The European fight against terrorism financing: Professional fields and new governing practices
Wesseling, M.

Citation for published version (APA):
Wesseling, M. (2013). The European fight against terrorism financing: Professional fields and new governing practices

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: http://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.
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
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).

Figure 7.1 Connecting liberty and security, but how? Photo by the author, Vienna, 2009.

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 through 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.