The European fight against terrorism financing: Professional fields and new governing practices

Wesseling, M.

Citation for published version (APA):
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\textsuperscript{25} 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.\textsuperscript{26} 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,
2006a, 2006b). 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.30

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 to 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 than 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

<table>
<thead>
<tr>
<th>Historical TFTP Value Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>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:</td>
</tr>
<tr>
<td><strong>November 2008 Mumbai Attack</strong></td>
</tr>
<tr>
<td>Following the attack the US Government provided information about members of the attack.</td>
</tr>
<tr>
<td><strong>January 2008 Barcelona Arrests</strong></td>
</tr>
<tr>
<td>TFTP information was used to identify the connections of the Spain-based network with connections to Asia, Africa, and North America.</td>
</tr>
<tr>
<td><strong>Summer 2007 German IJU Arrests</strong></td>
</tr>
<tr>
<td>The US Government surged analysis to investigate this threat and this information contributed to the investigation of the IJU network in Germany.</td>
</tr>
<tr>
<td><strong>June 2007 JFK Airport Plot</strong></td>
</tr>
<tr>
<td>TFTP information identified the specific financiers of the plot and revealed the scope of the network.</td>
</tr>
<tr>
<td><strong>2006 Transatlantic Liquid Bomb Plot</strong></td>
</tr>
<tr>
<td>TFTP information provided information that assisted in the investigation and conviction of individuals responsible for this attempted attack.</td>
</tr>
<tr>
<td><strong>2005 London ‘7/7’ Bombings</strong></td>
</tr>
<tr>
<td>TFTP information provided new leads, corroborated identities, and revealed relationships among individuals responsible for this terrorist plot.</td>
</tr>
<tr>
<td><strong>April 2005 Van Gogh Murder Investigation</strong></td>
</tr>
<tr>
<td>TFTP information revealed that the attacker had connections to individuals with global terrorism connections.</td>
</tr>
<tr>
<td><strong>2004 Madrid Train Bombings</strong></td>
</tr>
<tr>
<td>TFTP information was provided to multiple European countries to assist in the investigation that followed this attack.</td>
</tr>
<tr>
<td><strong>October 2002 Bali Bombings</strong></td>
</tr>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

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.