The Great (Data) Bank Robbery: Terrorist Finance Tracking Program and the "SWIFT Affair"

Anthony Amicelle

Research Questions
N°36 – May 2011

The Great (Data) Bank Robbery:

Terrorist Finance Tracking Program and the "SWIFT Affair"

Anthony Amicelle

Centre d'études et de recherches internationales
Sciences Po

The Great (Data) Bank Robbery:

Terrorist Finance Tracking Program and the "SWIFT Affair"[1]

Summary

The present paper examines current dynamics of surveillance regarding the fight against "terrorism" and its financing. Close analysis of the so-called "SWIFT Affair" and the US terrorist finance tracking program draw attention to one specific case-study which allows us to question the contemporary politics of massively accessing commercial data-banks for intelligence purposes. With reference to the SWIFT affair, the paper explores a sensitive aspect of transatlantic cooperation in the field of counter-terrorism.

Résumé

Ce texte a pour objectif d'examiner les dynamiques de surveillance à l'œuvre dans le domaine de la lutte contre le « terrorisme » et son financement. En proposant une analyse détaillée de l'« affaire SWIFT » et du Terrorist Finance Tracking Program américain, le présent texte met donc en lumière un programme spécifique qui va nous permettre de questionner les velléités contemporaines d'accès aux bases de données commerciales à des fins de renseignement. Cette étude explore ainsi un aspect sensible de la coopération antiterroriste à l'échelle transatlantique.

Anthony Amicelle is a doctoral candidate in political science (international relations) at Sciences Po Paris/ Centre for international studies and research (CERI). He is currently teaching assistant (ATER) at Sciences Po Lille and he is affiliated with the Lille centre for politics and administration (CERAPS). His main research interests revolve around antiterrorist policies, international mobilization against "dirty money" and practices of financial surveillance in Europe.

1. I thank the two anonymous referees for their helpful comments. I also would like to specifically thank Christian Olsson and Miriam Perier who helped me to improve the linguistic quality of a significant part of the paper.

Table of content

Introduction

> In combating terrorism, prevention is key. The entire Department of Justice has shifted its focus to a proactive approach to terrorism, reflecting the reality that it is not good enough to wait to prosecute terrorist crimes after they occur. For the law-enforcement officers responsible for staying a step ahead of the terrorists in these investigations, time is critical. Even a brief delay in an investigation may be disastrous. Therefore, these officers need tools that allow them to obtain information and act as quickly as possible. Administrative subpoenas are one tool that will enable investigators to avoid costly delays. An administrative subpoena is an order from a government official to a third party, instructing the recipient to produce certain information. Because the subpoena is issued directly by an agency official, it can be issued as quickly as the development of an investigation requires. (The United State Judiciary Committee 2004)

> As a part of our efforts to track the funds of terrorists, we are confirming that we have subpoenaed records on terrorist-related transactions from SWIFT. (US Department of the Treasury 2006a)

> This [terrorist finance tracking] program is exactly the kind of program that Americans want and expect from their government to prevent further terrorist attacks. (US Department of the Treasury 2006b)

Two years separate Rachel Brand's promotion of administrative subpoenas for counter-terrorism purposes and the official acknowledgement of the US Terrorist Finance Tracking Program (henceforth TFTP) which has been initiated shortly after the September 11th, 2001 attacks. This program represents a paradigmatic example of the recurrent use of such subpoenas against commercial companies, here the Society for Worldwide Interbank Financial Telecommunication (henceforth SWIFT). Furthermore, such an example perfectly illustrates at least two major convergent trends of contemporary counter-terrorism frameworks, the "prevention" claim and the prominence of financial dimension.

In connection with proactive management of the elusive "terrorist risk," the former technique of "following the money" is not only associated with deterrent and investigative functions but also with (questionable) preventive performance (Biersteker and Eckert 2008; Levi 2010; Malkin and Elizur 2002). According to Louise Amoore and Marieke de Goede, "money laundering regulation is evolving from a regulatory tool designed to confiscate criminal money after the act (with a desired deterring effect) to a regulatory tool required to predict and apprehend potential terrorists" (Amoore and de Goede 2005:152). Indeed, using "terrorist finance" as an intelligence tool in the name of proactive form of prevention becomes one of the routine practices of current counter-terrorism strategies. The pervasive rhetoric of technological fix and "public-private" (mostly law enforcement-banks) partnership insists on IT equipment and co-production of intelligence to prevent "terrorist risk" (for an analysis of such a rhetoric in practice and the blurred notion of "terrorist risk", see Amicelle 2011; Favarel-Garrigues *et al.* 2009).

Besides the institutionalized production of "public-private" intelligence led policing, the US terrorist finance tracking program and its correlated transatlantic "SWIFT affair" refer to this convergent trend between preventive orientation and the financial part of counter-terrorism. The present paper precisely aims at analyzing this TFTP program. Its very existence and ongoing transformation are

officially presented as a new approach in the fight against "terrorism" and its financing.[2] Somewhat paradoxically, though, this so-called new step in financial intelligence and remote surveillance mainly remain an under-research area. While there have been many speculations and misapprehensions from various sides since the unauthorized leak on the TFTP existence, the paper primarily proposes an overview of the SWIFT affair. We set out to highlight the various issues at stake from the disclosure of the US system of transnational communication and processing of (commercial) personal data for security purposes to the project of a European equivalent system. Taking stock of the E.U.-U.S. harsh debate on this affair, we argue that the main critical surveillance issue of the TFTP is not where it is supposed to be.

The paper begins with the presentation of US media disclosure of the TFTP, the role of SWIFT, and an attempt to put into context the issue of "secondary use" of personal data regarding the relationship between security and privacy. Then, I try to show the very functioning of the TFTP and, above all, how its modalities of financial surveillance via technology of databases do not block or oppose to mobility but operate and run through this latter one. Ultimately, close analysis of European reactions after the TFTP disclosure and then the transatlantic negotiations on E.U.-U.S. TFTP agreement allows to say more about the state of European security integration. Thus, drawing upon primary sources and interviews at the European level, I question the increased access to and use of non-state databases for State purposes.

I. Secondary Use: Commercial Company's Databases for Counter-terrorist Purposes

While prevention is clearly presented as the ultimate goal of counter-terrorism and also administrative subpoenas and programs such as the TFTP, this stance refers to a specific form of prevention. Indeed, prevention here does not fit into the classical understanding in terms of sensitization and attempt to address the root causes of criminal or political violence. Moreover, prevention here does not correspond to another classical form of prevention, which is deterrence to the extent that it is difficult to look for such deterrent function from a program that has been conceived as an "invisible tool" for the general public. Thus, the TFTP highlights the current significance of a third meaning that it is the proactive form of prevention in which the rationale is to "act before the other," to prevent potential harmful events from happening (Bigo 2006). This particular logic of prevention exceeds traditional practices of criminal investigation and the framework of criminal justice because it is not limited to finding and prosecuting criminals before they reoffend. Access to information is not only authorized when a crime has been already committed to the extent that preventative transfer of data is privileged. Official requirements of retrieving a maximum of information are less focused on finding evidence to prosecute and punish than on amassing intelligence to pre-emptively disrupt and incapacitate (McCulloch and Pickering 2009).

I.1. Media Disclosure of the US Terrorist Finance Tracking Program

The Society for Worldwide Interbank Financial Telecommunication describes itself as a "member-owned cooperative through which the financial world conducts its business operations with speed, certainty and confidence."[3] In other words, SWIFT is the main worldwide messaging service dedicated to the facilitation of international financial transfer. 239 banks from 15 countries created this Belgium-based cooperative in 1973 in order to substitute the telex with a presumably secure and reliable

2. See European Commission Road map 2001 on the current project of a European TFTP: http://ec.europa.eu/governance/impact/planned_ia/docs/2011_home_003_terrorist_financing_tracking_en.pdf

3. See www.swift.com

means of transmitting financial instructions between institutions. This company is now controlled by 2,200 shareholders amongst which the biggest banks in the world. It provides standardized messaging services and interface software to over 9,500 banking organizations and other financial institutions in 209 countries. It has acquired a kind of systemic character, as a key infrastructure of the international financial system (Banque nationale de Belgique 2005). In 2011, SWIFT processed an average of 17 million messages on a daily basis for a total number of more than 4 billion messages in 2010.[4] According to official assessment, the SWIFT network channels about 80% of the electronic value transfers around the world (Council of the European Union 2007:2). Thus, many financial institutions use the SWIFTNet FIN service everyday for the worldwide transfer of messages pertaining to financial transfers between financial institutions. Over the course of 2006, a secondary use of its role as intermediary and payment system hub leads it to be publically indicted in what would come to be known as the "SWIFT affair."

On June 23rd, 2006, the *New York Times* disclosed the existence of a confidential financial surveillance program initiated by the American government in the aftermath of September 11th, 2001 (*The New York Times* 2006a). Pointing out the abuses that could result from the scope of this program, the long article revealed the central place of SWIFT in this "scandal. For more than four years, the American authorities had secretly accessed the messages passing through the "central nervous system of the global banking industry" (*ibid.*) to trace the financial transactions of individuals suspected of terrorism. With the *New York Times* having clearly taken it upon itself to act as "whistleblower" (on this notion, see Chateauraynaud and Torny 1999), other papers decided to follow its lead and at the same time revealed that SWIFT had transferred copies of interbank messages coming from all part of the world (*The Los Angeles Times* 2006; *The Washington Post* 2006a; *The Wall Street Journal* 2006). The same day, two American lawyers launched a suit in order to take the business to court for violating their right to privacy (Köppel 2009:16-17). Once opened, the content of a SWIFT message concerning the payment of a bank client does indeed contain the amount of transaction, the currency, the date, the name of the originator's bank and the recipient client. It also provides information about the beneficiary and the ordering customer such as name, account number, address, national identification number and other personal data (General Secretariat of the Council of the EU 2009; Commission de la protection de la vie privée (Royaume de Belgique) 2007).

The reactions and reports that followed this public revelation contributed further information as well as a few corrections but ultimately confirmed most of the facts that had been presented in connection with the US Program. This program began almost immediately after September 11th, 2001, and given that the consent of the American Congress had not been a prerequisite of its application, it does not seem excessive to describe it as "secret" except for specialized communities working on terrorist financing issues and few members of the Congress. A division of the Treasury Department, the Office of Foreign Assets Control (OFAC) justified its action by reference to American statutory mandates (mention is made of The International Emergency Economic Powers Act of 1977 and The United Nations Participation Act of 1945) and the executive order 13224 authorizing the Department of the Treasury – in coordination with other federal agencies – to "use all appropriate measures to identify, track down and pursue" terrorist groups and their supporters (US Department of the Treasury 2006b). Using this legal basis, OFAC made do with issuing subpoenas that systematically constrained SWIFT to extract and transmit copies of messages requested on the basis of shared criteria (mainly dates and countries). Moreover, US Authorities have quickly described the TFTP – after the media disclosure – as a powerful investigative tool allowing for the generation of leads as well as for the identification and capture of "terrorists" and their financiers. But beyond a simple exercise to justify the legality and added value of its program, the Bush administration above all deplored the attitude of the press, stigmatizing it for having caused unpardonable harm to national security. This extremely critical stance would continue to deepen in the days following the revelations of the *New York Times*, giving rise to a genuine "reversal of the scandalous accusation against the accuser" (de Blic and Lemieux 2005:17).

4. See www.swift.com

In short order, it was no longer the generalized surveillance program that was called into question but rather the public act that revealed it. The initial scandal proved to have only been a brief opening sequence for what would become the "SWIFT affair" (On the game by means of which scandals are transformed into affairs, see Lemieux 2007). Republican Congressman Peter T. King (chair of the House Homeland Security Committee) went so far as to demand that an inquiry be opened and criminal proceedings initiated against the *New York Times*, accusing it of "treachery" in times of war (*The Washington Post* 2006b). Although other politicians did not share this point of view,[5] the virulence of political (and also in some cases public) reactions finally pushed Byron Calame (the New York paper's mediator) to justify the article's publication. In an opinion column dated July 2nd, 2006, Calame began by putting the secret nature of the surveillance program into perspective, underscoring the fact that it had been mentioned as early as 2002 in a public report from the United Nations (*The New York Times* 2006b[6]). From there, he proceeded to acknowledge that discretion is of course a vital element in information-gathering operations but pointed out that this should not exclude supervision by elected representatives and claimed that weak supervision by Congress justified public discussion of a temporary emergency measure that had become permanent (*ibid*.).

From this point of view, the particular example of the TFTP echoes the general issue of emergency measures deemed temporary but which tend to become *de facto* permanent. With reference to counter-terrorism practices, the situation of "temporary permanence" is historically well known (see for instance Donohue 1999; 2001). Other current practices have been criticized for similar reasons such as blacklisting and asset-freezing measures (i.e. the United Nations "terrorist lists" program). Martin Scheinin – UN special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism – has expressed concern that such supposedly temporary administrative measures turn out to be indefinite (UN General Assembly 2006). Regarding the financial aspect of counter-terrorism, the blacklisting and freezing approach is related to the preventive framework. While implementation of official terrorist lists also responds to a dual logic of deterrence and political spectacle (providing reassurance via visible state initiative, Edelman 1988), the very design of this approach is clearly preventive. The public designation of groups and individuals as suspected terrorists on the one hand, the freezing of their financial assets on the other hand, fall into the purpose of pre-emptive disruption. Such proscription constitutes a preventive intervention to the extent that listed entities have often received no trial and most of them are not even judicially prosecuted. The aim is less to condemn guilty parties than to incapacitate suspects. Blacklisted persons are suspects of "terrorism" following an executive decision, on the basis of intelligence outside judicial review. In other words, official blacklists "circumvent the 'normal' criminal procedure by placing the power to designate an individual or group as 'terrorist' in the hands of the executive and then preventing national courts from exercising judicial review of those designations. This effect is not simply an unforeseen by-product of the blacklisting regimes, but rather its raison d'être" (Hayes and Sullivan 2011:82). Hence, while confiscation of funds is related to a judicial criminal charge, asset-freezing is linked to a simple administrative measure. However, the difference between the permanence of a punitive decision and the temporariness of an administrative decision might be blurred in practice for individuals who have been blacklisted for more than five or even nine years (*ibid*.; Amicelle and Favarel-Garrigues 2009).

Michael Levi and David Wall also remind that once in place in the name of security emergency, mass surveillance technologies become "institutionalized and very hard politically to dismantle" (Levi and Wall 2004:210). Hence, "temporary permanence" mainly refers to the phenomenon of "ratchet effect" which underlines the extreme difficulty to reverse processes once they have been launched, even in the name of an exceptional situation of violence (Bigo and Guittet 2004). Furthermore, this

5. Arlen Specter (President of the Senate Judicial Committee), for example, held that: "On the basis of the newspaper article, I think that it is premature to call for legal action against the *New York Times*, just like I think that it is premature to say that the administration is completely right" (*The Washington Post* 2006b).

6. The report mentioned without further references being: Security Council, *Third Report of the Follow-up Group in Application of Paragraph 10 of Resolution 1390*, December 17th, 2002, point 31, p. 12.

phenomenon raises additional questions when it is associated with security practices that have been initially implemented in government secrecy, such as the TFTP, simply framed by executive-centered government and SWIFT standards. Without media disclosure, the TFTP would have remained under the radar of public or congressional committee scrutiny.

Several months later, however, the public controversy would push Byron Calame to make his public *mea culpa*, expressing regret that the July opinion piece had been published and acknowledging the apparent legality of the Terrorist Finance Tracking Program as well as the absence of evidence demonstrating that personal data collected under its aegis had been misused (*The New York Times* 2006c). Finally, in October 2007, the suit brought by the two lawyers on June 23rd, 2006, was dismissed, the judge having concluded that the plaintiffs did not offer sufficient evidence to support the claim that their personal data had been directly targeted by the Terrorist Finance Tracking Program.[7] The federal government was in any case one step ahead, announcing in August 2007 that it would call upon the legal tool of State Secret Privilege to halt any and all legal action against SWIFT (*The New York Times* 2007).

The framing of the US debate on the TFTP is highly interesting with regards to "surveillance studies" (see for instance Lyon 2007) and the security/privacy debate. Although the disclosure of the SWIFT case raised questions and denunciations in terms of government excess of surveillance, it is not as easy to formulate what is at stake in it. Indeed, it is extremely difficult to identify with the potential victims in this case as the use to which transmitted information is put is unknown, and the effects of their revelation are not tangible. Given that the identity of the victims is unclear, the damage caused to them uncertain and responsibility for it profoundly intertwined and difficult to discern, mobilization in the SWIFT affair struggles to take root or, for that matter, even to provoke public anger. Moreover, one can easily imagine that even if the two plaintiffs succeeded to prove the government's access of their (SWIFT) data, the court would have rejected the lawsuit because the two lawyers could not prove any "admissible harm." Indeed, although Daniel Solove does not develop his arguments on TFTP as such, he studied similar cases of information dissemination which were not necessarily linked to counter-terrorism purposes (Solove 2007).

> For example, after the September 11 attacks, several airlines gave their passenger records to federal agencies in direct violation of their privacy policies [counter-terrorism purposes] [...] A similar problem surfaces in another case, Smith v. Chase Manhattan Bank. A group of plaintiffs sued Chase Manhattan Bank for selling customer information to third parties in violation of its privacy policy, which stated that information would remain confidential [commercial purposes] (*ibid.*)

Both groups of plaintiffs were ultimately dismissed but Solove argues that court rulings reveal less the absence of privacy problems than the difficulty with the legal system in "recognizing harms that do not result in embarrassment, humiliation, or physical or psychological injury" (*ibid.*).

Cases such as the two examples or the TFTP refer to the problem of secondary use regarding information dissemination and information processing. "Secondary use involves data collected for one purpose being use for an unrelated purpose without people's consent" (*ibid.*; see also Solove 2006). Hence, the US Treasury has processed SWIFT data for purposes far beyond the scope of their original gathering. Solove acknowledges that such privacy problem frequently does not give rise to material (i.e. financial or physical) nor psychological injuries but, according to him, it is still harmful despite this fact. Hence, the harmful dimension tends to be a structural one to the extent that it concerns not so much particular individuals than populations as a whole. The harm is structural because it consists in power imbalance between SWIFT and its indirect users (i.e. banking customers) and between citizens and their government (and even between US government and non US citizens nor US permanent

7. District Court for the Eastern District of Virginia, *Ian Walker and Stephen Kruse, Plaintiffs, v. S.W.I.F.T. SCRI, Defendant*, 517F. Supp. 2d 801, 2007, pp.517-525v (Köppel 2009).

residents).[8] First of all, individuals are *de facto* put in a powerless position vis-à-vis SWIFT and SWIFT direct users (i.e. individuals' banks) because their data has been shared and processed in a way they could not know. As Solove states for his example regarding airlines passengers, the issue is not to question whether or not people know privacy policy of companies such as SWIFT. The issue is to understand that in any case there is a "social value in ensuring that companies adhere to established limits on the way they use personal information. Otherwise, any stated limits become meaningless, and companies have discretion to boundlessly use data" (Solove 2007). Secondly, individuals are also left in a powerless position in connection with their relationships with the US government. Indeed, US Treasury Department and US federal agencies have processed SWIFT personal information without citizens' knowledge or involvement, and without Congress oversight. Hence, individuals' powerless position is not so much related to the very existence of the TFTP than it is related to a mechanism of oversight and issues of public accountability to the extent that this existence was kept secret for the population and the Congress (as an institution) for five years.

This focus on the problematic of power imbalance reflects an underrated facet of the security/privacy debate regarding the TFTP disclosure which would deserve further analysis. Such secondary use of personal data raises specific privacy problems although there is no identification of individual cases of emotional or material injuries and that many people could state they have "nothing to hide" regarding what they might consider as non sensitive financial personal data. This problem of secondary use questions the relationships between businesses and end customers on the one hand, relationships between executive power and citizens on the other hand, and how programs such as the TFTP affect social structure by altering these relationships. As security issues, privacy ones should also be interpreted and analyzed in terms of collective and societal interests (Solove 2007).

I.2. SWIFT, Mirror and Black Box: How Does TFTP Work?

Under the TFTP, the Treasury Department's Office of Foreign Assets Control (OFAC) has thus issued administrative subpoenas ("investigative tools") requiring SWIFT's US operating centre to provide access to financial transaction records yielded by their US server. To be clear, the provision of a highly significant amount of US-stored messaging data does not mean that US Treasury has only accessed to US-related transactions. OFAC representatives have also accessed to interbank messages between countries that are not the United States and with personal data that are not linked to US citizens or US entities. This access to worldwide financial data stored by SWIFT has been technically feasible because the company runs two operating centers for its ordinary messaging activities[9]. One is located in the E.U. (in the Netherlands) and the other in the U.S. At these centers, the cooperative stores its millions of daily messages – that are transmitted everyday via its "SWIFTNet FIN" service – for commercial purposes, mostly as part of their service to customers "in case of disputes between financial institutions or data loss" (Article 29 Data Protection Working Party 2006). All messages are kept for a period of 124 days in the EU and US servers that "mirror" the financial data in order to provide "backup," should one of the servers crash.[10] Thus, SWIFT messages are initially collected for a limited amount of time as a classical routine practice to ensure commercial continuity in case of failure regarding one of the operating centers. Consequently, the US actors have issued orders on SWIFT with the aim of accessing and processing messages of interbank transactions stored by the company for business purposes.

Although the TFTP seems to be a specific project, it is part of a general trend of using databases held by commercial companies for counter-terrorism purposes.[11] There has been a continuous pressure

8. We will see that the US TFTP does not only concern, by far, American people.

9. We will see that this state of affairs has slightly changed since January 2010.

10. "Mirroring" constitutes a form of data processing meaning that the two servers "provide an exact copy of the data held by the other" (European Parliament 2007a).

11. Although it is not perfectly similar, another famous case is the PNR (Passenger Name Records) involving personal data

to access personal data and to use it for aims that are different from the ones it initially was collected for. The US Treasury's administrative subpoenas have enabled this kind of unilateral "exchange" of information stored in commercial databases. These "investigative tools" are imbued with a preventive approach focusing on the proactive surveillance of flows. According to SWIFT, at the end of 2006, it had received and complied to 64 subpoenas since September 11. It should be mentioned that the Treasury's searches on SWIFT data follow two steps. First of all, their requests are not individualized but quite general. Indeed, US SWIFT's operating centre has not the technical capacity to respond to targeted queries because of the codified structure of SWIFT messages. Hence, the broad scope of queries is defined in the subpoenas and it is "materially, territorially and in time very wide: these subpoenas are issued for any transactions which relate or may relate to terrorism, relate to X number of countries and jurisdictions, on *a* date, or 'from … to …' dates ranging from one to several weeks, within and outside the U.S." (Article 29 Data Protection Working Party 2006); "The SWIFT isn't made in the way that you can say I want M. X's transfers on the 16th of November, the 8 of June and 9 of August. It's not the system, you can always get a bulk" (Interview with European Official 2008). In concrete terms, the Treasury Department does not directly extract individualized data pertaining to a specific suspect. The broad "subpoenaed messages" are provided by the SWIFT operating centre in the U.S. and transferred into a "US Treasury black box." Secondly, US authorities use their own designed software in order to automatically decipher SWIFT messages and to launch name searches within their searchable database (the so-called "black box") (Commission de la protection de la vie privée (Royaume de Belgique) 2006a; General Secretariat of the Council of the EU 2009). Thus, they verify whether specific names appear in messages.

As a result, concerning the processing, the Treasury Department has asserted that "data provided by SWIFT is searched to extract only information that is related to an identified, pre-existing terrorism investigation" (OJEU 2007). Despite widespread concern about data mining procedures, US authorities have certified that it is not a "fishing expedition in the black box" (*ibid*.; Interviews with European Officials 2007-2008) and that there is no data mining nor automated profiling.[12] According to Under Secretary Stuart Levey, the data cannot be searched when there is no "terrorism nexus." Treasury Department representatives underline that US counter-terrorism analysts have ultimately opened and seen less than one percent of the subset of SWIFT messages stored in the searchable black box (*ibid*.). Consequently, the TFTP does not involve a surveillance operating on the basis of automated profiling aiming at the identification of "populations at risk" through recognition pattern tools. As opposed to technologies developed to detect pre-established patterns of suspect behavior or suspicious transactions, it would only involve localization technologies focusing on suspect individuals or suspect entities. Beyond any doubt, the TFTP exemplifies one of the technical forms taken by (financial) intelligence through databases and surveillance models based on the tracing of flows. According to this understanding, security can only be promoted provided the traces left by financial flows are followed. Contemporary financial intelligence is precisely associated with the willingness to take advantage of information technologies in order to identify, monitor and so manage the flows. To the extent that they promote fast, real-time transactions almost all over the world, technological developments would also enhance surveillance by leaving "electronic traces" which enable "money trails" in and out of sovereign territories (Levi and Wall 2004).

Practices of control hence feed on financial circulation, rather than attempting to curtail it. Indeed, control and surveillance at a distance suppose mobility without which they would lose their critical enabler. Thus, the US SWIFT server turns out to be one of the crucial pieces of an "assemblage" of mobility control. As a transnational database, the financial transaction records provided by SWIFT are claimed to allow for the identification and location of suspects as well as for the monitoring and analysis of their relationships. In the immediate aftermath of media disclosure, the US Treasury has immediately

transfer of passengers of transatlantic flights (see Salter 2008; Mitsilegas 2008).

12. Automated profiling is the result of a data mining process, which is "a procedure by which large databases are mined by means of algorithms for patterns of correlations between data" (Hildebrandt 2008:18). In other words, with regards to counter-terrorism, "data mining involves creating profiles by collecting and combining personal data, and analyzing it for particular patterns of behaviour deemed to be suspicious" (Solove 2008:343).

justified the TFTP by alleging that it has enabled the localization of suspects and the finding of addresses or links between known and "unknown terrorists" (US Department of the Treasury 2006a).[13] Consequently, the TFTP deploys mobile forms of surveillance that can be conceptualized as a kind of localization technology – tracking financial movements of suspects – which would allow for "social network analyses" (de Goede 2008) to map individual connections.

> "Following the money" is one of the most valuable sources of information that we have to identify and locate the networks of terrorists and their supporters. If a terrorist associate whom we are watching sends or receives money from another person, we know that there's a link between the two individuals. And, while terrorist supporters may use code names on the phone, when they send or receive money through the banking system, they often provide information that yields the kind of concrete leads that can advance an investigation. For these reasons, counter-terrorism officials place a heavy premium on financial intelligence. As the 9/11 Commission staff pointed out – and as Chairman Hamilton testified before this Committee – "following the money to identify terrorist operatives and sympathizers provides a particularly powerful tool in the fight against terrorist groups. Use of this tool almost always remains invisible to the general public, but it is a critical part of the overall campaign against al Qaeda." The Terrorist Finance Tracking Program was just such an invisible tool. (US Treasury Department Office of Public Affairs 2006)

Nevertheless, the massive access to personal data by US authorities has often been met with criticism and doubt. Besides the exclusively American aspect of the debate, the SWIFT affair is also and above all marked by its transatlantic dimension. The following section analyses the numerous tensions and ambiguities revealed by the "SWIFT case" in order to highlight what is at stake in transatlantic counter-terrorism relationships and what the TFTP tells us on intra-European tensions and European security integration.

II. Transatlantic Ambivalence and European Tensions

As soon as the existence of the TFTP became public, the disclosure of massive and long-term interception of bank transfer data from SWIFT by US services produced a political and legal shockwave in the E.U. The press reports basically claimed that US authorities had access to information on millions of EU citizens. Due to the programme's secretive character, the U.S. appeared to have successfully forestalled possible negotiations with European institutions and secretly monitored European population's (and others') financial transactions during five years.

II.1. European Union: A Unitary Actor on the "SWIFT Affair"? Not at All

The revelations concerning the financial surveillance program were picked up in Europe where part of the media sphere was quick to report them (*The Guardian* 2006; *Le Monde* 2006; *Le Soir* 2006), calling into question the collaboration between SWIFT and the American Treasury from the perspective of European legislation concerning the protection of personal data. Located in Belgium, the

13. We will see that two official reports for the E.U. have insisted, since 2008, on the value of TFTP-derived information with several examples.

cooperative company is actually subject to European law. In July 2006, it was revealed that European institutions, such as the European Parliament and the European Commission, had not been informed of the existence of this US security measure claimed to contribute to the common fight against "terrorism." The European Parliament strongly regretted that it had not been informed of the secret agreement between the global messaging company and the US administration (European Parliament 2006, 2007b). Referring to the journalistic inquiries and to a complaint lodged by the organization Privacy International,[14] the European Parliament adopted a resolution on this subject on July 6th, 2006, less than 15 days after the first information was divulged. There, the Members of European Parliament (henceforth MEPs) expressed their disappointment at having been kept in the dark and worried over the "creation of a climate marked by eroding respect for privacy and the protection of data" (*ibid*.). Given the crucial role played by the SWIFT network for European banks, the fact that it had been put under surveillance heralded massive access on the part of American authorities to the confidential information of millions of European citizens without the consent of EU institutions. The text of the resolution moreover insisted on the issue of economic sovereignty, denouncing the danger (at least theoretical) of large scale economic and industrial espionage resulting from the unsupervised communication of this data to third countries (in this case, the United States).

The general secretariat of the European Council and the Commission as a whole did not appear to have more knowledge on the subject matter than the MEPs, they learned of the "SWIFT matter" through the media. As claimed by numerous Commission officials, there was a "political shock" for two reasons. On the one hand, the TFTP notably involves personal data collected in Europe over several years, thus allowing for a particularly intrusive form of surveillance. On the other hand, although there are some differences in practices and discourses, the E.U. clearly claims to have the same political goal as its transatlantic partner in the fight against "terrorism." Thus, "it is quite surprising for a partner to read newspapers and to hear that the other partner is combing through the files of a European company (SWIFT) for a counter-terrorism purpose without informing the other" (interview with European Official, October 2007). The Belgian data protection authority, the "Article 29 data protection working party" (henceforth G 29)[15] and the European Data Protection Supervisor (henceforth EDPS)[16] also expressed serious concern and stressed the secret character of the US program. Accordingly, in spite of US first official statements on efficiency and legal safeguards, the TFTP has raised skepticism and concern within various EU institutions to which, according to officials discussing the very logic of the program, no other choice was left – just after media disclosure – than to trust US authorities. "The US Terrorist Financing Tracking Program is a very secret project, we don't get any access and I don't know what the added value, or the success factor of that is; I am not sure what they are doing really, we had a lot of difficulties with the U.S. when we were discussing the 'SWIFT case' to get a real picture of this program, because you can say whatever you want, but are they really restricting the program to terrorism financing and terrorism attacks? There will always be a discrepancy between what they are saying and what they are doing with the information. We have to take what they say for granted because we have no access, we have no insight information" (Interview with European official, September 2007). Both quotations represent a kind of ideal-type of the European officials' discourse

14. Starting in June 2006, this association for the defence of human rights, which specializes in monitoring government and business surveillance practices, lodged a complaint with bodies overseeing the protection of data and privacy in 33 countries. See www.privacyinternational.org

15. Created by Article 29 of the 1995 European data protection directive, this working group brings together representatives of each of the Member State's independent national data protection authorities. The mission entrusted to the G 29 consists in contributing to the elaboration of European norms by adopting recommendations, rendering opinions on the level of protection in third countries and advising the European Commission on any project having an impact on the rights and liberties of physical persons in regards to the treatment of personal data.

16. The office of the European Data Protection Auditor was created by (EC) Ruling no.45/2001 relating to the protection of physical persons in regards to the treatment of personal data by community institutions and agencies and the free circulation of data. An independent institution, its objective is above all to oversee the way in which personal data is processed by the EU administration.

following disclosure of the US program. However, such general discourse does not mean so much that all European actors were unaware of the TFTP than main European institutions were simply out of the loop.

The investigations carried out by data protection authorities show that the Central Banks of the Group of Ten countries (G 10 Group[17]) knew of these data transfers by 2002 (Commission de la protection de la vie privée (Royaume de Belgique) 2006a; Article 29 Data Protection Working Party 2006 ; European Data Protection Supervisor 2007). Given the company's global reach, the G 10 Group had set up an oversight mechanism focusing "primarily on ensuring that SWIFT has effective control and processes to avoid a risk to the financial stability and the soundness of financial infrastructures" (European Data Protection Supervisor 2007). Indeed, the European Central Bank (ECB) belongs to the group of ten central banks which supervise the activities of SWIFT. As such, it had been aware of the Terrorist Financing Tracking Program since 2002. However, the ECB did not contact European authorities to keep them informed. It justified this omission in the name of a strict interpretation of the G 10 Group's secrecy rules, arguing that the data-transfer and breaches to data protection rules were not within the remit of its oversight mechanism. Thus, according to this institution, the rules of confidentiality and the limited field of action inherent to its supervisory role did not allow it to pass on information to European data protection authorities nor to put pressure on SWIFT to do so. This restrictive interpretation was seriously challenged by the European Data Protection Supervisor (*ibid.*).Moreover, the main ambivalence came from within the European Council. Much more than a simple legal and technical affair, the SWIFT case was undeniably accompanied by a political dimension. Having learnt of the existence of the surveillance program via the press, both the European Parliament and the European Commission experienced it as a profound political shock exacerbated by the silence of such institutions as the ECB (interview with European Commission officials, Brussels, December 2007 and May 2008). In December 2006, the Belgian Privacy Commission issued a second opinion, urging European governments to not remain silent given the "justified grounds of protest."[18] Nevertheless, the unanimous criticism of data protection authorities came up against the apparent indifference of Member States. In lieu of a diplomatic condemnation, some of them – including France and the United Kingdom – on the contrary hastened to testify before the EU Council so as to the veracity of American claims regarding the program's usefulness for fighting terrorism, including in Europe (interview with European Commission officials, Brussels 2007).

First of all, some officials of the G 10 group have decided to inform their Justice and Interior Ministries about the existence of the TFTP (Interviews with European commission and Council officials 2008). Secondly, the intelligence services of some Member States had indeed received information from the Terrorist Finance Tracking Program via informal bilateral relations all along.[19] To some extent, this situation illustrates the absence of practical coordination between Member States at EU level in the field of the fight against terrorism and its financial aspects. Operational cooperation tends to be mostly bilateral. Some Member States' relationships to non-EU states play a significant role, especially with the U.S. The financial intelligence extracted from SWIFT via the TFTP has been thus exchanged in an informal and bilateral environment precluding any formal consultation of the "E.U. 27" and of the European arrangements. Seen in this light, while the TFTP illustrates US relationships with individual Member States, it mainly highlights the state of affairs regarding European security coordination and integration.

17. The G 10 Group is composed of the National Bank of Belgium, Bank of Canada, Deutsche Bundesbank, European Central Bank, Banque de France, Banca d'Italia, Bank of Japan, De Nederlandsche Bank, Sveriges Riksbank, Swiss National Bank, Bank of England and the Federal Reserve System (USA), represented by the Federal Reserve Bank of New York and the Board of Governors of the Federal Reserve System.

18. "The observation that, for years, the personal data of their citizens had been the object of a large-scale and hitherto uncontrolled and unilateral investigation by the authorities of a state with which close collaboration takes place in itself constitutes justified grounds of protest." Commission de la protection de la vie privée (Royaume de Belgique) (2006b).

19. As Gilles de Kerchove (European coordinator in the fight against terrorism) indicated during a public conference, *Challenge International Conference: The Exchange and Storage of Data*, Sciences Po, Paris, 10-11 October 2008.

II.2. Privacy and Economic Sovereignty: European Concerns and SWIFT Re-Architecture

With reference to their harsh critics on the US program, MEPs and data protection agencies have mostly insisted on privacy and economic issues. Beyond the issue of SWIFT's and financial institutions' (such as the European Central Bank's) co-responsibility, they have mainly emphasized the violations of fundamental European principles regarding data protection. The legal analysis of the latter is beyond the scope of this article (see Gonzales Fuster, de Hert and Gutwirt 2008). It is however worth mentioning that problems concerning the level of protection for the international transfer of personal data are involved, as well as questions pertaining to the guarantees for the transfer of data to a third country, the principle of proportionality and necessity, transparency and independent control mechanisms of the data processing, the right for the financial institutions' individual clients to be informed about how their personal data is processed and that US authorities might have access to such data. Although US representatives have always denied any use of a data mining process, this specific issue has remained a running concern for members of the European Parliament and data protection authorities.

With the matter having been referred to them for judgment, the Belgian and European data protection authorities made it their priority to deal with the affair. In September 2006, the Belgian Data Privacy Commission was the first to hand down an opinion. For the Commission, the crux of the issue turned on the role played by SWIFT in the transmission of personal data to the American Treasury Department. Its conclusion was free of all ambiguity: the systematic, massive and secret nature of the practices as well as the long duration of the effort vis-à-vis the OFAC constituted a violation of fundamental principles of the European legal order (Commission de la protection de la vie privée (Royaume de Belgique) 2006a). A public hearing was then held in early October 2006 by the European Parliament: it supplied Francis Vanbever (at the time financial director of SWIFT) with an opportunity to present the company's position. Vanbever rejected the opinion of the Belgian authority and, underscoring the particular legal status of SWIFT and the limitations negotiated with the Treasury,[20] challenged the claim that the company had committed any breach of European legislation. Presenting itself as a victim of legal conflict caught in a vice between Belgian data protection laws and American antiterrorist laws, the SWIFT Company reiterated its call for transatlantic dialogue on these issues.

Yet, notwithstanding SWIFT's efforts to present itself as the victim of competing legal forms, the later opinions of the G 29 and the EDPS did not differ from the Belgian assessment. As a result of a concerted effort, the G 29 opinion confirmed that infractions had been committed and condemned the circumvention of "existing mechanisms allowing for independent oversight of [financial] data processing" (Article 29 Data Protection Working Party 2006). Judging that this security-conscious use was disproportionate and incompatible with the original commercial aims of SWIFT data processing, the G 29 opinion held that this practice was capable of having direct repercussions on the life of the individuals whose data was concerned. Also called into question, European financial institutions – direct consumers of the SWIFTNet Fin service – were ordered to inform their clients of what had become of their personal data and the possibility that this information had been accessed by the American authorities. For the most part, they did this by way of inserting a box on their web page.

The Presidency of the European Council – held by Germany at the time of the talks with the US Treasury in the first semester of 2007 – was particularly worried by US access to intra-European SWIFT data (interview with European officials, 2007). Many European officials shared this stance and had the feeling that they were not treated as real partners by US authorities. The latter have not seemed to accept the idea that the collaboration that enables them to access data on European populations

20. Vanbever insisted on the safeguards obtained by SWIFT regarding the US storage of the subpoenaed data and added that "SWIFT has representatives on site at the Treasury. They review every query. They can stop any query in real time if they are not satisfied that it is related to an ongoing investigation into terrorism financing" (European Parliament (Hearing) 2006).

would have to be counter-balanced by a control on the part of the Europeans over their internal system and their use of this data.[21]

As a result, questions pertaining to the use of the data collected through SWIFT triggered widespread concern in Europe over economic and industrial espionage. Efforts on the part of the Department of Treasury to trace international banking system transfers of funds to and from "terrorists" also give access to "information on the economic activities of the individuals and countries concerned" (European Parliament 2006). The European Parliament and the EDPS have continued to highlight a risk to economic sovereignty since a third country (the U.S.) could access data on the commercial transactions of European companies without safeguards on the purposes of the data-transfer. European authorities thus complained about the danger of "function creep" from counter-terrorism to economic espionage. Finally, the data protection authorities have argued that the type of violations epitomized by the "SWIFT case" may threaten the financial stability of the payment system.[22] This statement represents a quite ironic reversal of official lines of argumentation on counter-terrorism since the data-transfer involving SWIFT is here defined as illicit flows undermining one of the official aims of the fight against terrorism financing. "Terrorism" is indeed perceived as a "threat to financial stability" (Basel Committee on Banking Supervision 2002) and the preservation of the integrity of financial institutions and the financial system is at the heart of counter-terrorism financing measures. The "SWIFT case" has hence been seen as a potentially counter-productive operation to the extent that it would slip into a paradox in which it would risk to endanger one the referent object (i.e. financial system) that it claims to secure.

Eventually an agreement was reached on the use of SWIFT data. During the first semester of 2007, the informal negotiations exclusively involved the US Treasury Department, the European Commission (DG Justice, Liberty and Security) and the German presidency of the European Council (through its Ministry of Finance) assisted by the Council Secretariat (mainly Gilles de Kerchove who was no yet the EU counter-terrorism coordinator). On June 28 of the same year, a set of unilateral commitments on the part of the US Treasury was disclosed as a result of the informal talks. "We did not need to have an official international agreement. If we could avoid an international treaty, in other words if we could do something simpler it is better because international treaty is much more complicated than a unilateral representation" (interview with a European commission official, March 2008). The so-called US "representations" include "insurances" that SWIFT data be used strictly for counter-terrorism purposes with internal safeguards and data retention obligations.[23] They include above all the appointment of an "eminent European" by the European Commission in consultation with the United States Department of Treasury. The French Judge Jean-Louis Bruguière was designated as the "eminent" person in 2008 and mandated to exercise independent oversight over the use of SWIFT data in order to confirm that US commitments are effectively met.[24]

Finally, the definitive opinion of the Belgian Privacy Commission (December 2008) seemed to mark the end point of the affair. This Commission had prolonged its investigations over a two-year period and had made a 180-degree turn with regard to its initial, 2006 positions (Privacy Protection Commission (Kingdom of Belgium) 2008). Any idea of legal proceedings against the cooperative society was abandoned since the decision concluded that the surveillance program was legal and that the data passed on by SWIFT had benefited from adequate protection (*ibid*.). The Belgian authority in part

21. Bigo, Didier. Unpublished working-paper, 2008.

22. "…the lack of compliance with data protection legislation may actually hamper also the financial stability of the payment system for at least two reasons: first of all, it could seriously affect consumers trust in their banks; secondly, it might lead European data protection authorities, as well as judicial authorities, to use their enforcement powers to block the processing of personal data which are not in compliance with data protection law" (European Data Protection Supervisor 2007).

23. Terrorist Finance Tracking Program – Representations of the United States Department of the Treasury, *op. cit*. Interviewees underline that data retention obligations were significant part of the negotiations because US authorities wanted to retain data for 40 years while the agreement finally imposes no more than five years (which is already a significant amount of time).

24. The main conclusions of his first report, which were presented in February 2009, officially insisted on the US privacy safeguards and the value of the TFTP in the fight against Terrorism, "notably in Europe" (Europa Press release 2009).

justified this about-face with reference to what had until then been little known facts, even though it was above all the efforts to which SWIFT had consented since 2006 which implicitly supported what was, *a priori*, a surprising decision (for an interpretation of the strategy of the data protection authorities, see Köppel 2009). In this respect, moreover, the final opinion only confirmed that advanced by its European counterparts beginning in October 2007. Under pressure once the existence of the US program had been made public, SWIFT had never fundamentally abandoned its defensive posture. In practice, however, it resigned itself to modifying the technical architecture of its network in order to protect its reputation (SWIFT press release 2007). Starting in late 2007, these changes were very favorably received by data protection agencies which, claiming credit for them, spoke of the "end of the crisis" (Article 29 Data Protection Working Party 2007:1; CNIL 2007:23-24).

The restructuring of the SWIFT electronic message architecture came down to the implantation of a new operational centre in Switzerland (scheduled for late 2009) so that the data from messages relating to European transactions should remain in Europe from now on. The SWIFT board of directors decided to partition messaging services into two distinct zones, the "Transatlantic zone" and the "European Zone" which is not limited to the E.U. The European messaging zone covers the European Economic Area (E.U. 27 + Norway, Iceland and Liechtenstein), Switzerland and territories associated with EU Member States. The transatlantic messaging zone covers the U.S. and its territories. All other States are by default assigned to the latter zone but they can request to be re-allocated to the European one. Therefore, the decision of re-architecture requires that each zone would have their proper pairs of operating centers that gather data for each zone. With regards to this re-architecture, the routine process of data mirroring continues but it becomes intra-zone to the extent that messages from the European Zone would only be stored in Netherlands and Switzerland. In other words, intra-European traffic would be strictly kept in SWIFT European operating centers, no such data would be mirrored with the US branch server anymore. At this moment, the US TFTP would exclusively concern messages to or from the transatlantic zone and would no longer include those emitted among clients present on the European Zone.

However, this new stance rather represents the conclusion of the first "round" than the end of the "SWIFT case." Indeed, in 2009 the fragile consensus of 2008 gave way to new disagreements, but this time between European institutions as well as between Member States (and even between ministers of national governments). It is precisely the modification in the SWIFT architecture that triggered these new harsh discussions.

II.3. Towards a European Terrorist Finance Tracking Program

Transatlantic informal negotiations resumed in 2009 to allow for the US TFTP to continue consulting SWIFT data unrelated to US territory (interview with an adviser of EU permanent representation of a Member State, May 2009). In July 2009, the European Council mandated the Commission and the Swedish presidency of the E.U. to strike a new deal. The E.U.-U.S. negotiations aimed to ensure US access to intra-European zone financial data-transfer in spite of their relocation to two SWIFT operating centers in Europe (in the Netherlands and Switzerland) at the end of 2009. Thus, the purpose of these negotiations was to anticipate the effective delocalization of the Belgian business' operational centers. Once again, becoming aware of this project by way of the press, MEPs were quick to complain to the Commission. This was reflected in the adoption of a new resolution meant to reiterate what were considered to be the necessary conditions for ensuring respect of privacy and the protection of data (European Parliament 2009a). Reviving fears of the potential for economic and industrial espionage, the deputies also solicited a number of minimal guarantees such as a mechanism of reciprocity "obliging the competent authorities of the United States to communicate upon request the relevant financial transfer data to the competent authorities of the Union" (*ibid.*). Unlike the Parliament, the

European Data Protection Supervisor was indeed consulted by the Commission in July 2009, giving him the opportunity to express doubts concerning the legal basis of the agreement (European Parliament 2009b). Finally, the Council of the E.U. found it difficult reaching a common position, with Austria and mainly Germany expressing reservations in regards to the level of data protection that had been agreed upon (*European Voice* 2009). A diplomatic cable from the US embassy in Berlin reveals how American diplomats "'were astonished to learn how quickly rumors about alleged US economic espionage' had taken root among German politicians who opposed the program" (*New York Times* 2010.) They identified Germany as the strongest holdout with regards to the project of agreement.

Such opposition in Germany led to US intense lobbying, which showed how the SWIFT case had not only raised intra-European tensions but also intra-governmental frictions. Indeed, the set of transatlantic negotiations coincided with the re-election of Angela Merkel in September 2009 and the end of the "grand coalition" with the SPD (Social Democratic Party). Merkel was able to form a new governing coalition between CDU/CSU (Christian Democratic Union/Christian Social Union) and FDP (Free Democratic Party) that had become the junior coalition partner. These new partners did not share the same views on the TFTP to the extent that several FDP leaders expressed concerns from the beginning of the Swedish negotiated mandate. Moreover, Justice Minister Sabine Leutheusser-Schnarrenberger (FDP) "had inserted language into the CDU/CSU-FDP coalition agreement specifically addressing the TFTP negotiations and directing Germany to call upon the E.U. to work towards a high level of data-protection."[25]

With regards to the reluctance from one part of this government, US authorities intensified their pressure with the direct involvement of Timothy Geithner (Treasury secretary), Hillary Clinton (Secretary of State), James L. Jones (National Security Advisor) and Eric Holder (Attorney General).[26] Furthermore, Philip Murphy (US ambassador in Berlin) extensively wrote to German ministers of Interior, of Justice, of Finance, of Foreign Affairs and of Special Affairs (i.e. chancellery) to convince German government not to block EU/US deal. Ultimately, "Ambassador Murphy met with Interior Minister de Maiziere (CDU) on November 27 and urged him to support EU-US negotiations on an interim TFTP agreement, to which de Maiziere indicated that he would abstain from voting on the agenda item at the November 30 COREPER[27] meeting"[28] in Brussels. On the one hand, US authorities welcomed this abstention because it allowed the transatlantic deal to pass at the European Council. On the other hand, Interior Minister's decision launched a harsh internal dispute between the new coalition partners because M. de Maiziere overruled his FDP Justice ministry colleague Leutheusser-Schnarrenberger who "complained that her views were ignored and that the decision 'upset millions of citizens of Europe'."[29]

Even so, European governments (with Austria and Germany abstaining during the Council's vote) finally concluded a new agreement with the American authorities on November 30th, 2009 – that is, just one day before the entry into force of the Lisbon Treaty, which significantly expanded the prerogatives of the European Parliament concerning this type of international agreement.[30] The agreement, however, was strictly provisional, a decision that was officially justified as necessary to prevent any

25. *Wikileaks*, "Coalition tested as US-EU TEFTP/SWIFT agreement passes on German abstention", Cable 09Berlin1528.

26. *Ibid*.

27. The COREPER (or Committee of Permanent Representatives) is responsible for preparing the works of the EU Council. Consisting of Member State ambassadors to the E.U., it is presided over by the Member State that holds the presidency of the Council.

28. *Wikileaks*, "Coalition tested as US-EU TEFTP/SWIFT agreement passes on German abstention", Cable 09Berlin1528.

29. In connection with this governmental clash, the diplomatic cable adds that minister "de Maiziere told the ambassador that he would be expressing some criticisms of the agreement publicly in order to reflect Minister of Interior concerns and to deflect criticism. He was subsequently quoted as saying that "a not completely satisfactory agreement is better that none at all" *(ibid*.).

30. Although Spain presidency of the E.U. officially began one month later, another US diplomatic cable stresses that the Spanish permanent representative to the E.U. "was very concerned that the interim agreement on TFTP was reached on the last possible day before the Lisbon Treaty came into force, which mean that Spain needed to be serious about damage control in the wake of suspicions that the United States and the EU Council colluded to pre-empt Parliamentary action on the agreement". *Wikileaks*, "Ambassador Kennard's meeting with Spanish permanent representative to the E.U.", cable 02Brussels128.

temporary break in the transfer of data to the United States as it was sent to be stored on the new SWIFT server. The Council thus reaffirmed the legality of this interim agreement and the utility of the Terrorist Finance Tracking Program for European security, and all this while announcing that a definitive transatlantic agreement would be negotiated by late 2010 with the participation of the Parliament.

Not everyone was convinced by this mollifying discourse, however. For instance, the European Data Protection Supervisor stated that the terms of the agreement remain very privacy intrusive while he was not convinced by "this necessity and the real added value with respect to more targeted existing instruments" (Hustinx 2010). Furthermore, the timely publication of the 2nd Bruguière report did not win over MEPs while the "eminent European person" insisted on the TFTP as "a highly valuable tool used by intelligence and law enforcement agencies to help map out terrorist networks, to complete missing links in investigations, to confirm the identity of suspects, to locate the physical whereabouts of suspects and to identify new suspects as well as to disrupt attempted terrorist attacks."[31] On February 5th, 2010, the Civil Liberties Parliamentary Commission (LIBE) adopted a text calling for the terms of the transitional agreement to be rejected (European Parliament 2010a). After being debated in plenary session, this position was approved on February 11th by the European Parliament by 378 votes to 196 and 31 abstentions. Officially in force 11 days earlier and now invalidated, the agreement thus fell victim to the first use of the veto that had been attributed to the Parliament by the Lisbon Treaty. The argument put forward by the Commission and Council warning of a "security gap" in the event of rejection (for example, see Council of the European Union 2010a) thus did not suffice, with Parliament's spokesman reiterating concerns about data protection and judicial recourse and expressing regret that the E.U. "continues to externalize its security services to the United States without reciprocity" (European Parliament 2010a). The SWIFT affair thus carried on and was increasingly defined around a European institutional (and intra-national[32]) confrontation to which ever more visible American pressure is added.[33]

Therefore, the so-called "SWIFT affair" continued with European institutional confrontation and US pressure during four months until the signature of another agreement (Council of the European Union 2010b, 2010c). Eventually this new version of the text was adopted by the Parliament on July 2010 as a result of the negotiation of some additional safeguards and commitments (Council of the European Union 2010b; European Parliament 2010b). While there is a slight rewriting of articles regarding judicial redress mechanisms, defense rights and procedural guarantees for European citizens and companies, the significant changes are not there. Two major last minute compromises emerged. The first one entails the appointment of an EU permanent overseer in the U.S. He joins the former team of SWIFT inspectors who have to audit and supervise "in real time and retrospectively" the US searches and uses of SWIFT messages stored in the Treasury black box. Secondly, Europol becomes the official body to control whether SWIFT data transfer requests from the US Treasury meet the terms of the new agreement. Consequently, any transfers of data from European Union to American authorities require Europol staff authorization. Of course, US requests are still broad in scope, not individualized but now officials of the European police office can block such bulk data provision to the US searchable database (black box) if they consider that requests are not sufficiently justified by counter-terrorism needs and/

31. This second report was made available to MEPs on February 1st. The report mentioned that 1550 TFTP-generated reports have been sent to Member-States intelligence services since 2001 and the report enumerated several concrete "TFTP value examples" (Bruguière 2010).

32. Another US diplomatic cable released by Wikileaks, dated February 12th, 2010, underlines Chancellor Angela Merkel's anger with regards to the lack of German MEP support for the agreement. *New York Times*, "Europe Wary of US Bank Monitors", *op. cit*.; "Wikileaks: Merkel furious at MEPs over SWIFT data sharing deal rejection", available at: http://www.finextra.com/news/fullstory.aspx?newsitemid=22073

33. Some Eurodeputies judged the pressure from American authorities on their institution to be very unusual, referring in particular to the telephone call and the letter from American Secretary of State Hilary Clinton to the President of the European Parliament, Jerzy Buzek, prior to the LIBE Commission's vote. See for example the video, *SWIFT Agreement: Issues, Procedure and Reactions* by europarltv. Dated February 5th, 2010, the letter of Hillary Clinton and Timothy Geithner to Jerzy Buzek is available at: http://www.europolitics.info/pdf/gratuit_en/266006-en.pdf

or do not comply with data protection standards. Although Europol's new role is a response to MEPs position for the designation of an EU authority "with the responsibility to receive requests from the United States Treasury Department," it is simultaneously a concession from MEPs because previous Parliament resolutions called for a public "judicial" body, not Europol (European Parliament, Committee on Civil Liberties, Justice and Home Affairs 2010).

Ultimately, in spite of its importance, this five years agreement has not brought the affair to an end yet. Indeed, the agreement has officially planned the next episode, that is, the examination of an EU TFTP that was already glimpsed in the previous deal although not so clearly. The idea of an EU equivalent system to the US program was formally launched by European Parliament resolution of September 17th, 2009 (European Parliament 2009a). Such MEPs' proposal aims at stopping bulk data transfer to the extent that the extraction and analysis of SWIFT data on EU territory would enable to merely deliver data linking to a "specific terrorist track" in connection with US query (European Parliament 2010c). Interestingly, the EU counter-terrorism coordinator quickly took up the possibility of an EU TFTP in the name of the "development of a more equal partnership with the U.S." (Council of the European Union 2009). Thus, this possibility is part of the E.U.-U.S. deal which makes clear that the Commission has to submit a legal and technical proposal one year after the 1st August 2010 entry into force of the agreement.[34]

This key commitment appears highly paradoxical. On the one hand, it is publicly presented as a success of the European Parliament regarding privacy issues (European Parliament 2010c). On the other hand, this so-called success in the name of privacy makes possible what was unthinkable for European security professionals a few years ago, an EU TFTP which would concretely mean Europol's centralized collection and analysis of massive flows of financial messaging data.[35] "I have recently heard that SWIFT decided to change its network architecture. SWIFT decided to create a new operating centre in Switzerland. Their decision would mean that European data would be only stored in Europe. Frankly, that is bad news for European intelligence services because we will never have the political ability to pass a SWIFT mechanism [i.e. TFTP] in Europe" (interview with a European Council Official, November 2007). While the EU TFTP is just a paper project for the moment, the state of play has changed since this interview in 2007 with an unlikely coalition of potentially contradictory interests that tends to support the setting up of an EU equivalent system. Thus, "just do it" would be the next motto within the European Council, the Commission and so the Parliament after the previous "laisser-faire" adopted by some Member States until the media disclosure of the TFTP and the current "faire faire" which consists in outsourcing to the U.S. what the EU security field cannot do (yet).

Conclusion

Counter-terrorism practices highlighted by the "SWIFT case" are based on techniques of tracing flows in order to account for mobility (financial, here). The TFTP aims at locating "suspects" and visualizing their relationships in following money in its context of movement without infringing on the principle of free circulation of capital. Hence, the US TFTP does not corroborate the idea of any mobility/security dilemma whatsoever. Mobility precisely tends to be the crucial element through which practices of control and surveillance can be widely deployed. As a result, intelligence is enabled by technologies extracting information and monitoring "electronic traces" with the stated aim of prevention. The "SWIFT case" shows how intelligence is understood as mass intelligence driven by databases and software related to a massive transfer of data between the global messaging company and the US Treasury "black box." The TFTP system has hence allowed for a focused research by US

34. The EU Commission published a first official document (i.e. the impact assessment) in November 2010. Available at: http://ec.europa.eu/governance/impact/planned_ia/docs/2011_home_003_terrorist_financing_tracking_en.pdf

35. This Europol option is the current proposition of the European Commission (European Commission 2010).

authorities, including on personal data that was neither related to American citizens nor generated on US territory. This case study is illustrative of the current trend in the field of security: security professionals increasingly try to gain access to commercial databases for intelligence purposes.

While this paper already emphasizes the uncertainties and multiple tensions of the SWIFT case's constitutive phases, this conclusion does not intend to sum up them, but seeks to open the debate on one question. Is the critical surveillance issue of the US TFTP where it is supposed to be? Although the privacy issue of secondary use and the related question of power imbalance has already been highlighted and needs further research, there is another underrated topic at stake regarding the TFTP functioning.

Indeed, the main Orwellian fear of European institutions and data protection authorities was the possibility of US generalized surveillance of all SWIFT data and fishing expeditions in the US Treasury Black box. Hence, the five years agreement insisted on the strict limitation of the US program to counter-terrorism purposes (no economic espionage for instance) and the prohibition of data mining or any type of automated profiling on financial transactions records stored in the US searchable database. OFAC queries to Europol (for SWIFT data from the European zone) have to be substantiated and each US counter-terrorist analysts' search in the black box needs to be targeted and justified by a pre-existing "terrorism nexus." Thus, US authorities have accepted to comply with Europol, not to engage in data mining practices and not to extract and process all subset of SWIFT messages transferred to their searchable database. Was it such a difficult decision for them?

First of all, the compliance function of Europol is undeniably the product of last-minute negotiations with regards to the US collection of data. Europol's task formally represents a new step of supervision with a significant move from a private overseer to a public one in order to verify the necessity, the proportionality and so the admissibility of US requests. Indeed, although SWIFT representatives stated that their company already "narrowed the scope of the subpoena to a limited set of data" (European Parliament Hearing 2006), Europol's empowerment has been presented as a stronger guaranty to ensure that US queries are "tailored as narrowly as possible in order to minimize the amount of data requested (Council of the European Union 2010b)." However, the first months of the E.U.-U.S. agreement did not tend to show such a stronger guaranty in practice. In March 2011, Europol Joint Supervisory Body (JSB)[36] published the conclusions of the first review of Europol's implementation of the TFTP agreement. JSB president underlines that "the most finding of the inspection was that the written requests Europol received were not specific enough to allow it to decide whether to approve or deny them. It was found that the US requests were too general and too abstract to allow proper evaluation of the necessity of the requested data transfers. Despite this, Europol approved each request it received" (Joint Supervisory Body 2011a, b). Whereas Europol representatives specify that certain officials have also received extra information from the US Treasury department via oral briefings that influence Europol's positive decisions, information provided orally cannot be checked by the JSB. Hence, the relationships between the security gap and the supervisory gap remain a controversial issue between the various actors engaging in the TFTP agreement.[37]

Secondly, the terms of the E.U.-U.S. accord do not seem to challenge US previous practices at all with reference to information processing. Indeed, there has presumably been no data mining since the creation of the TFTP and no comprehensive extraction as well as no evidence of any use of SWIFT-

36. The main task of this independent body is to ensure that Europol complies with data protection principles. See: http://europoljsb.consilium.europa.eu/about.aspx

37. Civil Liberty Committee MEPs strongly criticized Europol after the release of JSB's report, saying for instance that "entrusting this (compliance) task to Europol is like putting the fox in charge of the chicken coop." Although the Commission released a report which is much more positive regarding the first six months implementation of the TFTP agreement, the Commission review team also supported the JSB's concern. Furthermore, a note from the German delegation (European Council) already expressed concerns on the lack of information from the Commission and Europol regarding the implementation of the TFTP agreement. Finally, Europol published an information note to the European Parliament one month after the JSB's report (European Parliament Press 2011; German delegation 2011; European Commission 2011; Europol 2011).

derived data for other purposes than counter-terrorism. US authorities have always rejected allegations of data mining regarding TFTP as such since the media disclosure. US intense lobbying on a myriad of EU actors did not pressure to include such practices. Moreover, absence of profiling and existence of targeted use of data were even one of the main lines of the US argument to justify that the program respects "individual privacy."[38] According to current public record on the SWIFT affair, one can argue that US officials readily accepted to officially forbid any type of profiling to the extent that this acceptance changed nothing to the core of the TFTP but added a transatlantic legal framework and some legitimacy to this program. Although misunderstandings about TFTP functioning have longly focused harsh critics in terms of Orwellian and/or algorithmic surveillance, the program does not monitor all data and is not a search engine to identify suspicious transactions with the help of profiling software. As promoted by US officials and Jean-Louis Bruguiere's reports, TFTP consists in a device for "mapping out terrorist networks" which is based on pre-existing information (i.e. "terrorism nexus") on one suspect at least in order to visualize his financial connections.[39]

As a result, the surveillance of everyone's transactions is not and has never been on the TFTP agenda. The surveillance of people who already fall into the so-called "terrorism nexus" has. Seen in this light, the critical issue of the TFTP is not about data mining practices and monitoring of all data. The relevant interrogation becomes: "Who falls into the terrorism nexus defined by US agencies?"[40] The issue at stake slightly shifts from algorithmic global surveillance and profiling as pattern recognition to "terrorist lists" and nomination procedures.

Indeed, TFTP analysts search SWIFT messages which include persons or entities that have a "pre-existing nexus to terrorism." Consequently, their targeted search are mainly name based and they can use national and United Nations' official blacklists of suspected terrorists and see if any extracting transactions match with those publicly listed names. Nevertheless, one can assume that this kind of attempts is normally doomed to failure because such blacklisted individuals are deemed to have their bank account frozen and they *a priori* cannot do or receive any financial transfers. Therefore, TFTP analysts can use watch lists maintained by the federal government but which content is kept secret, contrary to the public blacklists. The analysts can resort to the TIDE (Terrorist Identities Datamart Environment) database available to US intelligence community and that supports the federal watch listing system.[41] This so-called "mother of all databases"[42] includes all US information about known or suspected "international terrorists." The TIDE database supplies the US consolidated watch list (i.e. the terrorist screening database), which has aggregated former distinct watch lists since 2004. The FBI manages this consolidated list that daily imports TIDE information. While the terrorist screening database also contains data on known or suspected "purely" domestic "terrorists," the subset of TIDE records represents by far the most part of the consolidated watch list. Various subsets of this list are used by government screeners from airport "no fly list" processes and visa procedures to local law enforcement checks.

As of May 2009, a report from the American Justice Department underlined that the consolidated list reached a total of 400,000 individuals corresponding to more than one million names and aliases in 2008.[43] In other words, the US consolidated watch list almost contained 50 times the number on the 2008

38. The argument is still present (see US Department of Treasury 2010).

39. While we have to be careful in order to distinguish between systems of justification of a classified program and "real" practices regarding such program, various sources (document and interviews) confirm at least this functioning of the TFTP.

40. As already glimpsed by Ben Hayes, see: http://database.statewatch.org/article.asp?aid=29980

41. See for instance: National Counterterrorism Center (2011). Terrorist Identities Datamart Environment – Factsheet. Available at: http://www.nctc.gov/docs/Tide_Fact_Sheet.pdf; See also the website of the US National Counterterrorism Center which manages the TIDE database: http://www.nctc.gov/about_us/about_nctc.html

42. As stated by John Scott Redd, the former director of the National Counterterrorism Center managing the TIDE database (in Kessler, Ronald. "NCTC: Up to 70 Terrorist Plots Each Day", August 15th, 2006. Available at: http://archive.newsmax.com/archives/articles/2006/8/15/92436.shtml).

43. "FBI policy requires that all subjects of international terrorism investigations be nominated to the consolidated terrorist watchlist. It also requires that any known or suspected domestic terrorist who is the subject of a full investigation be nominated

Interpol's list of terrorism suspects which almost contained 20 times the number of official blacklists maintained by the United Nations and the European Union.[44] While there are some differences other than the size of the lists, official blacklists and the US consolidated watch list and so the TIDE database share the same administrative and preventive character which place their designation process beyond judicial review. Hence, the aim is not to list individuals who have been convicted of a crime but the ones who are under suspicion in the name of prevention against harmful acts. Such as the listing/delisting procedures of official blacklists, the US watch list has been seriously criticized in connection with various flaws. Thus, the 2009 Justice Department report highlighted problems, mistakes and notably revealed that 24,000 persons wrongly figured on the FBI terrorist watch list (US Department of Justice 2009). As of March 2011, the TIDE database included 500,000 individuals.

Accordingly, the TFTP promoters refer to what they call targeted search – in other words targeted surveillance. This targeted dimension needs to be put into perspective. Even if TFTP analysts would work from a limited subset of TIDE information and the US consolidated watch list, they would work on thousands and thousands of individuals. Furthermore, the TFTP inevitably broadens suspicion because the purpose of the program is to trace money flows related to suspects in order to map out their relationships, that is, to connect the dots. Such social network analysis *de facto* entails a multiplier effect regarding the number of individuals who can be under suspicion by association. To some extent, the TFTP completes full circle. The program is based on pre-existing watch lists which can be then partly supplied by the program itself. Consequently, the critical analysis of the ongoing TFTP development cannot be limited to speculations on data mining practices and general surveillance in order to properly illustrate the issue at stake.[45] This program of transnational communication of personal data for intelligence purposes also needs to be questioned from the listing practices that determine the so-called TFTP targeted search. The formation of bloated lists of potential suspects represents another major counter-terrorism trend closely related to cross-cutting mechanisms for (financial) surveillance at a distance and mobility controls, in the name of prevention.

to the watchlist. Under certain circumstances, FBI policy also allows for the nomination of known or suspected terrorists for whom the FBI does not have an open terrorism investigation" (US Department of Justice 2009).

44. See: http://www.interpol.int/public/FusionTaskForce/default.asp ; Hayes and Sullivan (2011).

45. To be clear, the very functioning of the TFTP does not presumably refer to data mining process but the constitution of a watch list itself may be linked to such process.

References

Amicelle, Anthony, Gilles Favarel-Garrigues (2009) « La lutte contre l'argent sale au prisme des libertés fondamentales: Quelles mobilisations? », *Cultures & Conflits*, n°76, pp. 39-66.

Amicelle, Anthony (2011) "Towards a 'New' Political Anatomy of Financial Surveillance", *Security Dialogue*, vol. 42, n°2, pp. 161-178.

Amoore, Louise, Marieke de Goede (2005) "Governance, Risk and Dataveillance in the War on Terror", *Crime, Law and Social Change*, vol. 43, n°2, pp. 149-173.

Article 29 Data Protection Working Party (2006) *Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, 22 November. See: http://www.gov.im/lib/docs/odps/swiftopinionofarticle29working.pdf

Article 29 Data Protection Working Party (2007) *Press Release 62nd Session*, 11 October, p. 1.

Banque nationale de Belgique (2005), *Financial Stability Review 2005: Synthèse*, June.

Basel Committee on Banking Supervision (2002) *Sharing of Financial Records between Jurisdictions in Connection with the Fight against Terrorist Financing*. See: www.bis.org/

Biersteker, Thomas, Sue Eckert (2008) "Introduction: the challenge of terrorist financing", in Thomas Biersteker and Sue Eckert, *Countering the Financing of Terrorism*, New York, Routledge, pp. 1-16.

Bigo, Didier, Emmanuel-Pierre Guittet (2004) « Vers une nord-irlandisation du monde », *Cultures & Conflits*, n°56, pp. 171-182.

Bigo, Didier (2006) "Globalized-In-Security: the Field and the Ban-Opticon", in Naoki Sakai and Jon Solomon, *Translation, Biopolitics, Colonial Difference*, Hong Kong, University of Hong Kong Press, pp. 109-156.

Bruguiere, Jean-Louis (2010) *Second Report on the processing of EU-originating personal data by the United States Treasury Department for Counter Terrorism purposes: Terrorist Finance Tracking Programme*, January. Although this report is classified, it is available at: http://www.statewatch.org/news/2010/aug/eu-usa-swift-2nd-bruguiere-report.pdf

Chateauraynaud, Francis, Didier Torny. *Les Sombres précurseurs : une sociologie pragmatique de l'alerte et du risque*, Paris, Editions de l'Ecole des hautes études en sciences sociales, 1999, 476 p.

CNIL (2007) *28th Annual Activity Report,* Paris, La Documentation française, pp. 23-24.

Commission de la protection de la vie privée (Royaume de Belgique) (2006a) *Avis n°37 relatif à la transmission de données à caractère personnel par la SCRL SWIFT suite aux Sommations de l'UST (OFAC)*, September 27th. See: http://www.privacycommission.be/fr/docs/Commission/2006/avis_37_2006.pdf

Commission de la protection de la vie privée (Royaume de Belgique) (2006b) *Avis n°47 relatif à la préparation d'une convention concernant la transmission de données à caractère personnel par SWIFT à l'US Department of the Treasury (UST), December 20th*.

Commission de la protection de la vie privée (Royaume de Belgique) (2007) *Dossier Technique. Affaire SWIFT : la Commission belge de la protection de la vie privée (« CPVP ») demande de la transparence*, June. See: http://www.privacycommission.be/fr/static/pdf/cbpl-documents/note_dossier-technique.pdf

Council of the European Union (2007) *Processing and protection of personal data subpoenaed by the Treasury Department from the US based operation centre of the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*. Luxembourg, 11291/07, June 28th.

Council of the European Union (2009) Note from EU Counter-Terrorism Coordinator to Council/European Council: EU Counter-Terrorism Strategy – discussion paper, November 26th, 15359/1/09.

Council of the European Union (2010a) *EU-US Agreement on the Transfer of Financial Messaging Data for Purposes of the Terrorist Finance Tracking Program,* February 9th.

Council of the European Union (2010b) *Council Decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and the transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program*, Brussels, June 24th.

Council of the European Union (2010c) *Signature of EU-US agreement on financial messaging data for purposes of the US Terrorist Finance Tracking Programme*, June 28th.

DE BLIC, Damien, Cyril Lemieux (2005) "Le scandale comme épreuve: éléments de sociologie pragmatique", *Politix*, vol. 18, n°71, pp. 9-38.

De Goede, Marieke (2008) "Risk, Preemption and Exception in the War on Terrorist Financing", in Louise Amoore & Marieke de Goede (Eds.), *Risk and the War on Terror*, New York, Routledge, pp. 97-111.

Donohue, Laura (1999) "Temporary permanence: The Constitutional Entrenchment of Emergency", *Stanford Journal of Legal Studies*, vol. 1, n°1, pp. 35-71.

Donohue, Laura (2001) *Counter-Terrorist Law and Emergency Powers in the UK, 1922-2000*, Dublin, Irish Academic Press, 422 p.

Edelman, Murray (1988) *Constructing the Political Spectacle*, Chicago, University of Chicago Press, 137 p.

European Commission (2010) Impact assessment: Roadmap – European Terrorist Financing Tracking Programme (European TFTP), November.

European Commission (2011) *Commission report on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of financial messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program*, Brussels, March 16th.

European Data Protection Supervisor (2007) *EDPS opinion on the role of the European Central Bank in the SWIFT case*, February. See: http://www.europarl.europa.eu/hearings/20070326/libe/edps_opinion_swift_en.pdf

European Parliament (2006) *Resolution of the European Parliament concerning the Interception of Bank Transfer Data in the SWIFT System by American Secret Services*, Strasburg, July 6t. See: http://www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=B6-2006-0391&language=BG

European Parliament (Hearing) (2006) "SWIFT Statement: Francis Vanbever, Chief Financial Officer, Member of the Executive Committee, SWIFT", October 4th.

European Parliament (2007a) Public Seminar "PNR/SWIFT/Safe Harbour: Are Transatlantic Data Protected?", Brussels, March 26th.

European Parliament (2007b) *Resolution of the European Parliament concerning SWIFT, the PNR Agreement and Transatlantic Dialogue on These Questions*, February 14th, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2007-0039+0+DOC+XML+V0//EN

European Parliament (2009a) *Résolution du Parlement européen sur l'accord international envisagé pour mettre à la disposition du département du Trésor des Etats-Unis des données de messagerie financière afin de prévenir et de combattre le terrorisme et le financement du terrorisme*, September 17th.

European Parliament (2009b) *Joint Meeting of LIBE and ECON Committees on EU-US Interim Agreement Following the Entry Into Force of the New SWIFT Architecture: Peter Hustinx, European Data Protection Supervisor, speaking points*, September 3rd.

European Parliament (Press Service) (2010a) "SWIFT, Will Europeans' Bank Data Cross the Atlantic?, February 5th.

European Parliament (Press Service) (2010b), "Parliament examines SWIFT II agreement", 2 July.

European Parliament (Press Release) (2010c) "SWIFT II: Civil liberties Committee approves draft agreement", July 5th.

European Parliament (Press release) (2011) "SWIFT implementation report: MEPs raise serious data protection concerns", March 16th.

European Parliament Committee on Civil Liberties, Justice and Home Affairs (2010). *Draft Recommendation on the draft Council decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program*, Brussels, June 29th.

Europa Press release (2009) EU Review of the United States' "Terrorist Finance Tracking Programme" confirms privacy safeguards, 17 February 17th.

Europol (2011) *Europol Activities in Relation to the TFTP Agreement Information Note to the European Parliament 1 August 2010 – 1 April 2011*, The Hague, April 8th.

Favarel-Garrigues, Gilles, Thierry Godefroy, Pierre Lascoumes (2009) *Les Sentinelles de l'argent sale : les banques aux prises avec l'antiblanchiment*, Paris, La Découverte, 312 p.

General Secretariat of the Council of the EU (2009) *Information Note: EU-US agreement on the processing and transfer of financial messaging data for purposes of the US Terrorist Finance Tracking Programme (TFTP)*, November. http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/111559.pdf

German Delegation (2011) *Europol's role in the framework of the EU-US TFTP Agreement and state of play of operational and strategic agreements of Europol (specific focus: the agreement on exchange of personal data and related information that Europol has with the US) – EU information policy on the TFTP Agreement*, Brussels, February 8th.

Gonzalez Fuster, Gloria, Paul de Hert, Serge Gutwirt (2008) "SWIFT and the vulnerability of transatlantic data transfers", *International Review of Law Computers & Technology*, vol. 22, n°1-2, pp. 191-202.

Hayes, Ben, Gavin Sullivan (2011) *Blacklisted: Targeted sanctions, preemptive security and fundamental rights*. European Center for Constitutional and Human Rights (ECCHR). http://www.ecchr.de/index.php/home_en.html

Hildebrandt, Mireille (2008) "Defining Profiling: A New Type of Knowledge?", in Mireille Hildebrandt, *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Brussels, Springer Science, pp. 17-45.

Hustinx, Peter (EDPS) (2010) "Comments of the EDPS on different agreements, notably the EU-US and EU-AUS PNR agreements, the EU-US TFTP agreement, and the need of a comprehensive approach to international data exchange agreements", Brussels, January 25th.

Joint Supervisory Body (2011a) *Report of the inspection of Europol's implementation of the TFTP agreement, conducted in November 2010 by the Europol Joint Supervisory Body*, Brussels, March 1st.

Joint Supervisory Body (2011b) *Terrorist Finance Tracking Program (TFTP) Agreement: Europol Joint Supervisory Body inspection raises serious concerns about compliance with data protection principles*, Brussels, March 2nd.

Köppel, Johannes (2009) *The Swift Affair: Swiss Banking Secrecy and the Fight against Terrorist Financing*, Geneva, Graduate Institute of International and Development Studies, unpublished paper.

Lemieux, Cyril (2007) "L'accusation tolérante : remarques sur les rapports entre commérage, scandale et affaire" in Luc Boltanski, Elisabeth Claverie, Nicolas Offenstadt and Stéphane van Damme, *Affaires, scandales et grandes causes. De Socrate à Pinochet*, Paris, Stock, pp. 367-369.

Levi, Michael, David Wall (2004) "Technologies, Security, and Privacy in the Post-9/11 European Information Society"*, Journal of Law and Society*, vol. 31, n°2, pp. 194-220.

Levi, Michael (2010) "Combating the Financing of Terrorism: A History and Assessment of the Control of 'Threat Finance'", *British Journal of Criminology*, vol. 50, n°4, pp. 650-669.

Lyon, David (2007) *Surveillance Studies: An Overview*, Cambridge, Polity Press, 243 p.

Malkin, Lawrence, Yuval Elizur (2002) "Terrorism's Money Trail", *World Policy Journal*, vol. 19, n°1, pp. 60-70.

McCulloch, Jude, Sharon Pickering (2009) "Pre-Crime and Counter-Terrorism: Imagining Future Crime in the 'War on Terror'", *British Journal of Criminology*, vol. 49, n°5, pp. 628-645.

Mitsilegas, Valsamis (2008) "Coopération antiterroriste Etats-Unis/Union européenne : l'entente cordiale" in Didier Bigo, Laurent Bonelli and Thomas Deltombe, *Au nom du 11 septembre… Les démocraties à l'épreuve de l'antiterrorisme*, Paris, La Découverte, pp. 118-130.

Official Journal of the European Union (2007) *Terrorist Finance Tracking Program – Representations of the United States Department of the Treasury*, July 20th. http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/c_166/c_16620070720en00180025.pdf

Privacy Protection Commission (Kingdom of Belgium) (2008), *Supervision and Recommendation Procedure Initiated with Regards to the SWIFT srcl Company*, decision of December 9th.

Salter, Mark B. (ed.) (2008) *Politics at the Airport*, Minnesota, University of Minnesota Press, 183 p.

Secretariat General du Conseil de L'UE (2009) *Note d'information : Accord entre l'Union européenne et les Etats-Unis sur le traitement et le transfert de données de messagerie financière aux fins du programme de surveillance du financement du terrorisme (TFTP)*, Novembre.

Solove, Daniel (2006) "A Taxonomy of Privacy", *University of Pennsylvania Law Review*, vol. 154, n° 3, pp. 477-560.

Solove, Daniel (2007) "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy", *San Diego Law Review*, vol. 44, n° 745, pp. 745-772.

Solove, Daniel (2008) "Data Mining and the Security-Liberty Debate", *University of Chicago Law Review*, vol. 74, pp. 343-361.

The United States Senate Judiciary Committee, Subcommittee on Terrorism, Technology and Homeland Security (2004) "Tools to Fight Terrorism: Subpoena Authority and Pretrial Detention of Terrorists" Testimony of Rachel Brand, Principal Deputy Assistant Attorney General, Office of Legal Policy, U.S. Department of Justice, June 22nd.

UN General Assembly (2006) *Report of the Special Rapporteur [Martin Scheinin] on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, New York, A/61/267, August 16th.

US Department of Justice, Office of the Inspector General Audit Division (2009) *The Federal Bureau of Investigation's Terrorist Watchlist Nomination Process*, May.

US Department of the Treasury (2006a) *Statement of Under Secretary Stuart Levey on the Terrorist Finance Tracking Program*, June 23rd.

US Department of the Treasury (2006b) *Terrorist Finance Tracking Program - Fact Sheet*, June 23rd.

US Department of the Treasury (2010) *Terrorist Finance Tracking Program – Factsheet*, August 2nd.

US Treasury Department Office of Public Affairs (2006) Testimony of Stuart Levey, Under Secretary, Terrorism and Financial Intelligence, U.S. Department of the Treasury, Before the House Financial Services Subcommittee on Oversight and Investigations, July 11th. http://www.treas.gov/press/releases/hp05.htm

SWIFT press release, "SWIFT (2007) Le Conseil d'administration de SWIFT approuve la nouvelle architecture de messagerie", Brussels, October 4th.

Newspapers

The Guardian, "Bush under fire over tracking of money transfers", 23 June 2006.

Le Monde, "La CIA a espionné les flux bancaires internationaux", 25 June 2006.

Le Soir, “Les intrusions de la CIA dans les données confidentielles”, 26 June 2006.

European Voice, “Pressure Grows on Opponents of Bank Transfer Data Deal”, 26 November 2009.

The New York Times, “Bank Data Sifted in Secret by U.S. to Block Terror”, 23 June 2006(a).

The New York Times, “Secrecy, Security, the President and the Press”, 2 July 2006(b).

The New York Times, “Banking Data: A Mea Culpa”, 22 October 2006(c).

The New York Times, “U.S. Cites ‘Secrets’ Privilege as It Tries to Stop Suit on Banking Records”, 31 August 2007.

The New York Times, “Europe Wary of US Bank Monitors”, 5 December 2010.

The Los Angeles Times, “Secret U.S. Program Tracks Global Bank Transfers”, 23 June 2006.

The Washington Post, “Bank Records Secretly Tapped: Administration Began Using Global Database Shortly after 2001 Attacks”, 23 June 2006(a).

The Washington Post, “Lawmaker Wants Times Prosecuted”, 26 June 2006(b).

The Wall Street Journal, “U.S. Treasury Tracks Financial Data in Secret Program”, 23 June 2006.