised crime instead of (drug-related) criminal activity. This meant that the provisions of the new Directive also applied to organised crime, fraud, corruption or any other illegal activity damaging or likely to damage the European Community’s interests (European Union, 2001). The European Parliament’s Committee of Citizens’ Rights initially preferred a more restricted definition of organised crime than the European Commission, the Council, and finally a majority in the Parliament. The Citizens’ Rights Committee also objected to the Council’s extension of predicate offences to a broad notion of serious crime (Lehne, 2000). Yet, again, in the plenary session of the Parliament, a majority was in favour of the Council’s definition.

The European Parliament’s debate on the extension of professions concerned by the Directive was even more heated. The Second Directive extended the professions with a reporting duty to currency exchange offices, money transmission remittance offices, casinos, dealers in high value goods, external accountants, auditors and tax advisors, lawyers, notaries and real estate agents (see table 6.1). The inclusion of the legal profession led to especially fierce objections by the European Parliament. Many MEPs were deeply concerned that inclusion of the legal profession would violate the right to a fair trial and the principle of lawyer-client confidentiality (Gilmore, 2004, p. 203, Wahl, 2010, p. 131). They considered that the legal profession should benefit from broader exceptions with regard to some of the requirements of the Second Directive, a point they finally obtained. On the other hand, the EP wanted to include a much wider range of professions than the Council and the Commission. The latter concluded that for practical and definitional reasons an extension to dealers in art works and luxury goods would be problematic (Mitsilegas, 2003, pp. 95-98). Finally, the ‘9/11’ attacks increased pressure on the Parliament during the conciliation procedure and provided another justification for quickly revising the existing AML legislation (Lehne, 2001, p. 7). Finally, the Second Directive was adopted on 4 December 2001.
In sum, the Second Directive brought European legislation in line with international standards and adapted it to new money laundering practices and the latest technological developments. It broadened the scope of predicate offences as well as the regulated professions. It also strengthened the customer identification requirements, especially in case of non-face-to-face operations using computers. In addition, a new provision as to the information exchange of Suspicious Transaction Reports (STRs) was added, insisting on compliance with the FATF recommendation on the establishment of an FIU in each member state.

However, due to the fact that for pragmatic reasons the notion of a “competent authority” (i.e. the FIU) was left undefined, a heterogeneous landscape arose in which broadly four different models for reporting STRs can be distinguished (see table 6.2). Quite some EU member states adopted an administrative reporting model, in which regulated professions report suspicious transactions to an administrative body, for instance the Ministry of Finance, the central bank, or an independent body. This means that an independent administrative body investigates the justification of a STR before transferring this information to law-enforcement agencies. One of the advantages of this model consists of the ‘buffer’ it creates between the financial sector and law-enforcement authorities in charge of investigating and prosecuting financial crime (IMF, 2004, pp. 10-11). Others opted for a police model in which reporting entities send their reports to a law-enforcement agency. The rationale behind this model is the possibility of employing the existing institutional framework and existing expertise of financial crime units (ibid., pp. 13-14). A few EU member states chose a judicial model, in which the FIU is situated in the office of the public prosecutor. This model can be seen as more independent from political interference and as efficient with regard to the speed of receiving suspicions and prosecuting offences (Mitsilegas, 2003, p. 169, IMF, 2004, p. 16). Two countries adopted a hybrid model that combines the characteristics of at least two models. This model ‘serves as disclosure intermediary and a link to both judicial and law-enforcement authorities’ (Masciandaro, 2007, p. 66). The distinctions between these models are important, as different rules for data exchange and protection apply to information depending on whether it is gathered in an administrative, police or judicial context. In order to facilitate information exchange between the different FIUs of the EU member states, a Council Decision was adopted in 2000 (2000/642/JHA).
Typology of FIUs in the EU

<table>
<thead>
<tr>
<th>Model</th>
<th>Countries</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative</td>
<td>Belgium, Bulgaria, Czech Republic, France, Italy,</td>
</tr>
<tr>
<td>(11)</td>
<td>Malta, Poland, Romania, Slovenia, Spain</td>
</tr>
<tr>
<td>Police</td>
<td>Austria, Estonia, Germany, Hungary, Finland,</td>
</tr>
<tr>
<td>(11)</td>
<td>Ireland, Lithuania, Portugal, Sweden, Slovakia,</td>
</tr>
<tr>
<td></td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Judicial</td>
<td>Cyprus, Denmark, Latvia, Luxembourg</td>
</tr>
<tr>
<td>(3)</td>
<td></td>
</tr>
<tr>
<td>Hybrid</td>
<td>Greece, the Netherlands</td>
</tr>
</tbody>
</table>


6.2.3 The Third Anti-Money Laundering/Combating the Financing of Terrorism Directive

The EU decided to develop a Third AML/CFT Directive in response to the FATF’s Eight Special Recommendations on terrorism financing complied in the wake of 9/11 and their revision in 2003. In contrast to the Second Directive, the decision-making process went quickly. Negotiations started in 2004, and the Directive was adopted at first reading under the co-decision procedure in 2005. According to former Internal Market and Services Commissioner Charlie McCreevy, ‘intense cooperation between the European Parliament, the Council and the Commission has paved the way for a swift adoption of state-of-the art defences in the EU against money laundering and terrorist financing’ (European Commission, 2005).

However, the relatively quick adoption of the Third Directive should not be taken to mean that it consisted of only minor changes, or that it was accepted without opposition. The Directive extends the existing reporting requirements to new professions (see table 6.1) and new predicate offences. It also attempts to improve some of the shortcomings of the Second Directive, providing more guidance on customer identification requirements, for example. Moreover, it elaborates on some of the issues left undefined in earlier Directives, for instance, by describing the work and powers of FIUs and introducing the supervision of compliance and sanctions in case of non-compliance. Finally, repealing and replacing the First and the Second Directives, the Third Directive represents a qualitative shift in purpose, and consequently in the way the Directive operates as a governing practice. Two new elements are of particular importance to the Third Directive: an explicit inclusion of the fight against terrorism financing, and the embracing of a risk-based approach.

The extension of the Directive to include terrorism financing was considered a logical step in the War on Terror. It evidences the importance of anti-money laundering legislation as a central component in the global strategy to undercut terrorist financing (Mitsilegas & Gilmore, 2007, p. 125). According to the legal text ‘the preventive measures of the Directive
should cover not only the manipulation of money derived from crime but also the collection of money or property for terrorist purposes’ (European Union, 2005, p. 16). The definition of terrorist financing adopted in the Directive is similar to the definition expressed in the 1999 UN Convention on the Suppression of Terrorism Financing and involves:

the provision or collection of funds, by any means, directly or indirectly, with the intention that they should be used or in knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (ibid., p. 20).

According to the text of the Third Directive, terrorism financing often involves international transactions, cash transactions, criminal or clean money, and may also concern service providers outside the financial sector.

Whereas the explicit inclusion of terrorist financing in the Third Directive was presented as indispensable after 11 September 2001, it is interesting to recall that during discussions of the First Directive, terrorism was excluded from the draft in the early 1990s. In the First and Second Directives, the Commission decided to adopt a minimum standard approach defining the money laundering of proceeds of ‘criminal activity’ as applying to drug offences as specified in the Vienna Convention, and other criminal activity designated as such for the purposes of this Directive by each member state (Mitsilegas, 2004, pp. 66-68). Hence, EU member states could individually decide to include terrorist offences within the scope of the Directive, but prior to 9/11 most countries did not consider this necessary.

A second major change of the Third Directive was its shift from a ‘rule-based approach’ to a ‘risk-based approach’. The rule-based approach that characterized the First and Second Directives entails the application of a set of fixed norms to every transaction. In order to assess transactions, these norms must be very detailed and clear, as, for instance, the obligation to report every cash transaction that exceeds the amount of €15,000 (Van den Broek, 2011a, p. 171). One bank employee describes it as follows:

The rule based-approach is very much a check-the-box exercise. For instance, you go down the questionnaire and if you have 27 positive responses and 3 negative ones, it means that the transaction scores 27 points. If 25 points is the established threshold, it means that the transaction is suspicious and must be reported. It also works the other way around: if a transaction is 66% normal and the norm for reporting is below 60%, then the transaction becomes considered as completely unsuspicious (interview 14).

Banks have been increasingly opposed to the rule-based approach, which they consider ineffective and requiring a disproportionate allocation of resources. The rigid character of the norms effectively meant that all transactions had to be considered in the same way without
much reflection. Moreover, it was thought that criminals who were aware of the norms were able to adapt their transactions accordingly (Unger, 2007, Van den Broek, 2011a).

Since 9/11, risk has become crucial in waging the War on Terror. Risk management is ‘a particular mode of governing – a means of making an uncertain and unknowable future amenable to intervention and management’ (Amoore & De Goede, 2008b, p. 9). Governing through risk does not imply the reduction of existing risks, but an attempt to calculate them. It is rather about upholding the ‘myth of control and manageability’ by dealing with uncertainty in an organised way (Power, 2004). Adopting the lens of risk is to look at the world from a specific perspective in which control of the financial sector can be strengthened while the mobility of money continues and becomes even easier in some cases (De Goede, 2006, Bergström, 2011).

The risk-based approach adopted in the Third Directive focuses on transactions responding to specific combinations of criteria instead of monitoring all transactions. It allows for differentiation between different kinds of risk such as customer risk, product or services risk, and geographical risk. As a consequence, monitoring practices and identification requirements vary according to the risk scores assigned to the profile of the customer, the specific financial product or the services and countries involved in a transaction. In the terminology of the Directive, a distinction can be made between ‘simplified due diligence’ procedures for certain customers and ‘enhanced due diligence’ procedures imposed on others. Moreover, the norms are not only differentiated according to the kind and level of risk, but they are also flexible. Risks are evaluated according to changing terrorism financing trends and profiles. The proclaimed advantage of these malleable risk criteria is that criminals cannot adapt their behaviour to avoid attracting attention to their transactions. Finally, transaction monitoring is carried out continuously. In addition to an assessment at the time the account is opened, banks are also required to monitor customer accounts and transactions on an on-going basis. As such, unusual or out of the ordinary transactions are flagged almost instantly.

The risk-based approach introduced in the Third Directive addresses some of the main shortcomings of the rule-based approach. Regulated professions obtained much more flexibility and discretion with respect to transaction monitoring procedures. It was hoped that they might thereby avoid unnecessary administrative burdens and design procedures to be more cost-effective. Moreover, the risk-based approach ‘brings great efficiency in the system (…) in that it enables banks to dedicate their resources to those things which are of higher risk and (…) those customers of lower risk cannot be burdened with undue due diligence and such alike’ (House of Lords, 2009a, p. 25). In addition, the quality of the reports was expected to
be better, because banks could direct their attention to more limited sets of transactions and file STRs on the basis of reasoned judgement, instead of a general questionnaire. ‘[Banks] have to look at clients, our products and perhaps even whole [economic] sectors’ (interview 14). This, it was believed, would result in a more effective framework for combating money laundering and terrorism financing. However, one must bear in mind that the definition of and the value assigned to a specific risk are not readily established. The quality of reports and the effectiveness of the reporting system therefore depend largely on the design of the risk management software and the expertise of compliance officers.

As a governing practice, the risk-based approach requires more active behaviour on the part of banks. Reporting entities must be able to demonstrate that they have ‘adequate and proportionate policies and procedures of customer due diligence, reporting, record keeping, internal control, risk assessment, risk management, compliance management and communication’ to identify and prevent the terrorist financing risks their business faces (European Union, 2005, p. 29). Consequently, the requirements of the Third Directive entail a shift of responsibility and authority from the public sector to the private sector in the field of national security (Bergström et al., 2011, De Goede, 2006, Unger, 2007, Van den Broek 2011a).

Although both the inclusion of terrorism financing and the shift to a risk-based approach were widely supported, the adoption of the Third Directive was controversial for several reasons. The main issue was the question of individual privacy rights versus security interests. The LIBE Committee of the EP concluded that the proposal for the Third Directive ‘belongs in the grey area in which individual rights and freedoms may have to be sacrificed in the higher general interest of preventing and repressing terrorist activity’ (Nassauer, 2005, p. 148). However, two MEPs, Giusto Catania from Italy and Sylvia-Yvonne Kaufmann from Germany, maintained their minority opinion opposing the text of the Third Directive and stated that ‘control and surveillance are weighed far higher than the protection of civil liberties’ in the fight against terrorism financing (Borghesio, 2005, p. 9).

Furthermore, the European Parliament considered that the compromise reached in the Second Directive regarding the reporting duties of lawyers and notaries needed clarification. MEPs doubted whether ‘the complete confidentiality of the information communicated to a lawyer is still guaranteed’ when these professionals are required to report suspicious transactions (Nassauer, 2005, p. 82). This issue was also actively taken up by different interest groups. In a letter to the European Commission, the Council of the Bars and Law Societies of Europe (CCBE) called for delaying the Third Directive. They argued that the implementation
of the Second Directive had not yet been evaluated. The CCBE also repeated their claim that this Directive ‘breaches the fundamental rights of EU citizens’ and highlighted ‘that no research into the human rights’ and civil liberties’ effects of the Second directive has been carried out’ (CCBE, 2005). In addition, French Bar associations sent a petition to the European Commission in 2003 warning that the normal activities performed by lawyers could be impeded by the requirements of the Third Directive (Petition 693/2003, see also Nassauer, 2005, p. 149). They also brought a challenge before the Conseil d’Etat regarding the compatibility of the Second Directive’s requirements and the right to a fair trial based on independent lawyers and confidential lawyer-client relations. Likewise, the Belgian Bar Association asked the Belgian Cour d’Arbitrage to consider the same issue (CCBE, 2006, p. 2).

Representatives of banking and financial institutions were opposed to some of the new definitions and concepts described in the Third Directive. They heavily lobbied MEPs to convince them that the disclosure requirements imposed would be far too heavy a burden on their sector and suggested many amendments (EurActiv, 2005). Of particular concern were provisions on ‘politically exposed persons’ (PEPs). The Directive defines these as ‘natural persons who are or have been entrusted with prominent public functions and immediate family members, or persons known to be close associates, of such persons’ (European Union 2005, p. 22). These include, for instance, heads of state or of government, senior politicians, senior government, judiciary or military officials, senior executives of state-owned corporations, and important political party officials (House of Lords, 2009b, footnote pp. 31-32). According to the text of the Third Directive, foreign PEPs and their immediate family should be subject to enhanced due diligence procedures while low risk clients, for instance public authorities or actors providing State services, qualify for simplified due diligence procedures.35 The decision to single out this group of people must be seen in the light of several corruption scandals of which the ‘Abacha affair’, named after the Nigerian President and members of his inner circle who stashed away over 2.2 billion dollars in foreign bank accounts, received a lot of publicity (interview 14). Banks argued that it would be very challenging to identify all PEPs worldwide. The European Banking Industry Committee also maintained that the definition of a PEP stands in contradiction with the risk-based approach in that it included everyone, not only those posing a genuine risk (Euractiv, 2005). However, these arguments were overridden, as the inclusion of PEP requirements into the Third Directive stems from international agreements, such as the FATF’s guidelines and the United Nations Convention against Corruption.
MEPs and banks also objected to the requirement to identify and verify, on a risk-sensitive basis, the ‘beneficial owner’ of the bank account. This is ‘the natural person(s) who ultimately owns or controls the customer and/or the he natural person on whose behalf a transaction or activity is being conducted’ (European Union, 2005, p. 22). Based on a FATF recommendation, this requirement aims to identify the shareholders involved in corporate transactions. However, MEPs argued that the Commission’s initial proposal to identify all shareholders possessing or controlling 10% or more of a company is ‘overly ambitious and leads to unnecessary and onerous checks’ (Nassauer, 2005, p. 115). The European Banking Industry Committee considered that the concept of beneficial owner was ‘too restrictive’ (EBIC, 2005, p. 5). Likewise, the Federation of European Banks stated that ‘banks do not have access to reliable information which would enable them to properly identify beneficial owners’ (EurActiv, 2005).

Other issues raised in relation to the Directive concerned, for instance, the implications for universities and business schools of the requirement to investigate any cash payment of over € 15,000 for possible money laundering (KPMG, 2005) and the possibility for hotels providing money exchange facilities to be exempted from reporting obligations if they fulfilled certain criteria.

MEPs also questioned the lack of evidence regarding the effectiveness of the Third Directive. Already in the discussions preceding the adoption of the Second Directive, MEPs argued that ‘it has not yet been possible to prove any links between reports of suspicious transactions and convictions for money laundering or predicate offences’ (Lehne, 2000, p. 26). The main complaints in the discussions about the Third Directive consisted of the fact that the effectiveness of the Directive remained still unknown because the Directive had not yet been assessed and was in some cases not even transposed into national law (Nassauer, 2005, p. 83, 121). British Conservative MEP Theresa Villiers (EPP) stated, for instance, that there had been no serious scrutiny into the existing AML legislation, and that she had come to the conclusion that ‘these rules do almost nothing to catch criminals or terrorists and merely provide inconvenience to law-abiding citizens in carrying out innocuous everyday financial transactions’ (Villiers, 2004).

A related issue of contention, but of procedure rather than content, was the haste of the procedure. Both MEPs and professions covered by the Directive complained about the urgency of some member states and the European Commission to adopt a new AML/CFT directive. In fact, the deadline for EU member states to transpose the Second Directive into national law was June 2003, but approximately half of them had done so by that time. When
the Commission tabled the proposal for a Third Directive in 2004, the assessment of the Second Directive, required according to the text of the Directive, had not been made.

Despite this opposition, the European Parliament rejected a majority of the proposed amendments. The Third Directive was approved by the EP on 26 May 2005 and formally adopted on 26 October 2005 during the UK’s Presidency of the EU. It was recognized that further legislative measures would be needed to deal with various technical issues in order to achieve a consistent implementation across the European Union. Those measures are now contained in an Implementing Measures Directive that came into force on 24 August 2006. The Directive was to be transposed into domestic legislation before 15 December 2007. However, in mid-2008, 15 EU member states had not complied with this requirement.36 The Third Directive has been amended by Directive 2008/20/EC of the European Parliament and of the Council of 11 March 2008. A Fourth Money Laundering Directive is currently envisaged, and an official proposal from the Commission is expected in 2013, integrating the latest revisions of the FATF recommendations.37

The three Money-Laundering Directives have strongly shaped the European institutional architecture for combating terrorist financing and money laundering, notably through the establishment of Financial Intelligence Units (FIUs) and an obligation on an important number of private actors to supply information for national security reasons. However, it must be emphasized that the Third Directive differs significantly from the earlier AML Directives by its inclusion of the fight against terrorism (financing) in addition to combating money laundering. Moreover, the Third Directive alters considerably the initial AML framework by introducing a shift from a rule-based reporting system to a risk-based approach. The analysis of Third Directive practice shows how the Directive gave rise to a new field of governing and led to new governance practices. It also draws attention to the potential uncertainty, controversy and arbitrariness embedded in the execution of the Directive. The following section provides a theoretical discussion about the use of the theatre metaphor and explains how the notion of a ‘theatre of compliance’ contributes to a detailed examination of the Third Directive from a governmentality perspective.
6.3 Theatre of Compliance

Academics have used the metaphor of the theatre in several ways to describe aspects of terrorism as well as combating terrorism. The parallels between the theatre and (counter-) terrorism’s use of mass media have been especially attractive to explore. As early as the 1970s, Brian Jenkins wrote that ‘terrorism is aimed at people watching, not at the actual victims. Terrorism is theatre’ (1974, p. 4). He stressed that to be effective, terrorists create dramatic and carefully choreographed events capturing their audiences and generating maximum media attention for their demands. More recently, the use of the theatre metaphor in relation to terrorism has been taken up by other scholars. Similar to Jenkins, Gabriel Weimann stresses the importance of mass media for terrorism through his notion of the ‘theatre of terror’ (1983, 2006, 2008). He states that terrorists write the script and perform the drama while media may provide the stage to access worldwide audiences (2006, p. 38). In his view, the terrorist act is a theatric performance that is given a stage by the media.

Beatrice De Graaf (2010) argues that terrorist acts create a ‘theatre of fear’. Continuing the theatre metaphor, she states that media reporting or prosecution of terrorists in court can become a performance and provide a podium for terrorists to expose their case, and for the judicial authorities asking for greater punishments. The theatrical aspects of criminal proceedings are underscored by the staging of highly protected courtrooms, the creation of new prisons, the adoption of dramatic security measures during the proceedings, or suspects’ refusal to cooperate. This was, for example, the case in the trials of members of the RAF and the Brigate Rosse. Contrary to Weimann, De Graaf argues that the success of terrorists in creating a theatre of fear depends mostly on the reaction of the population to the attack, as well as on the capacity of the state and the terrorists to influence popular perceptions (ibid.). In sum, the works of Jenkins, Weimann and De Graaf use the terminology of the theatre to emphasize that terrorist acts and (combating) terrorism are a strategy of expression and communication to either draw people’s attention to terrorists’ objectives or to ‘stage the state’ (De Graaf, 2010, p. 261, emphasis added).

This chapter also adopts the terminology of the theatre, but the theatre metaphor will have slightly different purposes. The notion of a theatre of compliance will be used to further an understanding of EU’s fight against terrorism financing through implementation of the Third Directive and to demonstrate how some aspects of the Directive are theatrised. The terminology of the theatre helps to make the professional field of governing visible as well as
its governing practices. There are also communication aspects to the implementation of the Third Directive. Banks, for instance, have an interest in complying with AML/CFT requirements because press articles about non-compliance could seriously damage a bank’s reputation. However, this chapter is not directly concerned with the influence of mass media on efforts to combat terrorism financing.

A few scholars have used the theatre metaphor with respect to daily security practices. In his essay ‘The Psychology of Security’, Bruce Schneier (2008) distinguishes between the reality of security and the feeling of security. He uses the term ‘security theatre’ to describe security measures that only increase citizens’ feelings of security and do not influence the reality of security. One such security measure is, for example, the introduction of photo ID checks in office buildings. Schneier points out that ‘no one has ever explained why verifying that someone has a photo ID provides any actual security, but it looks like security to have an uniformed guard-for-hire looking at ID cards’ (2009). Another example of security theatre is the posting of National Guard troops at American airports after 9/11. They served to decrease the anxiety of the passengers rather than prevent hijackings or bombings (Schneier, 2003, p. 38). This element of managing the impact of terrorism by reassuring the population through measures that make them feel safer is also present in the implementation of the Third Directive.

Nield (2006) addresses the theatricality of the border. She examines how border spaces reflect a particular spatial imaginary and produces the individual who attempts to cross. She argues that the contemporary border ‘is not quite there’, fixed in a specific place (p. 69). Rather, the border appears in the bureaucratic production of it, and through the staging of mechanisms of regulation governing migration. These mechanisms ‘compel certain kinds of appearance’ (p. 64) and require border-crossers to simultaneously be present (as actors) and to represent themselves effectively (as characters). In addition, Nield stresses that ‘while appearing to be stable, and the same for everyone,’ the rituals that are part of crossing the border are not neutral instruments but ‘construct and perform difference’ (p. 67). The function of the border is thus not limited to marking a territory in which certain rules apply, but also serves to construct the national imaginary, giving a sense of belonging to some and excluding others (2006, pp. 66-67). Nield’s work is interesting because she draws attention to the border as a productive space, but also as a site that constructs national imaginaries and differentiates between insiders and outsiders. Like the mechanisms of border security, the procedures and practices of the Third Directive perform the idea of a clean financial sector free from dirty
money, and they establish norms defining who can (not) be part or make use of the formal financial system.

Amoore and Hall (2010) examine the ‘border theatre’ and investigate the theatrical rituals of border security – scanning, screening and verifying identity – to which we have become used and which we have ceased to question. They ask how surprising artistic encounters with techniques and technologies of security can revive and strengthen public engagement with border practices. In their view, the border resembles a theatre in the sense that border rituals are a matter of display or show. The space of the border ‘is a political stage for the performance of control’ suggesting ‘securability and controllability’ (p. 303). Moreover, the border is also productive, like the theatre, in the sense that it permanently creates and questions appearances and identities. It brings into being series of recognizable categories, such as state authorities, illegal aliens and risky travellers, and requires border crossers to appear in a certain way by demanding specific behaviours and responses.

To start questioning the security practices at the border and to understand the assumptions on which they are based, Amoore and Hall affirm that the principles of Berthold Brecht’s epic theatre are of interest. This form of theatre uses interruptions of the sequence in order to draw attention to the existing conditions. Like the theatre, border security practices also depend on repetitions and sequences.

It is precisely these too little noticed repetitive sequences of the border – the multiple calculations and identifications that constitute the sovereign practices of authorization – that make the very idea of security possible. It is not the single declaration of exception per se that produces sovereign power, but the multiple “repetitive acts” that write the very possibility of a securable state (p. 301).

Through interrupting these practices, they can be rendered strange and the repetitions on which they are based can be seen more carefully.

Analysing different artworks, Amoore and Hall highlight the ‘spaces of resistance that are always present in security practices’ (p. 301). For example, Toy an Horse, a ten metre high Janus-faced Trojan Horse placed at the border between Mexico and the US, defamiliarizes the border crossing through its presence and interrupts security sequences, potentially provoking a questioning of daily security practices. Another artwork, the Transborder Immigrant Tool, uses mobile phones equipped with GPS technology to indicate the safest and most aesthetic routes to pass the US-Mexican border through a Virtual Hiker algorithm. As such, it combines art and political act and temporarily reverses power by providing tracking technologies to those who are tracked. Finally, the art projects of Meghan Trainor use RFID (Radio Frequency Identification) technology. The essence of Trainor’s work
is to experience RFID outside the contexts in which they are generally used and detaching them from pre-established meanings. These works have in common that they make the forgotten patterns on which security rests strange. They do not impose or demand judgement, but rather ‘discomfort and unsettle one’s sense of certainty’ (p. 312); they also stimulate public engagement by re-introducing the unexpected.

Like the border theatre of Amoore and Hall, the theatre of compliance is understood as a stage suggesting controllability through the repetition of mundane security practices. This chapter considers how the theatre of compliance brings into being groups and categories by analysing the ‘actors’ appearing on the stage. Drawing attention to the script and scenario of the theatre of compliance, the chapter analyses the ‘multiple repetitive acts’ through which financial (ab)normalities and (ir)regularities are identified, established and developed. In order words, it explores how the risk-based approach works on a day-to-day level in banking practice, and how categories of suspicion and abnormality are constituted through mundane acts of repetition, rather than strictly through overarching and fixed risk classifications. Unlike the work of Amoore and Hall, this chapter will not consider how artworks may draw attention to and question security practices by interrupting them, but it does aim to provoke reflection on security practices within banks by making them more visible through detailed description.

The risk of using theatre as a metaphor is its connotation of being something that is false or consisting of only appearance. I certainly do not want to suggest that compliance with the Directive by banks is anything but sincere. My experience from a range of interviews is that banks take implementation of the Directive extremely seriously and feel it is important to implement the law correctly. What the theatre of compliance metaphor makes clear is that the professional field and professional practices are in motion, and have grown enormously in recent years. The metaphor also aims to make to make visible a disconnect between the objective of the Directive – combating terrorism finance – and the shift that takes place while implementing the Directive – complying with CFT requirements. As will become clear below, these two objectives do not overlap, which makes a study of the political and societal implications of these measures all the more urgent.
6.4 The Stage

Within political science literature, the notion of the stage has been used for various purposes and especially in relation to the nation (state) (e.g. Hogan, 2003, Kruger, 1992, Wilmer, 2004). In these accounts the stage often refers to a site of ritual or self-representation. In this section, the notion of the stage permits consideration of actors belonging to the theatre beyond the institutional boundaries of the bank, and of the roles these actors hold as well as the different locations in which the play takes place. It shows how implementation of the Third Directive within banks is productive, like the theatre, as it brings into being a field of governing in which participants or actors contribute to ensuring compliance. In this section the stage undergoing analysis comprises the whole compliance process within a bank, from shaping CFT policies to reporting suspicious transactions.

To relate back to the professional field of the Third Directive presented in chapter 2, the examination of the stage resembles the mapping of a field of governance in that it makes different participants and the relations between them visible. However, the investigation of the stage in this chapter is restricted to the performing of compliance by banks, as opposed to the field map of chapter 2, which considers a broader transnational governing process. The stage described here consists mainly but not exclusively of the participants possessing operational powers on a national level represented in the lower right case of the field map.

Before analysing the different actors and sites of the theatre of compliance, it is important to stress that the stages of the theatre are different in every bank and form a very heterogeneous environment involving numerous and dispersed actors and sites within the bank. Despite the fact that one of the aims of the Third Directive is to harmonize AML/CFT requirements within and between EU member states, this does not imply that it imposes or provides a ‘one-size-fits-all’ model or a miracle solution for organizing compliance. A high degree of flexibility was indispensable for coping with the specificities of the different regulated professions, as well as the great diversity within specific professions. Banks differ with respect to their size, their core activities, their profile and their geographic presence, yet the Directive must be implemented by all banks, ranging from small savings banks to mainstream national retail banks and internationally operating commercial banks. Moreover, the various stages of compliance procedures take place in different locations within the bank, either in the front office or in the back office, at the local bank or national and international financial districts like the City of London.
However, it is possible to discern certain ‘actors’ and ‘roles’ that participate in ensuring compliance. At the core of a bank’s compliance policy are specialized back office departments, such as ‘Legal’, ‘Compliance’ and ‘Security and Intelligence’. These departments shape the bank’s compliance policy by developing procedures and processes, giving advice and monitoring. However, each bank designs its own organizational structure and may, for instance, decide to merge the Legal and Compliance departments. In addition, each bank makes its own decisions regarding the tasks of each department and the division of tasks between the front office and the back office. Bearing this in mind, the tasks of these three departments can be described as follows.

The Legal Affairs department interprets the law at the most abstract level. When, for example, the FATF (Financial Action Task Force) requirements, the EU’s Third Directive and the national AML/CFT law differ slightly on certain definitions, the Legal department interprets these differences and tries to correctly adapt the bank’s compliance policy (interview 16). The Legal Affairs department also gives legal advice with respect to specific clients or practices. For instance, a local office of a bank may ask advice about whether: ‘a Dutch bank can accept a Spanish bullfighter as a client when bullfighting is legal in parts of Spain but illegal in the Netherlands’ (interview 16).

The Compliance department translates legal requirements into internal CFT procedures and automated processes. They assess if products, processes or procedures are compliant with the law. To be more precise, this department develops, for example, the procedures for carrying out due diligence in accepting new clients. This department may also provide independent but non-binding advice in response to queries from the front office, for instance with respect to clients labelled as ‘high risk’. Another task that is sometimes taken up by Compliance departments is monitoring the implementation of advice and guidelines within the bank.

The Security and Intelligence department analyses risks with regard to products, clients and countries. They assess whether risk indicators and scenarios operating in risk analysis software need to be changed, and if new criteria need to be added. This work is done on the basis of a range of information, which includes newspaper articles, Internet searches, reports of NGOs, governments and international organizations, guidelines published by (inter)national bodies and internal data held by banks.

The front office or ‘business’ is the primary agent responsible for the application of the CFT policy. When a new client, whether an individual or a multinational company, presents itself at a bank, account managers and money-laundering reporting officers
(MLRO’s) carry out the due diligence procedures set out by the Compliance department. Once the client is accepted, they are also responsible for monitoring their client’s transactions and for periodical review of the client. At each stage, risk assessments are carried out and clients or transactions are assessed as being low/normal risk or high risk. ‘Business’ interacts with and can ask for assistance of the Legal and Compliance departments.

When account managers and MLRO’s have suspicions with regard to a client or a transaction, they usually report this transaction internally and ask for advice from the Compliance department, which may in some cases even lead to direct involvement of the board of governors of the bank (interview 14). If further investigation leads to confirmation of the suspicion, the relevant department within a bank, often the Compliance or the Security and Intelligence department, may decide to send a suspicious transaction report (STR) to the national FIU. Such units are responsible for investigating the STRs and for taking further judicial action if needed. Furthermore, FIUs may also exchange information on suspicious transactions with FIUs in other countries, for instance, through FIUnet, a platform for enhanced cooperation between European FIUs sponsored by the European Union, or the Egmond Secure Web, an initiative from the Egmond Group of FIUs that fosters cooperation between FIUs worldwide.

In addition, national supervisory authorities such as Central Banks or national Financial Services Authorities evaluate and ensure compliance. Financial Authorities regularly visit banks or request information to assess (on a risk-sensitive basis) whether regulated entities have correctly implemented and executed (specific aspects of) the AML/CFT law. In the Third Directive, particular attention is given to the supervision of compliance, and it also introduces a section on penalties in case of non-compliance (Van den Broek, 2011a, p. 177). The EU-wide introduction of minimum standards for enforcement of compliance illustrates the seriousness of the theatre. Depending on national legislation and the nature of the infringement, sanctions may include a warning, blacklisting of compliance officers, or a fine. This last was the case for the Royal Bank of Scotland, which received a fine of £750,000 from the British Financial Services Authority for breaching AML/CFT rules (Financial Services Authority, 2002). Although it can be disputed whether the amount of the fee is dissuasive for a bank like RBS, the reputational damage to the bank has resonated throughout the international financial sector.

Finally, two more actors can be identified: banking customers and, in line with the previous chapter, the producers of due diligence software, as well as the software itself. While the transactional and personal data of customers are at the core of the AML/CFT compliance
policy, customers have only a marginal or ‘walk-on part’ in the theatre of compliance. Apart from delivering input to the compliance apparatus in the form of transactions or newly requested services, customers do not play a role. In fact, they are not supposed to be aware of the compliance procedures. Hindrance of ‘normal’ financial behaviour by identification and monitoring procedures should be minimized, while suspicious transactions and clients are to be silently flagged within the system of the bank or reported to the national FIU. In this latter case, the Third Directive, like its predecessors, explicitly prohibits informing the customer. With regard to the software used for monitoring transactions, the products developed by companies such as Fiserv, Bloomberg, Dow Jones and Wordcheck have become essential to being compliant with AML/CFT legislation. As discussed in the following sections, the design of these products influences the script and the performances within the theatre of compliance.

Considering all the different actors populating the stage, it may be noted that the numbers of actors involved can vary enormously according to context. A small savings bank may have only one or two persons responsible for compliance and legal issues (interview 20). The main office may be located in a stately home in a medium sized provincial town. At big international banks, on the other hand, each of the three back office departments may consist of 60 to 80 people (interviews 14, 16) working in big open-space offices at the main office in the heart of a financial district. The number of employees involved in AML/CFT-related tasks rises to between 500 and 1000 when including all the local branches of big banks, and often over 2000 when one takes into account internal auditors and tasks related to risk management (Favarel-Garrigues et al., 2009, p. 8). Likewise, the numbers of staff that analyse STRs within a FIU strongly differ. To give an impression of the differences, according to a 2005 IMF report the FIU of Slovenia employs 17 persons while 120 persons work for the British FIU (IMF, 2004, p. 12, 15). In 2008 the FIU in France employs approximately 70 persons (interview 5, see also Favarel-Garrigues et al., 2008), in the Netherlands 60 persons (interview 2) and that of Malta only four persons.39

While in the past banks have been reluctant to enforce AML compliance policies strictly, their attitude has changed over the last decade, especially since 9/11. Awareness that banks can be abused for terrorism financing or criminal activities is very high, and the commitment to defend the bank against this is very high too. Interviews with actors dealing with AML/CFT compliance within banks demonstrate that banks find it very important to be compliant. Many interviewees express a sincere concern about the damage terrorism and its financing do to society, and more importantly, the reputational risk of banks. They feel that
banks have a ‘moral obligation’ to fight terrorism financing and protect society (interviews 14, 16, 21). While some are sceptical about the efficiency of the Third Directive, all bank employees interviewed believe it is useful to have a barrier in place to make it more difficult to transfer money through the regular banking system. Moreover, it is highlighted that banks have no choice but to comply. Banks fear being publicly associated with terrorism, crime, dictators or other negative press since they are highly dependent on the public’s trust in their integrity. In the words of one bank employee: ‘you don’t want to open the morning newspaper reading on the front page that [your bank] is providing services to Osama Bin Laden or to President Mugabe’ (interview 14).

The cost of implementing the Third (and earlier) Directives and developing a compliance apparatus demands significant investment. This comprises not only the hire of specialized compliance officers, legal experts and security analysts, but also continuous staff training, the occasionally reliance on external expertise, and investment(s) in risk analysis and due diligence software. These software packages, which provide, for instance, data on blacklisted people and PEP’s, may ‘cost around 15,000 Euros per package’ (interview 21). Another estimate is provided by the British Banking Association: they believe that the overall annual cost of compliance with AML/CFT regulations is £36 million per individual institution (House of Lords, 2009a, p. 21). Yet it is difficult to assess the total costs and benefits of compliance with the Third Directive with any exactitude. Some interviewees estimate that the costs are ‘really enormous, and the (unintended) benefits, in terms of increased knowledge of customers and hence better marketing opportunities, are only marginal’ (interview 14). Others believe that ‘it is hard to assess but it might be the case that commercial benefits are equal to the additional costs of compliance’ (interview 17).

To conclude, the analysis of the stage shows that decision-making or, more generally, the exercise of power is dispersed over a range of actors across the public (FIUs, supervisory authorities) and the private sectors (banks). Further fragmentation takes place within institutions, such as the banks, and over different geographic locations. Moreover, the number of actors involved, their roles, their location, and the costs of compliance differ for each bank. This means that compliance with the Third Directive and other national and international CFT guidelines, gives rise to a field of governing in which participants have very specifically assigned responsibilities and powers that are however, non-transparent and difficult to assess by outsiders.
6.5 Script and Scenarios

Despite the variety of ‘stages’ on which AML/CFT compliance takes place, there is one common ‘script’ for being compliant set out in the Third Directive. This script consists of the Customer Due Diligence (CDD) procedures and practices that have been developed as part of the bank’s internal risk-based AML/CFT compliance policy. One aspect of the script is the use of scenarios, for instance those proposed by the FATF, against which transaction patterns are matched through the use of specialized software. An examination of the script and scenarios used for complying with counter-terrorism financing legislation highlights how assumptions about terrorism financing are translated into techniques of governing, and draws attention to the philosophy underpinning the governing of the fight against terrorism financing. For analytical purposes, the script (hence CDD) can be divided into two parts. The first concerns customer identification procedures that must be carried out when accepting or periodically reviewing a client. The second part of the script deals with transaction monitoring, which is a continuous activity. Both parts are structured by the risk-based approach introduced in the Third Directive.

6.5.1 Customer Due Diligence Part One: Customer Identification

In the First and Second Directives, the ‘Know Your Customer’ (KYC) principle was a central element. According to this principle, banks and other institutions in the financial services sector were required to know the identity of their customers and their transactions. This implies that they have ‘the duty to identify their customers and the corollary duty to keep records of identification and transactions’ (Mitsilegas, 2003, p. 69). In the Third Directive KYC has been replaced by more detailed and differentiated identification requirements under the notion of Customer Due Diligence (CDD).

Originally, due diligence was undertaken in case of corporate mergers and acquisitions. It entails a practice ‘through which the parties to a merger spend time checking the balance sheets and legal histories of their potential partners before closing the deal’ (Maurer, 2005, p. 476). These practices have also been introduced in offshore finance, where they involve ‘checking the details of a person’s or corporation’s identities against potential wrongdoing’ (ibid.). This same definition can be used for customer due-diligence procedures for the purpose of combating the financing of terrorism.
At the start of a business relationship, CDD procedures consist of information gathering via a face-to-face or telephone conversation on basis of a standardized questionnaire or an (online) application form. One objective of this procedure is to find out the purpose and the intended nature of the business relationship with the customer. It enables the bank to ‘predict with relative certainty the types of transactions in which the customer is likely to engage’.⁴⁰ ‘Of course we also learn a lot from this and there are commercial advantages of knowing your customer’ (interview 14). However, the CDD procedures do not appear to be an efficient preventive tool when it comes to uncovering new terrorists as yet unknown. Despite questions about the client’s intentions in opening a bank account, it is very unlikely that a terrorist will reveal his plans. As mentioned by a bank employee ‘of course a terrorist will not indicate that he wishes to open a savings account to save for explosives’ (interview 16).

Another objective is to establish the client’s identity or the beneficial owner of a company on basis of a reliable and independent source (Handoll, 2006, p. 153). The required documents for this differ among EU member states. For instance, the UK does not (yet) have an ID-card, while in most other European countries, a copy of an ID-card is required for opening an account or passing financial transactions. However, even when ID cards are used, these may be false or the translation of the identity of the consumer from another alphabet can provoke confusion. ‘Focussing on names is difficult as the translation from Arabic into European letters often leads to different ways of spelling a name’ (interviews 2, 20). It happens that ‘the database stores data of one and the same person under 14 different spellings’ (interview 2). In the case of companies, proof of registration with the Chamber of Commerce is often requested to establish the legal identity of the company. A risk assessment is carried out on the basis of the information provided and the customer data are also automatically matched against various blacklists.

In the case of combating terrorism financing, the most important blacklists are the UN, EU and national ‘terrorist lists’. The occurrence of a match against these lists should prohibit banks from doing any business with the client. However, interviewees confirm that hits against the terrorist lists hardly ever occur. Those mentioned on the list will simply not attempt to do any business with banks themselves or will assume a false identity. Concerning terrorists that have not yet been identified, these lists will obviously not be of use, as their names will not be included. Hence, in addition to the many important problematic aspects of blacklisting raised by legal scholars, notably with regard to due process and the international legal framework (i.a. Guild, 2008, 2010), one may ponder the implications of having to check all clients against lists while never provoking a hit.
Subsequently, clients are labelled as either low/normal risk or high risk through a system of points calculated by risk-analysis software (interviews 14, 15). An individual can for instance be labelled high risk when his or her name matches a name on Worldcheck’s database of Politically Exposed Persons (PEP), worth 75 points. As mentioned above, all foreign political, military and judicial leaders and their inner circles are to be considered PEPs. Usually these people are not terrorists, but they may also have a link to terrorism, be involved in corruption or engage in organised crime. It is, however, not forbidden to accept them as a client. Moreover, it is possible for a client to be considered a PEP at one bank and not another, because ‘the PEP software packages sold by for instance Bloomsberg or Dow Jones do not contain the same names and banks may also add new PEPs to their monitoring system’ (interview 17).

Labels are also assigned on the basis of the products used by the client. Opening a savings account, for instance, is considered low risk and is worth zero points. Companies might be indicated as high risk when they do business with high-risk countries. For illustration, an internal document of an international bank shows that (at least in one particular instance) this bank considered 69 countries as being high risk, while only 19 countries, of which only 9 are EU member states, were considered low risk (tables 6.3 and 6.4). This means that a slightly higher risk score is attached to transactions involving one or more of the 18 medium risk EU member states. Companies are also assessed according to their sector of activity. According to internal documents of this same bank, an agricultural firm is for instance rated at zero points; a convenience store rates 30 points and a money services business 75. On basis of the scores on these and other criteria, a score is calculated defining whether the client represents a low or a high risk.

However, the assumptions underpinning the risk-based approach are problematic in some respects. Although the attribution of these risk scores provides a semblance of support for the calculability of terrorism financing risks, the detection of potential terrorist financiers by means of risk analysis entirely depends on the assumption that terrorists display behaviour different from other customers. However, it has not been proven that this is actually the case. Consequently, it means that if terrorists and their financiers do not display different behaviour they will never be detected. In the words of a representative of the banking sector ‘if a yet unknown terrorist opens a savings account at our bank we will probably not detect this because it does not differ from something you and I could do’ (interview 27).
High Risk Country List

The following countries are considered high risk by one London bank, and therefore, any direct or indirect relationship a customer of this bank has with any of these countries must be noted in the Customer Due Diligence Questionnaire.

<table>
<thead>
<tr>
<th>Country</th>
<th>Country</th>
<th>Country</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>Afghanistan</td>
<td>East Timor</td>
<td>Lebanon</td>
<td>Sao Tome Principe</td>
</tr>
<tr>
<td>Angola</td>
<td>Equatorial Guinea</td>
<td>Liberia</td>
<td>Serbia</td>
</tr>
<tr>
<td>Azerbaijan</td>
<td>Eritrea</td>
<td>Libya</td>
<td>Sierra Leone</td>
</tr>
<tr>
<td>Bangladesh</td>
<td>Ethiopia</td>
<td>Macedonia</td>
<td>Solomon Islands</td>
</tr>
<tr>
<td>Belarus</td>
<td>Gabon</td>
<td>Malawi</td>
<td>Somalia</td>
</tr>
<tr>
<td>Bolivia</td>
<td>Gambia</td>
<td>Maldives</td>
<td>Sri Lanka</td>
</tr>
<tr>
<td>Bosnia-Herzegovina</td>
<td>Guinea</td>
<td>Mongolia</td>
<td>Sudan</td>
</tr>
<tr>
<td>Burkina Faso</td>
<td>Guinea-Bissau</td>
<td>Montenegro</td>
<td>Syria</td>
</tr>
<tr>
<td>Burundi</td>
<td>Guyana</td>
<td>Myanmar (Burma)</td>
<td>Tajikistan</td>
</tr>
<tr>
<td>Cambodia</td>
<td>Haiti</td>
<td>Nepal</td>
<td>Togo</td>
</tr>
<tr>
<td>Cameroon</td>
<td>Iraq</td>
<td>Nicaragua</td>
<td>Turkmenistan</td>
</tr>
<tr>
<td>Central African Republic</td>
<td>Ivory Coast</td>
<td>Niger</td>
<td>Uganda</td>
</tr>
<tr>
<td>Chad</td>
<td>Kazakhstan</td>
<td>North Korea</td>
<td>Uzbekistan</td>
</tr>
<tr>
<td>Comoros</td>
<td>Kenya</td>
<td>Pakistan</td>
<td>Venezuela</td>
</tr>
<tr>
<td>Cuba</td>
<td>Kyrgyzstan</td>
<td>Palestine</td>
<td>Yemen</td>
</tr>
<tr>
<td>Democratic Republic of Congo</td>
<td>Laos</td>
<td>Papua New Guinea</td>
<td>Zambia</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Republic of Congo</td>
<td>Zimbabwe</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 6.3 Source: Internal Memorandum an internationally operating bank in London. (May 2010).

Low Risk Country List

The following jurisdictions are considered low risk in the same bank.

<table>
<thead>
<tr>
<th>Country</th>
<th>Country</th>
<th>Country</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antarctica</td>
<td>Denmark</td>
<td>Netherlands</td>
<td>Switzerland</td>
</tr>
<tr>
<td>Australia</td>
<td>Finland</td>
<td>New Zealand</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Austria</td>
<td>France</td>
<td>Norway</td>
<td>United States</td>
</tr>
<tr>
<td>Belgium</td>
<td>Iceland</td>
<td>Singapore</td>
<td>Vatican City</td>
</tr>
<tr>
<td>Canada</td>
<td>Luxembourg</td>
<td>Sweden</td>
<td></td>
</tr>
</tbody>
</table>

Table 6.4 Source: Internal Memorandum, an internationally operating bank in London. (May 2010).

Furthermore, the level of risk given to a transaction or client is not simply the outcome of an objective computerized risk assessment. The number of points assigned to each product, country or sector of activity, and on which the risk calculations are based, are defined by banks themselves and they can be modified. Moreover, ‘there is quite some room for manoeuvre within the definitions of the law. Which means that compliance officers have to make choices on how they appreciate a situation’ (interview 9). High risk scores, for instance, do not automatically lead to reporting to an FIU or the closure of a business relationship. In practice, it is possible and happens that customers are labelled high risk and they are not rejected. As long as it is not strictly forbidden by law to do business with a specific customer, it is seen as part of the ‘commercial freedom’ of a bank to either accept or reject a customer. While these risk calculations remain attached to the client’s file, and past risk flags always

200
remain visible, bank personnel have some discretion to judge these risks themselves and may
decide to ignore high-risk flags, or to scale clients back from high risk to normal risk.

On the other hand, banks and financial services providers may also decide not to
engage in business activities with individuals or businesses for other reasons than official
blacklisting or high-risk scores according to established risk criteria. For instance, in 2010,
Bank of America, Visa, MasterCard, Western Union and PayPal decided preventively to
refuse all payments to Wikileaks (Arthur, 2012). Another example is the refusal of two Dutch
banks, Rabobank and ABN AMRO, to open an account for Marthijn Uittenbogaard, a
publicly known advocate for the acceptance of paedophilia (Heijne, 2012). Hence, the due
diligence procedure as a whole, and risk assessments in particular create a grey zone in which
banks themselves ‘can decide how tough they want to be on certain criteria [of the compliance
policy]’ (interview 14) and which considerations in addition to those specified in the Third
Directive they take into account.

This implies that risk analysis does not reflect an objective reality, but depends on the
interplay between the officer assessing flagged transactions or customers and the compliance
software. A hearing on money laundering and terrorism financing before the select committee
on the EU of the House of Lords is very insightful in this respect and is worth quoting at
length. In response to the question on what basis suspicious transactions are to be reported,
the Deputy Chief Executive of the British Bankers’ Association stated:

(…) it is a suspicion based regime. (…) You rely on your instincts; you have the
framework of the law; you have the framework of the banks’ own methodology for
assessing risks, whether it is the type of customer or the product they are taking, or the
country in which they are situated, and that is the suspicion, it is the experience of the
person concerned that triggers that (2009a, pp. 26-27).

Responding to the question on whether reports can be made ‘on that feeling’, she responded,

Absolutely; you are required to, that is what the law requires (…) We have to. The law
requires that if you suspect you must report (ibid., p. 27).

These responses not only highlight the involvement of human considerations as part of risk
analysis, but they also emphasize the need for bank employees to share the norms and ethical
standards of the bank and make their decisions accordingly. ‘The risk-based approach
requires discipline and confidence in your employees [making the security decisions] because
[the bank] counts on their opinion, your objectivity’ (interview 14).

This analysis of the customer due diligence procedures undertaken at the start of, or during, a
business relationship with a client shows that, much like border security, these consist of
multiple repetitive and protocolled acts of ‘scanning, screening and verification’. However, the detailed description of these acts to ensure compliance shows that the risk-based approach is not merely a simple and straightforward calculation of risk-scores. In order to know the customer, a significant portion of the CDD procedures rests on a subjective estimation and weighting of information regarding the customer’s identity and intentions. Hence, despite the apparent objectivity of the calculation of risk scores, subjectivity is an important aspect of the risk-based approach, because personal conviction, professional instincts and knowledge about terrorism financing partly influence the assignment of risk scores and the consequences of these scores.

6.5.2 Customer Due Diligence Part Two: Transaction Monitoring

In addition to the procedures concerning the acceptance of new clients, the continuous monitoring of customer transactions is another important part of the script of the theatre of compliance. Currently the banking industry passes through 550 transactions a second (House of Lords, 2009a, p. 14). To monitor all these transactions on a risk-based basis implies that ‘during the night a bank’s computer system matches enormous datasets with thousands of customer requests each day, against a number of detection, monitoring and filtering systems’ (interview 14). The continuous risk assessment of customers’ transactions is a very similar process to the initial risk assessment that is part of the customer identification procedures. Different aspects of a financial transaction are translated into risk criteria and are given a certain number of points. Depending on the total number of points, a transaction may emerge as ‘risky’ or ‘requiring further attention’ on the computer screen of a Money Laundering Reporting Officer or an account manager. On average, 2% of all transactions produce a hit in the system and require further attention, meaning that the customer is asked to provide additional information, which is then recorded in the system.

One of the difficulties of detecting terrorism financing through the risk assessment of transactions is the modest and strongly decreasing cost of an attack. The risk-based approach entails checking the amount of each transaction; transactions above a certain amount will provoke a hit in the system. The Third Directive, for instance, prescribes that transactions above € 15,000 are to be considered risky. However, the estimated cost of the 2004 Madrid attacks was only € 10,000, and costs for the 2005 attacks in London were only one tenth of that amount. Furthermore, these funds were raised completely through legal means such as salary and savings money (Buchanan, 2006).42 ‘These amounts cannot be detected unless you
allow for screening everyone’s expenses up to a few Euros at the local groceries store. It does not work’ (interview 15).

Aside from assessing transactions against specific risk criteria, all transactions of each client are also checked against scenarios. This means that:

certain patterns are expected. Especially with regard to private customers, 95% of them have the following pattern: at the end of the month money comes in, on the first day of the month rent or mortgage, gas, electricity and insurance bills are paid and the rest is used for consumption and perhaps savings and an occasional holiday. This is considered as a normal process (interview 14).

A fully automated process is run by specialized risk monitoring software such as ERASE, a program developed by a Dutch company NetEconomy, one of the market leaders in this sector and since 2007 part of the American company Fiserv. There are also specific scenarios for businesses. A normal pattern for a bakery is to make regular purchases of flour and eggs, for instance, and to earn income within a certain range. If a bakery suddenly has an enormous increase in income or requests services that do not correspond with its business, this can provoke a hit or red flag in the system.

While the object of risk assessments involving specific criteria and scenarios is to enhance control over financial transactions, it must be emphasized that they also entail a vision of how a customer’s ‘normal’ financial life should look. When customers correspond to the scenario, their transactions pass unnoticed through the system. If their transactions differ from the scenario, a ‘risk flag’ or a ‘hit’ is produced. This is for instance the case ‘when suddenly receiving three times 17,000 Euro in four weeks’ (interview 14) or when ‘suddenly receiving 50,000 dollars from an account in the US’ (interview 17). Or ‘when we see that money comes in several times a month or we see that transactions are made to foreign countries, frequent cash transactions or rapid movements of funds, these are not normal for an average household’ (interview 14).

On the basis of reports by international organizations such as the FATF, the World Bank and the IMF, commercial companies have also developed specific scenarios for detecting terrorist funding. However, banks seem sceptical about these scenarios. ‘We [automatically] check against the proposed scenarios but there are no hits’. ‘Moreover it is impossible to make scenarios of terrorists because every attack is different. There is no profile of a terrorist’ (interview 14). The FATF also acknowledges that the diversity and multifaceted nature of terrorists’ financial activity makes it challenging to establish general alerts and indicators that suggest a particular transaction presents a risk of terrorist finance. They do, however, propose that large cash or electronic transfers and cross-border currency
transactions might be signs of terrorism financing (FATF, 2008, p. 29). Other indicators that are often found in revealing terrorism financing cases are the sending or reception of funds by international transfer from or to locations of specific concern, atypical business or account behaviour, transactions linked to a charity organisation, large scale cash transactions, and media coverage of account holder’s activities (ibid., p. 31).

When a hit occurs and a transaction is considered suspicious, banks fill out a suspicious transaction report (STR) indicating the characteristics of the transaction (sender, beneficiary, currency, amount…) and the type of suspicion, which is sent (electronically) to the national FIU. At this moment, the transaction moves from the private sector to the public sector. The FIU stores the STRs it receives in a huge database. In countries such as the UK and the Netherlands, the number of STRs received daily by the FIU exceeds their capacity to analyse. ‘It is impossible to look at all STRs’ (interview 2). Subsequently, officers of the FIU investigate STRs that are flagged on a risk-sensitive basis similar to the approach adopted by banks. ‘We make lists of risk criteria, to detect terrorism, for instance, it is important to look which countries are involved, and the STRs that receive most points on basis of the risk assessment are investigated’ (ibid.).

However, cooperation between the public and private sectors goes beyond the mere reporting of suspicious transactions. The FATF encourages banks and FIUs to regularly exchange information on terrorism financing. Specific cases or trends found in the financial intelligence gathered by FIUs could provide clues for the terrorism financing scenarios that are developed by banks themselves, while banks could give feedback on the results obtained from the scenarios suggested by a FIU (FATF, 2008). However, this cooperation is still to be developed. Although the EU Financial Intelligence Unit Platform has dedicated attention to this issue (EU Financial Intelligence Unit Platform, 2008) and some FIUs have started to strengthen their relations with reporting entities, bank employees stress the lack of feedback they receive regarding the STRs they send to the national FIU (interview 2). In the UK, the Serious Organised Crime Agency (SOCA) has increasingly provided feedback to banks and other reporting entities with regard to the reports they have made and new trends that have been observed. However, so far, reporting entities are qualifying the feedback as ‘not very helpful in that they are too general’ and claiming that it ‘tends to confirm what the industry already knows’ (House of Lords, 2009a, pp. 30-31).

Moreover, while the lack of terrorism financing hits might be understood as reassuring news about the threat of terrorism to our society and the integrity and soundness of the financial system, it does create a little unease within some banks. It leads to what has been
called ‘defensive reporting’ which the risk-based approach aimed to avoid by introducing more flexible reporting standards. If banks have doubts about a suspicion, they decide to report and be on the safe side of the law. Another reason banks report defensively is to satisfy monitoring authorities. According to a bank employee: ‘every year we send one or two “defensive reports” to the FIU’. ‘We know it is not a terrorism case but we do not want to mark zero detections in our statistics and if we report some they notice at least that we are not sleeping’ (interview 15). The British Bankers Association even explains that they have some sort of agreement with SOCA with regard to separating the wheat from the chaff in the STR reports that they send (House of Lords, 2009a).

In sum, examining the script and scenarios of the theatre of compliance makes the rationality of governing the fight against terrorism financing visible. Customer Due Diligence procedures prescribe how the customer must produce and represent him or herself to gain access to the formal financial system. Risk assessments and scenarios call into being certain ideal types of normal financial behaviour to which the financial lives of ordinary customers should correspond, and produce risk flags in response to suspicious or unusual transactions. The assumptions regarding what is potentially a sign of terrorism financing are strongly shaped by the FATF special recommendations on this topic, and are occasionally informed by financial intelligence from FIUs. These assumptions are integrated in a bank’s risk-analysis software and transaction scenarios and structure the fight against terrorism financing. In practice this means an increase of surveillance on citizens and businesses that make international transactions, that transfer money to charities, or that make large (cash) transactions. The quality and follow-up of decisions taken on the basis of these scripts and scenarios depend on the relations between public and private authorities. The adoption of the theatre metaphor and the examination of the practices of the Third Directive in terms of script and scenarios also draws attention to the subjective and controversial aspects embedded in these practices.

### 6.6 Performance

Performance can be defined in several manners. In conventional economic and financial analysis, performance is an important indicator. It usually intends to make the achievements of businesses or government agencies measurable, providing ‘a logic of calculability and an appearance of scientific objectivity’ (De Goede, 2005, p. 3). Such
indicators are, for example, customer satisfaction grades, rising stock prices, or numbers of received STRs. From this perspective, the performance of the Third Directive can be expressed in terms of effectiveness with regard to the objectives of the Directive.

Understood in reference to the theatre, performance has increasingly been used as a valuable concept in social and political analysis over the past two decades (Nield, 2006, p. 63). De Graaf (2010), for instance, assesses the performance of combating terrorism in different countries. In her study, performance does not refer to the effectiveness or success of counter-terrorism policies, but rather entails the presentation and perception of counter-terrorism measures. Performatory power can be defined as the imaginative power and persuasiveness of a counter-terrorism policy and includes parameters such as agenda setting, public support and discourse (De Graaf, 2010, p. 139). Performative power is high when political and public opinion are strongly mobilized. This section examines the performance of the Third Directive from both the economic and the theatrical perspectives.

A first objective of the Third Directive is to detect terrorism financing and identify terrorists and their associates. The number of STRs falling under terrorism financing may offer a rough idea of the effectiveness of the Directive in combating terrorism (and of compliance with the Directive). It must be stressed, however, that the FIUs of EU member states do not always publish their statistics in comparable formats, they do not always indicate the number of reports related to terrorism financing separately; these numbers also include reports that do not lead to prosecution. For instance, the UK FIU, SOCA, reports that 247,601 Suspicious Activity Reports (SARs) were reported in 2011, of which 662 (less than 0.25%) were related to terrorism financing. Approximately 73% of all reports were filed by banks (SOCA, 2011, p. 52). The 2010 annual report of the Dutch FIU indicates that it received a total of 183,395 STRs in 2010 and notices that ‘with regard to the financing of terrorism several interesting cases have been shared with investigation [officers]’ (FIU-NL, 2010, p. 11). However, the report does not provide detailed numbers on terrorism financing as the Dutch Ministry of Finance has decided to suppress the box indicating a suspicion of terrorism from the STR form in 2005, to alleviate the administrative burden on reporting entities (interview 2). The French FIU, TRACFIN, notes that very few cases of terrorism financing are detected; 17 cases were transferred to the judicial authorities in 2007, 5 in 2008, 9 in 2009 and 6 in 2010 (TRACFIN, 2011). According to a representative of the Polish FIU, it had received only one STR in relation to terrorism financing within that year, and after investigation it appeared to be a false alert (EIPA, 2008). However, given the extremely low incidence of terrorist acts, it is difficult to conclude whether the few potential cases of
terrorism financing that are reported, and the sporadic prosecution on the basis of STRs are to be interpreted as a success or not.

The opinion of participants involved in reporting suspicious transactions on the performance of the Third Directive with regard to detecting and identifying terrorism financiers is rather more negative. According to one bank employee ‘it is a utopia to believe we can detect terrorists through transaction monitoring. This policy is symbolic, the person that holds the illusion that this works does not live on this planet’ (interview 14). In hearings before the House of Lords, the British Law Society and the British Banking Association expressed that they ‘continued to have concerns as to the effectiveness of the scheme’ (House of Lords, 2009a, p. 4). Also, FIUs are critical of the effectiveness of the system, especially due to the overload of information it creates. ‘What we attempt to do is not finding a needle in a hay stack but finding a needle in a stack of needles’ (interview 2). Similarly, on the level where guidelines and legal frameworks are designed, it is known that results are limited. EU officials do not appear to be convinced by the effectiveness of the Directive (interview 10). In a similar vein, a recent FATF report acknowledged ‘that financial institutions will probably be unable to detect terrorist financing as such’ (FATF, 2002, p. 3).

The other objectives of the Third Directive are even more difficult to assess quantitatively. As mentioned briefly in the introduction of this chapter, the deterrent effects of the Directive cannot be easily measured, as this implies counting terrorism-related transactions that did not take place (in the formal financial system). It is possible that the dissuasive effects of the Directive have resulted in a shift to other means of transferring or accumulating money outside those services and businesses subject to the Third Directive. In that case, the Directive has achieved its objective of denying terrorists access to the formal financial sector, but terrorists may still have access to alternative means of financing. On the other hand, it is possible that terrorist financiers continue to make use of banks and financial services but avoid detection by using false identities and leading financial lives that do not raise red flags.

Likewise, the more general objectives of the Third Directive, being the stability and reputation of the financial sector and confidence in the financial system, cannot easily be judged in terms of effectiveness. The number of terrorism related STRs does not reveal the total terrorism financing transactions that take place in the formal financial system and it is virtually impossible to know what percentage of terrorism transactions is intercepted. Moreover, it can be questioned whether the sums of money involved in financing terrorism would indeed suffice to destabilize the global financial system. In fact, similar to the point
raised by Nield (2006) with respect to the border, the Third Directive does not objectively regulate existing norms of integrity or reliability, but contributes to producing the idea of a sound and clean financial sector through the creation and performance of AML/CFT practices.

Considering the performance of the Third Directive in theatrical terms helps to explain why the theatre of compliance continues even when performance in economic terms is low or proves to be elusive. First, the monitoring and reporting requirements of the Third Directive are considered a barrier making it, in theory, more difficult for terrorists to gain access to the regular banking system. It is precisely the extensive and strict requirements, the establishment of public and private structures assessing suspicious transactions and the supervision of compliance that contribute to a belief in the control, integrity and soundness of the financial sector, irrespective of actual results. This also touches upon Schneier’s argument of the ‘security theatre’ in which counter-terrorism policies aim to reassure the population.

At the level of banks, respecting AML/CFT regulations and maintaining good relations with supervising authorities are part of the communication strategy for presenting the bank as trustworthy and solid. Banks have invested heavily in being compliant and want to avoid reputational damage at virtually any cost. According to Tsingou, the largest global financial players even have a business interest in maintaining the status quo, as they helped shape the current standard that ‘affects small institutions disproportionately,’ as their means to make the required investments in compliance are more limited (2010, p. 183). In addition, banks seem to derive at least some benefit from the CFT requirements, as better knowledge of their customers generates additional marketing opportunities.

Already twenty years ago, banks such as the American Citibank understood the business opportunities of, at that time, Know Your Customer information. For instance, through transaction monitoring banks may notice that you inherited $50,000 and they can commercially anticipate on that by advising you what to do with this money (interview 17).

Hence, from a broader economic perspective, the theatre of compliance is also a power struggle of big banks and smaller ones, and it increases the power of banks over their customers.

Finally, there is a question of audience. The above may suggest that one of the audiences of the theatre of compliance is constituted by the supervising authorities that evaluate banks’ performance. The efforts banks undertake for being CFT compliant need to satisfy supervising authorities. However, supervising authorities can also be considered part
of the theatrical performance, in the sense that their opinion may (or may not) convey credibility and legitimacy to banks. From a broader societal perspective, the theatre of compliance is performed for the population, and increasing their feelings of security and their confidence in the current financial system. In this light, it is interesting to notice that this audience has no access to the stage, the script and the scenarios as described in this chapter. They cannot watch how CFT compliance is carried out, but it is crucial that the performance, in economic and in theatre terms, is convincing to them. The final section recapitulates how the Third Directive has created a new professional field, sets in motion new governing practices and addresses their implications.

6.7 Conclusion

The theatre of compliance metaphor offers a new and important approach for examining the daily governing practices that have been created to implement the Third Directive. It provides insights in the way public and private authorities cooperate to combat terrorism financing, in risk-based financial surveillance practices and the often overlooked implications of these new forms of governing.

The analysis of the stage of the theatre shows that the professional field which has emerged from the risk-based implementation of the Third Directive consists of both private and public authorities. Private actors, most notably banks, identify risky clients and monitor suspicious transactions, while public authorities either act upon the information delivered by the private sector or supervise the implementation of the Directive. The division of roles among the participants of the field and the design of the stage are of great importance. In daily practice, it means that a range of private professionals (developers of detection software, compliance officers within banks, legal experts…) are responsible for the filtering and pre-selection of the risky profiles and transactions through an accumulation of individual and fragmented decisions. Subsequently, these decisions structure the investigations led by FIUs and eventually the prosecution of terrorism financiers. Hence, by charging banks with the responsibility to combat terrorism financing, a shift has taken place as banks are now involved in national security questions and are even the first to make certain security decisions.

Moreover, the analysis through the theatre metaphor has also shown that it not indifferent whether the public or the private sector is responsible for combating terrorism. Although the argument that the private sector can combat terrorism financing more efficiently
and more cheaply on the grounds that it already possesses financial data has some legitimacy, it needs to be emphasized that a bank’s primary mission is not combating terrorism financing. While banks claim to feel a social and moral commitment with respect to combating terrorism financing, their first reflex is to not act as ‘unpaid criminal investigators’ (interview 14). In practice, this leads to a discrepancy between the Directive’s objective of combating terrorism financing and the banks’ objective of being compliant with CFT measures and calls the effectiveness of involvement of the private sector into question.

Furthermore, the responsibility of the private sector to detect suspicious clients and transactions and the diffused decision-making procedures across multiple departments within institutions lead to an almost complete lack of transparency and accountability. In the words of a representative of the British Banking Association: ‘there is a risk to the risk-based approach itself in that it does mean that banks have to make judgements, people have to take responsibility (...)’ (House of Lords, 2009a, p. 25). So far it is unclear to outsiders when decisions are taken and on the basis of what information. As the monitoring and reporting process are and must be entirely hidden to clients it is impossible for them to control, complain or appeal against a bank’s decisions. Yet, the fact that defensive reporting of fictive suspicious transactions takes place and may lead to erroneous inclusion in police databases makes the case for accountability all the more urgent.

The risk-based approach introduced in the Third Directive also gave rise to a mode of governing terrorism financing through supposedly objective and scientific calculations. Through the daily repetitive acts of matching profiles against watch lists, calculating risk scores and monitoring transaction scenarios and with the help of ‘smart’ software programmes, security is enforced and the future appears manageable. However, an analysis of the Third Directive from the theatre of compliance perspective destabilizes the idea of the risk-based approach as a neutral practice. It shows that the specific characteristics of this approach – mobile norms and high flexibility for implementation – are not uncontroversial.

The analysis of the script shows that risk analysis depends on the risk indicators that are themselves based on client and transaction information gathered by the bank, and on risk classifications produced by the bank or by specialized compliance software and consulting companies. Hence, risk analysis is not made according to some objective standard, but emerges from the information suitable for calculation, and from the subjective shared assumptions about terrorism financing (and other crimes) of the professional field. Moreover, decisions regarding the suspiciousness of transactions deemed risky and decisions to report transactions to the FIU are always made by human beings. As such, decisions about suspicion
and risk are in essence ethical and social rather than technological and mathematic. The risk-based approach relies strongly on the subjectivity of the participants of the field and the institutions they represent. Security decisions are taken on the basis of their experience and knowledge, which is partly based on international guidelines. This again means that security decisions taken within banks are rather opaque and can be controversial, as for example when similar cases might be treated differently by different banks or bank employees (interview 9).

Another principal characteristic of the risk-based approach is the flexibility of norms and practices to combat terrorism financing. Flexibility is, on the one hand, justified by the fact that the modus operandi of terrorists may continuously change, and the Third Directive covers a wide range of professions within which a great variety may also exist. Yet, the downside of the mobile norms and flexible implementation of the risk-based approach is that it introduces legal uncertainty and lacks transparency. The fact that, within the limits of the law, each bank can define its own compliance policy and makes its own risk assessments, makes it unclear how exactly banks monitor their clients, what criteria they have developed for assessing their customers, and how strictly they enforce these criteria. It can even lead to discrimination as compliance officers are supposed to make their decisions on their intuition and personal expertise. Moreover, customers (must) remain almost entirely uninformed about the fact that their data are continuously assessed and might be reported to Financial Intelligence Units without their being notified.

The shortcomings of the risk-based approach – lack of transparency and accountability – are important in the light of the finding that the Third Directive has a theatrical function in reassuring citizens and financial markets but is not well suited to combating terrorism financing. In fact, detecting terrorism financing through the monitoring of clients and transactions is very complicated. The cost of terrorist acts is relatively low and decreasing, the financing of an attack does not necessarily require atypical financial behaviour and the occurrence of terrorist acts is too rare and similarities between the methods of financing are too low to establish meaningful scenarios.

Finally, the findings of this chapter, as well as those of previous chapters, start from the basis of governance practices and new professional fields that have emerged in the name of the European fight against terrorism financing. In the next and concluding chapter, the findings of the two case studies will be discussed in relation to the broader academic debate over financial surveillance in Europe. Are the practices of the Third Directive and the TFTP best understood as examples of financial surveillance, as suggested by certain scholars? Moreover, both cases have shown that these new governance practices lead to a variety of not
only legal but also political and societal questions. The final chapter also discusses the extent to which the (financial) surveillance prism can make these wider implications of the fight against terrorism financing visible.
Chapter 7.

Financial Surveillance in Europe

Ten years after the 11 September 2001 terrorist attacks on the World Trade Center triggered a “War on Terrorism,” counter-terrorism policy needs to be properly evaluated, not least to ascertain whether the measures taken are based on evidence, or merely on assumptions.
—European Parliament Committee for Civil Liberties, 2011b

7.1 Evaluating Ten Years of War on Terrorism Financing

The tenth anniversary of the 9/11 terrorist attacks has led citizens, civil society and politicians to a call for an in-depth evaluation of the international War on Terror. In June 2011 for instance, the European Parliament adopted a resolution requesting that the European Commission undertake a study surveying the last ten years of European counter-terrorism policies. The study was meant not only to map existing measures and address their costs and effectiveness, but the EP also explicitly asked for an examination of: ‘whether the measures taken to prevent and combat terrorism in the EU have been evidence-based (and not based on assumptions), needs-driven, coherent and part of a comprehensive EU counter-terrorism strategy’ (European Parliament, 2011).

The present dissertation offers part of such an evaluation by examining how the fight against the financing of terrorism has taken shape in Europe. It started with the observation that the assumptions underpinning the global War on Terror have important parallels with Laplace’s demon. In particular, measures for combating the financing of terrorism are based on a data- or intelligence-led approach, which implies the analysis of massive sets of personal data by ‘smart software’ in order to detect suspicious transactions and prevent future terrorist acts from happening. The previous chapters have shown how professional fields and data-led governing practices have emerged, changed or expanded in the European Union in response to the prioritization of the fight against terrorism financing. Moreover, these chapters examined how the European fight against terrorism financing was framed, and drew attention to some of the societal and political implications of this fight.
A critical historical perspective on the question of how the European fight against terrorism financing took shape and became important in the EU was given through investigation of the genealogy of this fight. Chapter 3 shows that terrorism financing has not always been considered a vital arena for combating terrorism, but has gradually been framed as such since the 1980s. From the mid-1980s until the adoption of the 1999 UN Convention for the Suppression of the Financing of Terrorism, the perception of what constituted terrorism financing progressively broadened; eventually it became defined as a separate crime from the terrorism so financed. After 9/11, discourse on terrorism financing changed again, and terrorism became perceived as an act of war instead of a crime.

In addition, the genealogical analysis of the fight against terrorism financing also shows that the importance of combating terrorism financing must be seen in a broader political and societal context. Prior to the attacks on the World Trade Center, a few small groups of experts were concerned with terrorism financing as a problem requiring international governance, but other considerations were deemed more important – the deregulation of financial markets, the assurance of civil liberties, the absence of major terrorist attacks, and on-going discussions over the insignificance of the amounts of money involved in terrorism and the effectiveness of international sanctions. The 9/11 attacks disturbed the hierarchy of these different societal debates, as the urgency and importance assigned to terrorism increased tremendously and provided great momentum for the adoption of previously controversial measures.

This analysis has shown that the European CFT measures developed since 9/11 cannot be understood separately from earlier representations of and discussions over terrorism financing. It also emphasizes that the understanding of (combating) terrorism financing is not a linear process but evolves permanently and is subject to discussion, negotiation, improvisation and political struggle. In the two weeks following the attacks, for instance, it was not immediately or naturally decided what kinds of measures should be taken or which (inter)national institutions would be in charge of combating terrorism financing. Furthermore, this long-term analysis points to three important shifts that shaped the European fight against terrorism financing after 9/11. These include the securitization of terrorism financing, the focus on prevention of terrorism with the help of high-tech data-led practices, and the involvement of the private sector in questions of national security.

A theoretical framework for examining closely these post-9/11 forms of governing based on the use of ‘smart’ risk or link analysis software, great amounts of personal data, and the involvement of public and private authorities across geographic boundaries was
introduced in chapter 2. Building on literature from the fields of European Studies and Surveillance Studies, it is argued that the Foucauldian notion of governmentality and Bourdieu’s professional field can help us examine how power is exercised in the European fight against terrorism financing. Studying this fight as a European field of governing allows us to go beyond formal legal frameworks and pre-established institutions to consider a wider set of institutions, procedures, calculations, tactics and even objects through which power is exercised. It also draws attention to the production of meaning and the distribution of power in the fight against terrorism financing.

The Terrorism Finance Tracking Programme (TFTP) or SWIFT affair and the EU’s Third AML/CTF Directive were selected as case studies, representing the two most important policy initiatives for combating terrorism financing. In this final chapter, conclusions are drawn comparatively across these two cases, and the key findings of the dissertation are summarized in relation to the three themes set out in the theoretical framework: European security governing through public-private cooperation, preventative surveillance practices based on smart technology, and the collection of massive amounts personal data. The next section recapitulates how the two case studies share a number of characteristics key in the European fight against terrorism financing, and more generally the international War on Terror, and constitute examples of contemporary financial surveillance. The following sections show how the theoretical lenses of governmentality and the professional field, provided new insights with regard to the way in which power is exercised in the name of a European fight against terrorism financing. Section 7.3 discusses the empirical findings with regard to public-private cooperation and the proliferation of private sector power. Section 7.4 critically considers the high-tech and data-led governance practices of the fight against terrorism financing. Section 7.5 focuses on the collection of personal data and the findings of the case studies in light of the debate over the relation between liberty, in the form of privacy, and security. Finally, section 7.6 contrasts the considerations set out in the previous sections with the empirical findings regarding the effectiveness of these measures in preventing terrorism financing.
7.2 Two Cases, One Philosophy

At first, the case studies of the TFTP and the Third Directive seem rather different. Whereas the SWIFT affair led to a vivid outcry, both in the media and among (mainly European) politicians, few people beyond the banking and financial sectors were aware of the existence and scope of the Third Directive (Amicelle & Favarel-Garrigues, 2012). Moreover, the CFT provisions in the Third Directive are built on pre-existing anti money-laundering legislation, while the TFTP was initiated shortly after 9/11 and remained a secret and partly illegal programme for several years. Furthermore, the Third Directive concerns mainly the gathering and analysis of information on a national level within the EU, although the exchange of information among Financial Intelligence Units within Europe and internationally is not excluded, whilst the TFTP is an American initiative involving the transfer of (inter)national transactions towards US intelligence services. However, despite these differences, in their origins, purposes, methodology and institutional design, both programmes share and are exemplary of a common philosophy that characterizes many post-9/11 surveillance initiatives.

At first, the ‘origins’ of both programmes seem to differ sharply, since the Third Directive is a legal instrument while the existence of the TFTP was concealed and operated without a clear legal basis, at least with regard to European data. Yet, if we understand origins as ‘entstehung’ (Foucault, 1977, see chapter 3) it can be argued that both cases stem from a broader quest for customer identification and transaction monitoring already present in the 1990s. During that decade, the FATF requested that banks increase the quantity and quality of customer data they maintain in order to facilitate the War on Drugs. For this same purpose, the US authorities sought to access the SWIFT database in the 1990s, but were denied access at that time. In addition to increased data collection, the scope of the AML framework was also broadened from money laundering in relation to drugs to all kinds of ‘organised crime’, including terrorism. The attacks of 11 September 2001 provided a political ‘window of opportunity’ that reinvigorated existing arrangements (Den Boer & Monar, 2002, p. 21) propelling further expansion of financial surveillance practices. The political will to implement such programmes increased, as did the willingness of private companies (including banks and SWIFT) to cooperate with measures taken in the name of counter-terrorism and the pursuit of terrorist monies.
Another parallel between the Third Directive and the TFTP is the purpose for which the financial data are used. In both case studies, the primary aim is prevention of terrorism financing, or more generally, financial crime. Private authorities, most notably banks, gather personal financial data that are redeployed for security purposes. It is believed that with the help of specialized monitoring and analytical software programmes, suspicious (relations between) customers or abnormal financial behaviour can be identified and that known and unknown terrorist financiers can be detected at an early stage. These technologies are used for the production of more general financial intelligence. In the case of the TFTP, banks enter ‘raw’ data into the SWIFT database, of which a select part is analysed at a distance by US intelligence services. The Third Directive, on the other hand, imposes a responsibility on banks for assessing the risk posed by suspicious transactions and behaviour of their clients and reporting this to their national Financial Intelligence Unit. However, both case studies showed that the preventive powers of these approaches are limited.

Due to the many millions of daily transactions contained in the datasets, ‘smart software’ is crucial both to the TFTP and to fulfilling the obligations of the Third Directive. In order to be compliant with the Third Directive, banks are required to identify and to risk-assess their customers and transactions with the help of specialised risk-analysis software. This leads to a classification of low risk or high-risk customers and transactions about which the bank needs to make a decision. On the other hand, the SWIFT data are analysed through link analysis, which departs from the data of one customer and establishes links to people with whom the initial customer makes financial transactions. Despite the use of partially overlapping datasets, these two methodologies lead to different kinds of output; the former focuses on the degree of suspiciousness of a customer, while the latter establishes potentially suspicious relations between individuals.

Finally, both cases are based on a close cooperation between the public and private sectors. Although the participation of the private sector is imposed by governments, banks and other financial companies are now closely involved in shaping and facilitating financial surveillance. In the beginning of the TFTP, SWIFT prepared the data requests for the US Treasury and transferred the selected data through a so-called black box. This process continues, but is now monitored, and the demands of the Treasury assessed by Europol. In the context of the Third Directive, the monitoring of transactions, decisions as to the suspicious nature of a transaction, and the reporting of these transactions are all made within banks. In fact, compared to the TFTP, the provisions of this Directive constitute a much more comprehensive method of financial surveillance in the sense that banks not only assess
specific international transactions, but *all* transactions made by customers and other forms of contact with the client. In this sense, the measures taken under the Third Directive affect virtually the whole population, since it is very difficult to live without having a formal bank account in Western societies. The following sections deepen our understanding of this philosophy and its societal and political implications by thematically discussing the empirical findings of the case studies.

7.3 Public-Private Cooperation: the Proliferation of Private Sector Power

Our investigation of the EU’s fight against terrorism financing in terms of a professional field made the prominence of public-private cooperation in the fight against terrorism visible and emphasized the importance of including private authorities in an analytic model of European security governing. Examination of the implementation of the TFTP and the Third Directive has shown that the data-led and high-tech pursuit of the War on Terror relies on commercial databases and on a close interaction between the public and the private sectors. From these two case studies, four important inferences can be drawn with regard to the way in which power is exercised through public-private cooperation. Two of these findings build upon existing theorizations of financial surveillance, while two others provide new insights into public-private cooperation for security purposes.

First, and contrary to conventional concepts of surveillance, such as Big Brother or the panopticon, which depict the state as a central all-seeing eye watching over a population (for instance, Vlcek, 2007), the case studies show that financial surveillance takes place in a dispersed and fragmented manner and throughout society. In the name of the Third Directive, the monitoring and assessment of clients and transactions takes place in a patchwork of banks spread over the globe and ranging from the local bank in a little town to the headquarters of internationally operating banks in leading centres of global finance. In the case of the TFTP, the actual analysis of the information takes place at a CIA facility in the US. However, neither the CIA nor the US Treasury can be understood as a centralized form of surveillance, as they do not themselves collect the financial data and the data they use are not primarily collected for security purposes. Banks in virtually all countries of the world make use of the SWIFT system for, mostly international, but also for national transactions which may in turn become part of the black box data requested by the US authorities.44
Second, the cases shed light on the relations between public and private authorities and the division of responsibilities with regard to combating terrorism. As Favarel-Garrigues et al. point out, the involvement of private authorities in this fight is not the result of privatization, as ‘there never was a time when public authorities were in charge of the issue’ (2008, p. 2). From the beginning of the fight against money laundering and later terrorism financing, the public and private sectors have had a shared responsibility. Several authors have attempted to conceptualise these public-private relations. Marron (2008) has coined the notion ‘government at a distance’ and mentions ‘deputization,’ proposed by De Goede (2006). Levi and Gilmore describe the public-private collaboration as ‘entrustment’ (2002) while Favarel-Garrigues et al. (2009) speak of joint surveillance and joint intelligence production or the co-production of financial surveillance (Favarel-Garrigues et al. 2011, see also Amicelle & Favarel-Garrigues, 2012). Favarel-Garrigues et al. also examined whether such public-private cooperation should be seen as a partnership in which both parties are equal and willing (2011). The case studies in this thesis suggest that a straightforward answer to this question cannot be given. It appears that the positions of public and private authorities are characterized by multiple and evolving interests, and that their relation can better be understood as one of permanent negotiation.

The opening, for instance, of SWIFT’s black box and the analysis of the role of SWIFT in the SWIFT affair show that in the wake of the 9/11 attacks the company appears to have been a willing partner to the US Treasury. However, when the programme continued for a longer period of time, the company became concerned about its own reputation and legal justification for the extraction of confidential financial data from their database for security purposes. This led to a permanent dialogue and negotiation between the company and the representatives of the US government over additional safeguards to the programme. Later, the banking consortium also actively defended itself and negotiated with the Belgian Privacy Commission once the TFTP came under public scrutiny in Europe. The banking consortium played a role in the negotiations between the EU and the US authorities and helped identify solutions when the transfer of data appeared to be problematic with regard to European privacy laws. Finally, with the inception of a European counterpart of the TFTP, the European Commission suggests that SWIFT, as ‘most important world-wide provider of [financial] messaging services’ is again a central in the development of this financial surveillance system (European Commission, 2011, p. 7).

Similarly, beyond societal expectations and the moral commitment of banks to fight terrorism financing, banks have an interest in being compliant with the Third Directive for
reputational reasons and to avoid fines from supervising authorities. Meanwhile, strengthened regulations to combat terrorism financing also imply additional investments in the form of specialised monitoring software and man-hours. From a commercial perspective, the banks’ interest is to keep the administrative burden and costs related to AML/CFT compliance low. The case study on the Third Directive makes visible the continuous negotiation between the public and the private sector. The regulated professions are often organised: they form committees, associations, groups, bar associations or law societies. Through these platforms, they can maintain an informal or formal dialogue on the nature and scope of measures to combat the financing of terrorism with governments, European decision-makers, regulatory bodies and law enforcement agencies. During the development of a new or revised European directive and subsequently its transition into national law, negotiation between the public and the private sectors takes place in the form of lobbying and stakeholder consultation. With regard to the implementation of the Directive, consultation takes place between banks and supervising authorities; continuous dialogue and feedback between the banks and national FIUs is strongly encouraged, for instance, regarding a common understanding of useful data elements.

Thirdly, this thesis has shown that making the private sector responsible for national security matters leads to a shift in the purpose of counter-terrorism (financing) practices. The examination of the Third Directive as a theatre of compliance highlighted the fact that the priority of banks is being compliant with (inter)national CFT regulations, which is different from actually combating terrorism financing. It means that terrorism financing through the formal financial sector may continue, even as banks entirely fulfil CFT requirements if, for instance, terrorists have low risk profiles and make use of low risk services, and are therefore not detected as such. Alternatively, banks may estimate the risks of their clients and transactions potentially related to terrorism as acceptable. It also suggests that people are erroneously included in FIU databases, as banks may defensively report transactions to their FIU in order to satisfy supervising authorities.

In addition to the empirical evidence given in chapter 6, the difference between combating terrorism financing and being CFT-compliant was confirmed in HSBC’s money laundering and terrorism financing scandal, revealed in July 2012. In response to the findings of the US Senate’s Permanent Subcommittee on Investigations with regard to this case, David Bagley, then HSBC’s head of Compliance, admitted that “in hindsight […] I think we all sometimes allowed a focus on what was lawful and compliant rather than what should have been best practices [to avoid money laundering and terrorism financing]” (quoted in
Rushe, 2012). This discrepancy between being compliant with AML/CFT legislation and a vision of undertaking all possible efforts to inhibit terrorism financing is important. It raises questions about the limitations on the involvement of banks and, more generally, of private authorities as partners (or deadly weapons) in the War on Terror.

A fourth and related finding involves the implication of organising financial surveillance in a way in which the private sector delivers and thus structures or designs the datasets that are transmitted to law enforcement agencies. In both case studies, banks act at the front line of national security decisions. Under the Third Directive, employees of various departments within a bank are the first to value and filter transactions and profiles as to their suspiciousness before a decision is taken to send a suspicious transaction report (STR) to an FIU. Investigations and analysis by FIUs depend on the information provided by banks in the STRs they send. It appears that this organisation of the fight against terrorism financing leads to a lack of accountability and transparency, as outsiders do not know on basis of what expertise and information judgements within banks are made, how errors can be found, or who can be held responsible for the decisions that are taken. This finding is all the more important given banks’ focus on compliance with CFT rules rather than on combating terrorism financing.

Likewise, the TFTP depends on the use of banks of the SWIFT system worldwide, and the information that SWIFT requests. The analysis made by the CIA depends on the design of the SWIFT’s financial services messaging system and on the accuracy and completeness of the information provided by bank employees or banking information systems that make use of SWIFT’s services. The way in which SWIFT’s black box is structured by the banking sector largely defines the possible outcomes that can be obtained by intelligence agents.

Finally, on a more abstract level, these four key findings show that the imposition of strengthened CFT regulation must not be simply interpreted as a reassertion of state power on the deregulated and deterritorialized financial sector. In fact, both case studies show that a proliferation of private sector power has taken place as banks become involved in states’ national security decisions and as state authorities depend to a large extent on the private sector’s willingness to transfer data and its ability and commitment to select useful data. Hence, paradoxically, strengthened CFT regulation has led to the exercise of a fragmented, negotiable form of power, structured by the private sector and directed to the limitation of reputational risks of this sector.
7.4 Power Effects of Risk- and Link-based Governance Practices

The introduction of this thesis stated that the daily governing practices of tracing suspicious financial flows in the context of combating terrorism needed elucidation. The analysis of the two case studies through a governmentality lens sheds light on the way in which risk and link analysis work. This section reflects on what we have learned from the case studies about the way in which risk practice and power operate in relation to financial surveillance. To improve debates on financial surveillance measures, it is important to emphasize that the daily governing practices of the TFTP and the Third Directive are different from each other and lead to different kinds of output. This section discusses three aspects of risk and link-based governing practices made visible by governmentality. First, the case studies have shown the subjectivity embedded in the supposedly objective risk and link-based governance practices. Second, the risk-based approach to financial transaction monitoring can also be understood as a technique of governing through which financial surveillance is strengthened while the vast majority of (international) financial transactions continue to circulate unaffected. Third, risk and link-based governing practices also lead to the exercise of a specific form of power over the population.

In both case studies it became apparent that in several ways, the link-based analysis of the TFTP and the risk-based approach advocated in the Third Directive inevitably involve subjective decision making. Despite the aura of ‘objectivity’ assigned to mathematical risk calculations or the seemingly straightforward principles of establishing links of social networks, these practices also involve the use of intuition, expertise and self-regulation. For instance, once a customer profile is flagged or a transaction provokes a hit in the bank’s monitoring system, human decisions must be made about the significance of the results the software has produced and their procedural follow-up. This is the decision to report a customer or not. Likewise, not all of the possible links that specialised computer programmes can establish between dots of data are relevant to terrorism investigations. On the basis of additional information, expertise and intuition, financial investigators have to assess which persons are potentially part of a terrorist network and which are in contact with the suspect for other (including perfectly legal) reasons. Subjectivity is also integrated in earlier stages, when the analytic software is developed. The design of smart detection software is not neutral, but based on assumptions on how terrorism is financed, the available data elements and the possibilities for exploiting the data. This finding suggests that in addition to calculation, bank employees and financial investigators have to interpret and judge the legitimacy of their
customers and the logic of their behaviour on the basis of limited context. The case studies have shown that this may have implications for clients with certain profiles (in particular those with Islamic names) or behaviour (such as transfers to foreign countries, the use of certain products, a logic of the transaction in relation to other transactions).

Chapter 6 also confirmed the finding of scholars studying financial surveillance who found that the re-regulation of the financial sector for national security purposes and the liberalisation of finance can go hand in hand, either through the introduction of technological and procedural solutions (Shields, 2005), or by increasing barriers against non-Western countries’ access to the international financial system (Warde, 2007). Considered as a technique of governing, the risk-based approach adopted in the Third Directive is a device through which re-regulation of the banking and financial sectors implied at the same time a continued liberalization of the formal financial system. The Third Directive imposed on banks the responsibility to combat terrorism financing, but gave them a substantive amount of flexibility to design their internal AML/CFT compliance policies. The introduction of the risk-based approach prescribed by the Directive allows for the continued flow of money, on condition that potential risks be assessed and acted upon. As such, at least on paper, uncertainty and the danger of terrorism financing is ruled out, and the administrative and commercial burdens to the financial sector are kept relatively low compared to other forms of regulation.

Finally, the governmentality lens draws attention to the way in which risk and link-based governing practices exercise power over the population, and raises questions about what kind of power this is. Political and societal discussions about the use of high-tech, data-led security practices, for instance, certain debates on the SWIFT affair in the European Parliament, sometimes lead to slightly Pavlovian responses making reference to Big Brother or the emergence of a panoptic society. Although this thesis emphasizes the importance of a proper debate on the implications of an intelligence-led approach to terrorism financing, the study of the governing practices related to this approach showed the shortcomings of a debate that makes reference to these metaphors. In fact, the use of risk and link-based governance practices for fighting terrorism is not identical to a totalitarian society in which everybody’s (financial) life is inspected all the time.

It can be debated to what extent risk and link analysis exercise disciplinary or normalising power (Foucault, 1995, 2007). Participation in the formal financial system does subject citizens to a form of discipline, as it requires individuals to discipline themselves in a particular way, often with the help of specific documents or personal codes. Moreover, the
Third Directive clearly requires the establishment of norms and the assessment and classification of normal and suspicious customers. In case studies, the expertise and intuition used by financial investigators and compliance officers is also grafted onto a specific normative framework. Yet on the other hand, both case studies also depart from disciplinary models such as the panopticon. The seeing/being seen dyad that disciplines subjects is absent in both case studies, as citizens were and largely continue to be unaware of the (potential) inspections of their finances. Moreover, citizens cannot adhere to specific norms, as each bank or FIU designs its own norms, which are flexible and easily changed. In fact, citizens are explicitly not supposed to be familiar with the norms on which financial surveillance rests, as their objective is the detection of suspected terrorists’ deviation.

In sum, risk and link-based governing practices operate in a heterogeneous, invisible and rather unpredictable way, selecting and categorizing clients and transactions with the help of mathematical models. This form of exercising power may have exclusionary effects, banning individuals with certain characteristics from the formal financial system, for instance individuals who lack certain documentation about themselves or those considered an unacceptably high risk. It also has inclusionary effects, in the sense of the ‘collateral damage’ inflicted on people wrongfully drawn into terrorism investigations. Somewhat paradoxically, the lack of predictability of these preventive technologies is problematic. From a legal perspective, but also because it is the aim of a just society, ‘the law must be foreseeable,’ (interview 9). It must be clear what a suspicious profile is and what rights a person with a suspicious profile has (ibid.). From a societal perspective it can be debated whether the exercise of power through risk- and link-based surveillance practices leads to ‘neurotic citizens’ (Isin, 2004, De Goede, 2011, p. 64) who are led by stress and govern themselves through their anxieties, and/or ‘public apathy’ (Levi & Wall, 2004, p. 209), ignoring the implications and cumulative effects of financial surveillance practices.

7.5 The Collection of Personal Data: Going Beyond the Privacy Debate

Whereas the years immediately following the 9/11 attacks can be characterized by a call for strengthened security measures and a period during which ‘privacy and civil liberties [were] merely described as being opposed to the “collective right to security”’ (Brouwer, 2006, p. 138), in recent years, political and societal debates show an increased concern for human and fundamental rights. During the campaign for the elections of the European
Parliament in 2009, for example, the EP tried to promote a debate on relations between and the compatibility of security and liberty (see figure 7.1).

Scholars have called into question the supposed opposition between liberty and security, and the discourse on the ‘right balance’ between these two values. Bigo states that there is no straightforward balance between liberty and security. According to him, the relations between these two values can be conceptualized in at least six ways – ranging from absolute freedom to absolute security – depending on the meaning and the weight given to each (2006). On the other hand, it can also be argued that the metaphor of a balance is misleading, as liberty and security are not analogous values that can be compared and weighed against each other. Based on this finding Bigo, Carrera and Guild assert that ‘security only comes from the respect and protection of human rights and fundamental freedoms through the rule of law (…)’ (2009, pp. 3-4).

As discussed in chapter 2, research on post-9/11 European counter-terrorism measures has often emphasized the importance of liberty in the form of privacy and data protection
rights and pointed to the shortcomings of these measures in this respect. This section first
discusses the privacy issues that were raised in the case studies, and then explains how the
study of these cases through a governmentality lens has led to two new insights: the
consideration of privacy as a technique of governing, and the limitation of the concept of
privacy with regard to intelligence-led security practices.

With regard to the SWIFT affair, privacy advocates on both sides of the Atlantic found
the massive scale of the data transfers and the secret handling of personal data highly
problematic. As discussed in chapter 4, the privacy issues that were raised in the US were
dismissed quickly and successfully, while in the EU, privacy remained an issue of concern
throughout the year-long negotiations and debate concerning the transfer of SWIFT’s data;
furthermore, additional privacy safeguards were integrated to the TFTP as a consequence.

This difference can be explained through cultural differences between the US and
Europe in the understanding of privacy and what counts as private (see Roessler, 2005, pp.
13-15). In the US, the understanding of privacy is articulated principally as the right (of US
citizens) to be free from intrusion of the state and ‘to be left alone’. Thus, in its defence of the
programme, the Bush administration emphasized that the TFTP did not breach privacy laws
since the programme did not analyse transactions of American citizens and that individuals
believed to be foreign terrorist agents have no privacy rights (Meyer & Miller 2006; see also
section 4.3.2). Likewise, the central accusation in the court case against SWIFT and the US
government was the state’s intrusion into the financial life of the plaintiffs and of every
American making an international financial transaction. Because the plaintiffs (due to the
secrecy of the programme) could not prove the interference of the state in their financial lives,
the court ruled that the TFTP had not violated any privacy laws.

In Europe, the attitude of the state towards individual personhood appeared not to be
the main concern. For instance, one MEP declared that ‘if private information, personal data,
are necessary for public purposes, law enforcement or something else, that’s fine. We can
agree that [something] is a legitimate purpose for government action’ (interview 6). Likewise,
the EU Counter-Terrorism Coordinator states that in relation to the TFTP ‘we can accept a bit
more intrusion into people’s privacy’ (European Commission, 2010b). What seems to be key
in the European understanding of privacy is the freedom from inspections of one’s daily life.
Hence, voyeurism of the state must be governed through strict legal safeguards and citizens
must be informed about the handling of their data in order to be able to maintain a certain
degree of control over it. For this reason the negotiations between the EU and the US
focussed on the ‘injection of privacy safeguards’ (interview 22) and detailed discussions on
the limitation of data transfers in bulk, the inclusion of an independent review process, improved access to documents and the access to American courts for redress.

Despite the fact that the invasion of privacy is potentially greater under the Third Directive because it continuously monitors all transactions performed by all banking clients, privacy concerns with regard to these practices were only briefly discussed in the European Parliament before adoption of the Third Directive, and remained a matter of concern primarily in specialized debates among ‘experts’. These debates concentrated on three main issues. First, some legal professionals (notably notaries and lawyers), who had been included in the European AML framework since the Second Directive, maintained that the obligation to report suspicious transactions conflicts with the confidential nature of the lawyer-client relationship. This, they argue, infringes upon two human rights: the right to a fair trial, and the right to respect for private life (Mitsilegas, 2003, pp. 146-149). Concerning this first issue, the European Court of Justice did not agree with the Belgian bar associations that, albeit with a few exceptions, the right to fair trial is violated by the Third Directive (ECJ, 2007). The right to respect for private life was considered by the European Court on Human Rights, which has rendered an important judgement in the André and Other v. France case (ECHR, 2008). In this case, the Court ruled that privacy violations had taken place during a search and seizure of documents at André’s law office by tax inspectors. This judgement enhances respect for professional secrecy, and confirms the limits of the authorities’ power to interfere in the confidential lawyer-client relationship.

Secondly, privacy concerns exist with regard to specific aspects of the Third Directive. The identification and verification of the beneficial owners prescribed by the Directive leads to concerns among some professionals that reporting entities, ‘perceiving the collection of information on beneficial owners often as being privacy intruding’ (Deloitte, 2011, p. 69). Moreover, the Third Directive gives maximum powers to the FIUs to ‘access directly or indirectly, on a timely basis, to the financial, administrative and law enforcement information that it requires to properly fulfil its tasks’ (EU, 2005, p. 27). This, it is suggested, ‘can conflict with data protection obligations causing privacy issues for the [reporting] entities involved’ (Deloitte, 2011, p. 291; see also Mitsilegas & Gillmore, 2007, p. 127).

Thirdly, scholars have referred to the breach of the right to privacy as one of the many legal shortcomings of the various public blacklists of suspected terrorists (Amicelle & Favarel-Garrigues, 2009, Tappeiner, 2005). The use of these blacklists is part of the customer due diligence procedures requested under the Third Directive. The main question in this
context is the justification for a public designation of individuals and entities suspected of terrorism, and the damage in the form of stigmatization that results from being listed.

The legal and societal discussions on privacy raised in both case studies are very important. Yet, the study of the cases from a governmentality perspective allows us to go beyond these discussions. In fact, the case studies, and in particular the analysis of the SWIFT affair, suggest that privacy and data protection laws can be seen as a technique of governing: a means of reducing the debate to specific problems that require a ‘technological’ solution. The analysis of the American and European debates on the TFTP shows that the focus on legal issues and in particular on privacy rights has led to a depoliticization of the TFTP. The debate over the TFTP quickly became structured around questions of legality, privacy and data protection rights. Although these issues deserve thorough discussion, they also limit the debate. The political questions that were expressed in initial reactions to the disclosure of the secret programme – calling into question the desirability, necessity and effectiveness of the programme – seemed to be forgotten in favour of questions regarding the storage period of non-extracted data, independent oversight of the TFTP, and limitations on the bulk transfer of data (inter alia European Data Protection Supervisor, 2010). By framing the debate in terms of privacy and data protection issues, a shared understanding of the programme emerged between participants in the professional field, and technical and legal ‘solutions’ could be developed though the governmental apparatus. Procedures involving assessments of the SWIFT case by various national and European privacy and data protection authorities were set in motion, and contributed, albeit unintentionally, to the legitimization and continuation of the TFTP. In other words, it is precisely by establishing the legality of the programme, by assuring that it is in line with privacy and data protection norms, by involving institutions such as data protection agencies or courts, and by following specific procedures that power is exercised and the TFTP can continue.

The detailed study of the governance practices of the European fight against terrorism financing – opening the ‘black box’ of SWIFT and describing the theatre of compliance of the Third Directive – also shows that privacy regulation is not well adapted to the mathematical modelling that characterizes the practices of financial surveillance. In fact, privacy safeguards can, on the one hand, be fully respected while carrying out risk or link-based forms of analysis, while on the other they do not fully cover certain other problematic aspects of the data-led and high-tech practices characteristic of the War on Terror.

Privacy safeguards can be fully respected, as access to (all) names or other sensitive data is not essential for risk and link-based analysis. Names on a watch list and in a database
containing financial records can be matched (automatically and) without having to access all data. In the context of the TFTP for instance, only the hits between data (allegedly) related to terrorist suspects and the SWIFT data can be accessed. Likewise, within banks, the monitoring software searches for hits between customers and a number of watch lists. Although these practices may occasionally generate erroneous hits due to customers who share the same or very similar names with designated terrorist suspects, client monitoring does not entail detailed inspection of the entire database.

Moreover, an important aspect of risk analysis entails the establishment of norms and patterns for normal or suspicious behaviour, in order to calculate deviations from those norms and patterns, and depending on the outcomes to take security action. For classification of customer behaviour and the computerized confrontation of sets of personal data and with established norms for normal financial behaviour, identification of the customer is irrelevant, and these practices are therefore difficult to consider as at odds with the concept of privacy. Only when the transaction patterns of a specific account are considered suspicious enough to be reported does identification of the customer(s) related to this account regain importance.

In addition to privacy issues and the increased exclusion from the formal financial system of certain groups mentioned in chapter 2, financial surveillance practices also seem to have discriminatory effects. In the context of the TFTP for instance, the findings of this thesis suggest that the programme seems to target primarily non-American citizens or residents, people with Islamic names or people maintaining private or professional relations with high-risk (this is mainly non-Western) countries (see chapter 5). Moreover, it became clear, ironically enough, that by specifically targeting subjects, a form of discrimination is built into structure of the software and the link analysis of the TFTP; these issues fall beyond the current scope of privacy and data protection laws. Also, risk-based analysis within banks may potentially lead to discrimination, as compliance officers have to make decisions on the basis of their expertise and intuition, which may be biased or subject to prejudice. Likewise, banks may decide to refuse customers on the basis of their own norms instead of a legal obligation. The examples given in chapter 6 show that this may lead to discrimination by denying controversial groups or individuals access to the financial sector. Finally, even without explicitly filtering out certain categories, different norms for financial transactions and customer behaviour must be codified in the software and valued to make the computerized calculations possible. Therefore these classifications are not neutral but imply discrimination against certain groups or services on the basis of criteria that are not (always) transparent.
The integration of technical fixes to existing surveillance programmes is often the privileged response for resolving security and privacy concerns. The EU Counter-Terrorism Coordinator explains, for instance, that ‘the system [can be built] in such a way that the number of those who get access is more restricted, that the conditions for getting access are stricter and that you try to minimize the impact of new technologies by [their] design’ (Fashi, 2012). This last means that modifications are made to the way in which queries of the database can be carried out, or that software tools are introduced that enhance the privacy of the data subjects, by making certain information fields invisible, for example. These privacy-enhancing technologies (PETs) or ‘privacy by design’, which may limit unauthorized access to personal data or separate the ‘data’ and the ‘subject’ are offered by companies such as Microsoft (Sciences-Po, 2008, UK Information Commissioner Office, 2008). Another solution advanced by the Belgian Privacy Commission with regard to SWIFT is the preference of ‘pull’ constructions – only making the requested information available – over ‘push’ constructions – giving access to search the entire database (interview 9). The aim of these technological fixes is to enhance privacy while ensuring that information continues to flow. However, the adoption of such fixes bypasses the question of the desirability of a society in which virtually everyone’s personal financial data is stored and can become the subject to investigation. In addition, stricter privacy regulation does not address potentially discriminating and exclusionary effects, nor the lack of transparency and accountability that are embedded in the financial surveillance practices of the Third Directive and the TFTP.

7.6 An Intelligence from which the Human Mind Will Always Remain Infinitely Removed?

Finally, the case studies demonstrate that, although today ‘supercomputers’ have a calculative capacity that Laplace would never have imagined, the tangible results of high-tech, data-led financial surveillance practices in predicting and preventing terrorism (financing) are limited. In neither case has strong evidence establishing the effectiveness of the European measures to prevent terrorism financing been found. This can be partially explained by the difficulty of putting a number on terrorist acts that have not taken place. It may also be that comprehensive reports of the results are not publicly available. In some cases, for instance in the 2011 report evaluating the EU-US TFTP agreement, reporters decided not to focus on effectiveness (European Union, 2011). Nonetheless, the empirical evidence of the two case studies strongly suggests that under the Third Directive there have
been virtually no suspected terrorists detected by the monitoring system, and that in the case of the TFTP, the success in preventing terrorism has been very limited.

Contrasting this lack of effectiveness with the societal, political and personal implications of the governing practices identified in the previous paragraphs stresses the need for a critical debate concerning the societal desirability of these practices. Moreover, the opening of the black box of the TFTP has shown that there is also a link between the dark side of the War on Terror and the clean fight against terrorism financing. Some of the ‘success cases’ of the TFTP have been detained without charges in secret prisons and are currently held on Guantanamo Bay. These findings therefore call into question the three arguments – effectiveness, preventive power and non-violence – that are used to justify the TFTP.

In the light of the meager results of risk and link-based governing practices in the European fight against terrorism, it seems appropriate to conclude with another phrase from Laplace. In the same paragraph as the opening quote of this dissertation, Laplace reflects on his thought experiment and states that ‘[the human mind] will always remain infinitely removed’ from the ‘vast intelligence’ he described (Laplace, 1902, p. 4). The mathematician emphasizes that the desire to make an uncertain future governable may be very strong, but remains utopian. However, such a conclusion would ignore other important arguments of this dissertation. An important purpose of the Third Directive is, for instance, to show citizens that something is being done, to call into being a ‘security theatre’ (Schneider, 2003, 2009), and provide a sense of security that strengthens belief in a just and sound financial sector. Thus, the value attributed to risk calculations, smart technology, and private sector involvement and expertise goes beyond the actual outcomes and evidence.
## Annex 1: Overview of conducted interviews

<table>
<thead>
<tr>
<th>Sector of activity</th>
<th>Reference number</th>
<th>Date of the interview</th>
<th>Main themes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Intelligence Units (the Netherlands, France and the FIU.net bureau)</td>
<td>1*</td>
<td>10-06-2008</td>
<td>Implementation of the Third Directive, high tech, data-led practices, results and development of policies.</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>15-08-2008</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>5-11-2008</td>
<td></td>
</tr>
<tr>
<td>Law Enforcement (police services, customs)</td>
<td>3</td>
<td>4-11-2008</td>
<td>Pre and post 9/11 CFT practices. High tech and data-led policing. Patterns of terrorism financing.</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>5-11-2008</td>
<td></td>
</tr>
<tr>
<td>European Commission</td>
<td>8*</td>
<td>04-03-2009</td>
<td>Development and implementation of the Third Directive, content of the TFTP and handling of the SWIFT affair, general governing practices of the EU fight against terrorism financing.</td>
</tr>
<tr>
<td></td>
<td>10*</td>
<td>29-06-2009</td>
<td></td>
</tr>
<tr>
<td></td>
<td>24</td>
<td>08-06-2009</td>
<td></td>
</tr>
<tr>
<td></td>
<td>25</td>
<td>08-06-2009</td>
<td></td>
</tr>
<tr>
<td></td>
<td>26</td>
<td>30-06-2009</td>
<td></td>
</tr>
<tr>
<td>European Council</td>
<td>22*</td>
<td>20-04-2009</td>
<td>Development and implementation of the Third Directive, content of the TFTP and handling of the SWIFT affair, general governing practices of the EU fight against terrorism financing.</td>
</tr>
<tr>
<td></td>
<td>23</td>
<td>08-06-2009</td>
<td></td>
</tr>
<tr>
<td>European Parliament</td>
<td>6#@</td>
<td>25-08-2008 08-04-2009</td>
<td>Content of the TFTP and handling of the SWIFT affair, general governing practices of the EU fight against terrorism financing.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>03-09-2010</td>
<td></td>
</tr>
<tr>
<td></td>
<td>11@</td>
<td>11-05-2010</td>
<td></td>
</tr>
<tr>
<td>National and European privacy and data protection authorities</td>
<td>7</td>
<td>04-03-2009</td>
<td>The handling of the SWIFT affair, the Third Directive, automated data-led police investigation.</td>
</tr>
<tr>
<td></td>
<td>9*</td>
<td>20/04-2009</td>
<td></td>
</tr>
<tr>
<td>Journalists, researchers, consultants, think tanks</td>
<td>12</td>
<td>18-08-2010</td>
<td>Practices of the fight against terrorism financing, handling of the SWIFT affair and content of the TFTP, societal reactions on data-led security programmes.</td>
</tr>
<tr>
<td></td>
<td>13</td>
<td>19-08-2010</td>
<td></td>
</tr>
<tr>
<td></td>
<td>17</td>
<td>09-11-2010</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------</td>
<td>-----------------------------------------------------------------</td>
</tr>
<tr>
<td>Banking industry</td>
<td>14</td>
<td>28-10-2010</td>
<td>Implementation of the Third Directive, daily practices to</td>
</tr>
<tr>
<td></td>
<td>15</td>
<td>24-11-2010</td>
<td>combat terrorism financing, cooperation with law</td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>17-11-2010</td>
<td>enforcement, results and effectives of the fight</td>
</tr>
<tr>
<td></td>
<td>20@</td>
<td>28-10-2010</td>
<td>against terrorism financing.</td>
</tr>
<tr>
<td></td>
<td>21</td>
<td>17-12-2010</td>
<td></td>
</tr>
<tr>
<td></td>
<td>27</td>
<td>08-11-2010</td>
<td></td>
</tr>
<tr>
<td></td>
<td>28*</td>
<td>25-11-2010</td>
<td></td>
</tr>
<tr>
<td>International</td>
<td>18</td>
<td>18-08-2010</td>
<td>International and transatlantic efforts to combat terrorism, pre</td>
</tr>
<tr>
<td>organizations (IMF,</td>
<td></td>
<td></td>
<td>and post 9/11 CFT initiatives and mentalities, data led</td>
</tr>
<tr>
<td>World Bank)</td>
<td>19@</td>
<td>10-09-2009</td>
<td>financial security practices.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note:

To guarantee the anonymity of the respondents, requested by many of them, each interview was assigned a number and categorized according to their sector of activity. In some cases two or three respondents of a same organisation participated in the interview. These are thus represented under the same number and indicated with *. With some of the respondents repeated interviews have been conducted. These are considered as supplement to the original interview and are indicated with #. In a few cases (follow up) interviews were conducted via the telephone. These are marked by @. The numbering of the interviews follows the chronological order in which interviews have taken place. A more detailed discussion on the methodology adopted with regard to the research interviews can be found in chapter 2.
# Annex 2: List of investigated newspapers

<table>
<thead>
<tr>
<th>Country</th>
<th>Newspapers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netherlands</td>
<td>Algemeen Dagblad, Metro, Het Parool, Trouw, Nederlands Dagblad, Reformatorisch Dagblad, De Volkskrant, De Pers, NRC Handelsblad, Spits!, Het Financiële Dagblad, NRC, NRC.Next, De Telegraaf</td>
</tr>
<tr>
<td>Europe</td>
<td>EU-Observer, European Voice</td>
</tr>
</tbody>
</table>

**Note:**

This list provides an overview of the (online) newspapers that have been used for the analysis of the American and European debates concerning the disclosure of the TFTP. The English, French and Dutch articles have been retrieved with help of the LexisNexis database. Articles from the European press have been gathered through searches in the archives of the newspaper websites. Additional articles have been included in the analysis through Internet research.
Nederlandse Samenvatting

Meer dan tien jaar na de terroristische aanslagen van 11 september 2001 in Amerika en daarop volgende aanslagen in onder andere Madrid en Londen, is de internationale War on Terror nog steeds een belangrijk politiek gegeven. Hoewel de bestrijding van terrorisme financiering een centrale pijler is in de strijd tegen terrorisme, zijn de maatregelen op dit gebied, hun betekenis en hun maatschappelijke en politieke gevolgen, relatief weinig besproken en onderzocht. Met name de wetenschappelijke literatuur over de maatregelen tegen terrorisme financiering die genomen zijn door de Europese Unie is nog van bescheiden omvang. Deze dissertatie gaat over de manier waarop de Europese strijd tegen terrorisme financiering is vorm gegeven en wat de gevolgen zijn van de genomen maatregelen. De aandacht ligt daarbij in het bijzonder op het gebruik van massale databestanden met persoonlijke financiële gegevens en het geloof in de preventieve kracht van wiskundige modellen en slimme software (de ‘intelligence-led approach’) (hoofdstuk 1).

Om een diepgaand begrip te krijgen van de Europese strijd tegen terrorisme financiering is het belangrijk om het totaal aan genomen maatregelen, alle betrokken deelnemers en de dagelijkse processen en praktijken ontwikkeld in deze strijd, te bestuderen als een bestuurlijk veld (field of governing) dat institutionele, sectorale en geografische grenzen overschrijdt. Met behulp van het door Michel Foucault geïntroduceerde begrip ‘governmentality’ en de veldtheorie ontwikkeld door Pierre Bourdieu, wordt een theoretisch kader opgezet waarmee de gedachtevorming waarop beleidsinitiatieven in de strijd tegen terrorisme financiering stoelen en de bestuurlijke praktijken die in dit kader binnen Europa zijn ontwikkeld kritisch kunnen worden onderzocht (hoofdstuk 2).

Vervolgens wordt eerst de vanzelfsprekendheid van het bestrijden van terrorisme financiering onderzocht (hoofdstuk 3). Klopt de onderliggende aannamaat dat terrorisme kan worden uitgeroeid door het dichtdraaien van de geldkraan? Een zoektocht naar de oorsprong van maatregelen tegen terrorisme financiering laat zien dat de betekenis en het belang van het bestrijden van terrorisme financiering geen vaststaande gegevens zijn. Zij komen tot stand door middel van discussie, onderhandeling en politieke worstelingen. In de jaren 60 en 70 bijvoorbeeld werd de financiering van aanslagen en terroristische groeperingen nauwelijks van belang geacht. Vanaf de jaren 80 begonnen Amerikaanse en Britse politici terrorisme financiering actief te ‘framen’ als misdaad en in verband te brengen met het witwassen van drugsgelden en de georganiseerde misdaad. In de jaren 90 werd de definitie van terrorisme
financiering uitgebreid naar zowel crimineel als legaal verworven gelden. Na 9/11 werd terrorisme financiering betiteld als oorlogsdaad. Een bredere analyse van maatschappelijke debatten laat bovendien zien waarom na 9/11 het nemen van financiële maatregelen aantrekkelijk was voor politici en hoe controversiële maatregelen door het ontstane momentum van de aanslagen genomen konden worden. Daarnaast onderstreept deze analyse dat onze ideeën over terrorisme financiering veelal overeenkomen met die aspecten waarop het dominante politieke discsours en de beleidsinitiatieven zich richten maar grotendeels losstaan van de werkelijke wijze waarop terroristische groepen fondsen verwerven en verplaatsen.

Met behulp van twee case studies, het Terrorist Finance Tracking Program (TFTP ofwel de SWIFT affaire) en de Derde Europese AML/CFT Richtlijn wordt vervolgens meer in detail onderzocht hoe de Europese strijd tegen terrorisme financiering de afgelopen jaren vorm gekregen heeft. Een analyse van de debatten in de SWIFT affaire, laat zien dat zowel in de VS als in Europa, de politieke en maatschappelijke discussie over dit onderwerp eenzelfde structuur volgde (hoofdstuk 4). Na de onthulling van het veiligheidsprogramma door de New York Times volgde er een kort moment waarin er nog geen politieke interpretatie van de onthulling is. Op dat moment konden wezenlijke politieke vragen worden gesteld over de effectiviteit en de wenselijkheid van een in eerste instantie geheim veiligheidsprogramma waarin de financiële persoonsgegevens van alle burgers worden opgeslagen door de CIA (een moment of openness). Dit moment wordt snel gevolgd door een fase van politieke interpretatie waarin de discussie versmalt. Het debat wordt zo veel mogelijk beperkt tot vragen van administratieve, juridische of technische aard. Ten slotte, volgt een fase van depolitisering waarin de belanghebbenden een nieuwe consensus over het probleem en de oplossingen vormen (en waarin in Amerika de ‘aanstichters van het probleem’ – de journalisten die de onthulling hebben gedaan – in diskrediet worden gebracht). De analyse van de debatten maakt zichtbaar dat ondanks het feit dat de vragen wel zijn gesteld, er over twee essentiële politieke onderwerpen nooit wordt gedebatteerd: de filosofie waarop de War on Terror is gebaseerd en de effectiviteit van het TFTP. Het ontbreken van deze onderwerpen moet echter niet worden toegeschreven aan toeval. Zij komt voort uit een neiging naar de voorspelbaarheid van politieke processen, de moeilijkheid om nationale veiligheidsvraagstukken kritisch bespreekbaar te maken en de afwezigheid van politieke en maatschappelijke belanghebbenden die verantwoordelijk zijn voor deze vraagstukken of zich deze toe eigenen.

De vraag hoe de bankgegevens binnen het TFTP worden geanalyseerd, hoe effectief en succesvol het programma is en hoe zich dit verhoudt tot de bredere filosofie van de War on
Terror kan echter met openbare bronnen wel deels worden beantwoord. In hoofdstuk 5 wordt geprobeerd de *black box* van het SWIFT programma te openen. Een inventarisatie van degenen die wisten van het bestaan van het programma laat zien dat de groep ingewijden veel groter is dan men zou kunnen denken. Ook laat de manier waarop het TFTP tot stand gekomen is en de analyse van de ingewijden, een belangrijke verschuiving zien in de manier waarop aan nationale veiligheid gerelateerde informatie circuleert en dat private actoren een snel groeiende rol hierin spelen. In het geval van de SWIFT zaak heeft dit geleid tot minder transparantie en verantwoording. Ook wordt duidelijk dat het programma gebruikt wordt om specifieke informatie van verdachten op te zoeken en om netwerken in kaart te brengen door middel van link of sociale netwerk analyses. Deze netwerken ontstaan door het linken van (onder andere) bancaire gegevens uit de SWIFT database tot vijf of zes stappen verwijderd van de eerste verdachte. Een analyse van dit programma maakt duidelijk hoe bestaande juridische kaders voor gegevensuitwisseling door het TFTP werden omzeild en hoe het begrip privacy onvoldoende is om tot het kernprobleem van het SWIFT programma te komen. De belangrijkste pijnpunten zijn namelijk niet (meer) de afscherming van persoonsgegevens maar de twijfelachtige resultaten van het programma door enerzijds de subjectieve en politieke voorkeuren die tot uiting komen in de opzet van het programma en anderzijds door het in verband brengen van individuen en het uittekenen van netwerken zonder enige of op basis van geringe contextuele informatie. In plaats van een scherp harpoen is het programma beter te vergelijken met de werking van een cluster bom. Een analyse van de bekendgemaakte resultaten en successen laat bovendien zien dat deze beperkt zijn in aantal en dat het merendeel betrekking heeft op informatieverschaffing na een aanslag in plaats van de beloofde preventieve informatie inwinnung ter voorkoming van aanslagen. Een dieper onderzoek van de resultaten van het TFTP toont bovendien dat het programma geen schone of geweldloze manier van terrorisme bestrijding is aangezien een van de succescases en een ander individu verbonden aan een van de successen van het TFTP zijn vastgehouden (en wellicht gemarteld) in geheime gevangenissen (vermoedelijk in Afghanistan) en op Guantanamo Bay. Deze vaststelling roept onder andere vragen op over de consistentie van de Europese opstelling, voor het TFTP enerzijds en tegen Guantanamo Bay anderzijds.

Naast link-analyse van bankgegevens en trans-Atlantische gegevensuitwisseling, worden in het kader van de strijd tegen het terrorisme ook een permanente controle en risicoanalyse uitgevoerd op alle financiële gegevens van burgers door hun eigen bank. De belangrijkste wetgeving die banken hiertoe verplicht is de Derde Europese AML/CFT Richtlijn. Met behulp van een theater metafoor wordt de uitvoering van de richtlijn binnen
banken inzichtelijk gemaakt. Een belangrijke vaststelling is niet alleen dat publieke en private actoren de strijd tegen terrorisme financiering gezamenlijk vormgeven. Ook de manier waarop dit gebeurt, de onderlinge taakverdeling en de procedures binnen banken zijn van groot belang. De verschuiving van verantwoordelijkheid voor nationale veiligheid naar banken leidt namelijk tot een discrepantie tussen het bestrijden van terrorisme financiering en het uitvoeren van CFT maatregelen. Bovendien is de transparantie en verantwoordelijkheid van banken met betrekking tot veiligheidsbesluiten vooral nog niet goed vastgelegd omdat het van belang geacht wordt om de procedures zoveel mogelijk geheim te houden. De bestudering van de risicoanalyses die banken uitvoeren toont dat deze subjectief zijn in plaats van objectief en dat de flexibiliteit van de normen besloten in de analyse ook leidt tot juridische onzekerheid, een gebrek aan transparantie en zelfs discriminatie. Daarbij is ook gebleken dat risicoanalyses van banken (nagenoeg) geen transacties opsporen die in verband kunnen worden gebracht met terrorisme (financiering). De waarde van de betrokkenheid van banken in de strijd tegen terrorisme financiering ligt vooral in de symbolische, geruststellende effecten van de maatregelen in plaats van de efficiënte opsporing van terroristen (financiers).

Ten slotte worden de empirische bevindingen in een breder kader geplaatst (hoofdstuk 7). Er worden parallellen tussen de twee cases getrokken en er wordt uiteengezet hoe beide cases passen in het gedachtegoed van de War on Terror en de Financial Surveillance literatuur. Vervolgens worden de belangrijkste kenmerken van de Europese strijd tegen terrorisme financiering aan de hand van de bevindingen uit de case studies besproken: de groeiende macht van de private sector in het vormgeven van de nationale veiligheid, de gevolgen van risico- en linkanalyse op bestuurlijke processen en machtsuitoefening, en de privacy aspecten van de twee case studies alsmede de tekortkomingen van dit begrip om bepaalde problematische aspecten van financiële surveillance te vatten.
References


De Hert, P. & De Schutter, B. (2008). International Transfers of Data in the Field of JHA: The


overheidsoptreden rondom de moord op de heer Th. van Gogh, 18 December 2006.


National Bank of Belgium (2006). Oversight of SWIFT. Press release, 25 June 2006, available at: http://www.nbb.be/pub/01 00 00 00 00/01 06 00 00 00/01 06 01 00 00/20060626_swift.htm, last accessed: 23 November 2011.


Integration Thirty Years On, From Reform to Crisis, Cambridge: Cambridge University Press.


Notes

1 The first English edition appeared in 1902.
2 Laplace’s firm belief in the power of science is illustrated by the anecdote in which Laplace is said to have responded to Napoleon’s question regarding the absence of a creator in his explanation of the system of the universe by saying he: ‘does not need this hypothesis’ (Rouse Ball, 1960, p. 343).
5 The cooperation between the FBI and First Data and Western Union is sometimes described as a ‘mini version of the TFTP’ (interview 13).
6 In Bigo’s work (for instance Bigo 2005, Bigo et al. 2006; 2007) and more generally that of the CHALLENGE research programme the importance of technology is certainly acknowledged and they have included a number of migration related databases on the European level in their field map of European Security Agencies (Bigo et al. 2007). However, I believe that our understanding of the political significance and the agency of financial data can be developed further by building on works from Science and Technology Studies.
9 Is available at http://www.g8.utoronto.ca/terrorism/terror98.htm
10 See www.swift.com
11 These numbers steadily increased during the first decade of the twenty-first century. In September 2011, 10,005 banks and financial institutions in 209 countries make use of the SWIFT network, sending a total of 3,314 billion messages during the first nine months of the year (SWIFT, 2011).
12 Although the SWIFT affair was also front-page news outside the US and the EU, for instance in Australia, Canada, and Switzerland, the specifics of these debates will not be taken into account here. It may be noted however that the privacy of financial data played an important role in all these countries.
13 It needs to be emphasized, however, that the notions of politicization and depoliticization, just like the notions of politics and the political, are not always defined in the same manner. In fact the notions are closely intertwined and the distinction between them is a subject of societal struggle and different academic interpretations. Moreover, in democracies political and public debates are rarely completely homogenous and dissent or holding marginal opinions is of course possible. Understanding a debate in terms of politicization or depoliticization therefore refers to the dominant discourse at a certain moment in time. Since the publication of the SWIFT affair, there have been attempts to repoliticize a depoliticized debate and attempts to depoliticize a politicized debate.
14 The First Amendment reads as follows: “Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.” The Fourth Amendment reads as follows: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”
15 On 7 July 2006 the Congressional Research Service of the Library of Congress published a report for Congress addressing the issues that were raised in the American debate on the TFTP and on 11 July a hearing on the TFTP was organised by the House Financial Services Committee’s Oversight and Investigations Subcommittee. However, these events did not reopen the debate but confirmed the conclusions that the programme was legal.
16 This is the text of the official minutes of the European Parliament. The literal text as pronounced in the plenary session of the EP as translated by the translator of the European Parliament reads: ‘The situation now with the Americans is that of secret flights, the abduction of people accused of certain offences, the removal of people from European territory. . . . And now we discover that our powerful friend and ally is rifling through our private bank accounts. What will happen next, I ask you? It is high time that the Parliament puts its foot down and brings this state of affairs to an end.’
The Group of Ten (G-10) consists of 11 industrial countries: Belgium, Canada, France, Germany, Italy, Japan, the Netherlands, Sweden, Switzerland, the United Kingdom and the United States. The Bank of International Settlements (BIS), the European Commission, the IMF, and the OECD are official observers to the G-10.

The literal text as pronounced during the plenary session reads: “Citizens were never informed about the transfer of their financial records. I wonder whether Europe would be as tolerant had it been Russia or China collecting the data.”

The law in question was the Privacy law (loi de la Vie Privée) of 8 December 1992 regarding the protection of privacy with regard to automatic processing of personal data (DPL) and Directive 95/46/EG of the European Parliament and the Council dated 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (95/46/EG Directive).

It is interesting to note here that in 2010 Guy Verhofstadt was a member of the European Parliament and an active opponent of the 2010 agreement.

The qualification used in Dutch is ‘ongeloofwaardig’.

For the significance of the word ‘vital’, see the discussion on ‘lifeblood’ in chapter 3.

The 25 members of the Executive Board hold functions at: JP Morgan Chase Bank (US), UBS AG (Switzerland), SECB Swiss Euro Clearing Bank GmbH (Germany), Euroclear SA/NV (Belgium), The Standard Bank of South Africa (South Africa), Fin-Force (Belgium), ING (the Netherlands), The Royal Bank of Scotland (UK), Deutsche Bank AG (Germany), Raiffeisen Zentralbank (Austria), NATIXIS (France), The Bank of New York (US), DnB NOR Bank ASA (Norway), The Bank of Tokyo-Mitsubishi UFJ Ltd. (Japan), Credit Suisse (Switzerland), BNP Paribas (France), CLS Services (Australia), SIA Ced Borsa SpA (Italy), The Bank of Nova Scotia (Canada), Banco Bilbao Vizcaya Argentia (Spain), HSBC Asia Pacific (Hong Kong), Nordea Bank AB (Sweden), Deutsche Bank (UK), Clearstream International (Luxembourg), and The Association of Banks in Singapore (Singapore). SWIFT Annual Report 2006, pp. 26-27.

This Oversight Group includes the G10 countries and the European Central Bank.

These include: the Belgian Privacy Commission, the European Data Protection Supervisor, the Article 29 Group, Canada, Switzerland, and Hong Kong.

Under the current EU-US agreement also a permanent independent overseer appointed by the EU participates in the verification of the searches on the SWIFT data. According to the report of the first review of the agreement ‘all overseers, including the EU appointed one, had blocked searches to request additional information’ (European Union, 2011, p. 10)


The TIDE database is used to compile various different watch lists requiring various forms of action. The No Fly List contained 50,000 persons in 2008 and denies people air transport. The Selectee list contains names of people that are allowed to fly but require more careful searches at airports. The terrorist watch list is the most general and broadest list and contains anyone who is thought capable of harming the US. The US terrorist watch list is very controversial for several reasons, not the least for its inclusion of many false positives.


An updated version of this list is publicly available as part of the US Treasury’s FAQ on the TFTP. This list also mentions three more recent terrorist attacks ‘in which the TFTP provided valuable lead information’, the Nigerian Independence Day car bombings in Abuja, Nigeria in 2010, the Jakarta hotel attacks in 2009, and the hijacking and hostage operations by Al Shabaab, including the hijacking of the Belgian vessel MV Pompeii in 2009.

As will be discussed, the Directive lists a number of financial and non-financial professions. The focus in this chapter will be on banks, since they are dealing with by far the most transactions and issue the most suspicious transaction reports.

For contestation over this claim, see chapter 3.

These sources do not always classify all EU member states and do not classify them in the same way. Masciandaro (2007), for instance, includes the Romanian model in the category of hybrid model, while the IMF (2004) qualifies the Romanian FIU as an administrative model. For the compilation of this table, the information of the IMF has been privileged.

Directive 2006/70/EC defines the criteria according to which these procedures should be applied. This Directive also provides for exemption on grounds of a financial activity conducted on an occasional or very limited basis.

These are: Belgium, the Czech Republic, Greece, Finland, France, Ireland, Luxembourg, Malta, the Netherlands, Poland, Portugal, Spain, Sweden and Slovakia. La Semaine Juridique Notariale et Immobilière, n° 24, 13 Juin 2008, act. 521.

These include, for instance: reports from OECD, World Bank, Amnesty International, Transparency International, local NGOs and government reports (interview 14).

This number was communicated to the author in a private conversation with a representative of the FIU of Malta.


It might be noted here that the perpetrator of the 2011 attacks in Oslo, Anders Breivik, hired a farm as a cover to obtain large quantities of fertilizers.

Some other sources (House of Lords, 2009c) estimate the costs of the 2005 London attack higher, at around or below £ 8000.

The UK FIU speaks of Suspicious Activity Reports (SARs) instead of Suspicious Transaction Reports, but the meanings of these terms overlap.

It is telling to note that the number of countries making use of SWIFT’s services largely exceeds the number of UN members (212 vs. 193).

The leeway given to banks under the risk-based approach is illustrated in the US Senate’s report on the HSBC case. The report reveals that HSBC continued business relations with Al Rajhi Bank, despite several serious public allegations of the bank’s links to terrorism financing. However, HSBC did classify Al Rajhi Bank as a ‘Special Category of Client’ (SCC), its highest risk designation. This designation was due to the bank’s location in Saudi Arabia, which HSBC classified as a high risk country and to the fact that the bank was owned in part by a Politically Exposed Person (PEP), Abdullah Abdul Al Rajhi, who was a major shareholder, a member of the bank’s board of directors, and a member of the Northern Borders Provincial Council in Saudi Arabia (US Senate, 2012, p. 204).

Some new examples of the added value of the TFTP in combating terrorism and its financing are, however, provided in the 2012 report on the second joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program (European Union, 2012).