CEPS Paper in
LIBERTY and SECURITY in Europe

The EU's Paradoxical Efforts at Tracking the Financing of Terrorism:

From criticism to imitation of dataveillance

Anthony Amicelle

No. 56 / August 2013

Abstract

In July 2011, the European Commission published a Communication aimed at setting out different options for establishing a European terrorist finance tracking system (TFTS). The Communication followed the adoption of the EU-US agreement on the US Terrorist Finance Tracking Program (TFTP) in 2010. The agreement concluded various series of national, European and transatlantic negotiations after the disclosure through public media of the US TFTP in 2006. This paper takes stock of the wide range of controversies surrounding this security-focused programme with dataveillance capabilities. After stressing the impact of the US TFTP on international relations, the paper argues that the EU-US agreement primarily has the effect of shifting information-sharing practices from the justice/judicial/penal/criminal investigation framework into the security/intelligence/administrative/prevention context as the main rationale. The paper then questions the TFTP-related conception of mass intelligence through large-scale databases and transnational communication of bulk data in the name of targeted surveillance. Following an examination of the project creating an EU system equivalent to the TFTP, the paper emphasises the fundamental paradox of transatlantic security matters, in which European criticisms of American programmes tend to be ultimately translated into EU imitation of US dataveillance practices.

ISBN 978-94-6138-345-7
Available for free downloading from the CEPS website (http://www.ceps.eu)

Contents

The EU's Paradoxical Efforts at Tracking the Financing of Terrorism:

From criticism to imitation of dataveillance

Anthony Amicelle*

CEPS Paper in Liberty and Security in Europe No. 56 / August 2013

Introduction

The term *dataveillance* refers to "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons".[1] "[A] variation of 'surveillance', [the term] emphasises the importance of databases, rather than visual or auditory means of watching over people, in the practices of states and companies" to influence, manage, protect or control individuals, social groups or populations.[2] Practices of tracking, monitoring and keeping data files on populations for governmental purposes did not begin with the rise of computer databases. The filing of personal records has been widespread in different political contexts (democratic and authoritarian) since the 18th century in Europe, for instance.[3] While the illusion of novelty must be carefully avoided, technology leapfrogging deserves critical attention with regards to data storage and data processing capacity. Thus, the term *dataveillance* has been coined "to describe the surveillance practices that the massive collection and storage of vast quantities of personal data have facilitated".[4]

---

* Anthony Amicelle is Assistant Professor, School of Criminology, University of Montreal and the International Centre for Comparative Criminology (ICCC). He would like to thank Elspeth Guild and Sergio Carrera for their useful comments on an earlier version of this paper. He is also grateful to the members of the security research group at the Peace Research Institute Oslo (PRIO) for fruitful discussions related to the content of the paper..

[1] R. Clarke, (1988), "Information Technology and Dataveillance", *Communications of the ACM*, Vol. 31, No. 5, pp. 498-512.

[2] D. Murakami Wood, K. Ball, D. Lyon, C. Norris and C. Raab (2006), *A Report on the Surveillance Society*, London: Report for the Information Commissioner by the Surveillance Studies Network, p. 20. See also L. Amoore and M. De Goede (2005), "Governance, risk and dataveillance in the war on terror", *Crime, Law & Social Change*. Vol. 43, pp. 149-173; L. Amoore and M. De Goede (2012), "Introduction. Data and the war by other means", *Journal of Cultural Economy*, Vol. 5, No. 1, pp. 3-8; M. Levi and D. Wall (2004), "Technologies, Security and Privacy in the Post-9/11 European Information Society", *Journal of Law and Society,* Vol. 31, No. 2, 2004, pp. 194-220; S. Leman-Langlois (ed.) (2012), *Technocrime: Policing and Surveillance*, New York : Routledge.

[3] I. About, "Les fondations d'un système national d'identification policière en France (1893-1914). Anthropométrie, signalements et fichiers", *Genèses*, No. 54, 2004, pp. 28-52; C. Dandeker, *Surveillance, Power and Modernity*, Cambridge: Polity Press, 1990; V. Denis, *Une histoire de l'identité. France, 1715-1815*, Seyssel: Champ Vallon, 2008; M. Dennis and P. Brown, *Stasi: Myth and Reality*, Harlow: Pearson Education Longman; J. Dunnage, "Social control in Fascist Italy: the Role of the Police", in C. Emsley, E. Johnson and P. Spierenburg (eds), *Social Control in Europe. 1800-2000. Vol.2*, Columbus, OH: Ohio State University Press, 2004, pp. 261-280; J. Dunnage, "Policing Right-Wing Dictatorships: Some preliminary comparisons of Fascist Italy, Nazi Germany and Franco's Spain", *Crime, History & Societies*, Vol. 10, No. 1, 2006, pp. 2-28; J. Dunnage, "Surveillance and Denunciation in Fascist Siena, 1927-1943", *European History Quarterly*, No. 38, 2008, pp. 244-265; C. Fonio, "Surveillance under Mussolini's regime", *Surveillance & Society*, Vol. 9, No. 1/2, 2011, pp. 80-92; K. Haggerty and M. Samatas (eds), *Surveillance and Democracy*, New York: Routledge, 2010; T. Lindenberger, "Secret et public: société et polices dans l'historiographie de la RDA", *Genèses*, Vol. 3, No. 52, 2003, pp. 33-57; D. Murakami Wood, "Editorial. People Watching People", *Surveillance & Society*, Vol. 2, No. 4, 2005, pp. 474-478; D. Murakami Wood, "The 'Surveillance Society': Questions of History, Place and Culture", *European Journal of Criminology*, Vol. 6, No. 2, 2009, pp. 179-194; U. Poppe, "Que lisons-nous lorsque nous lisons un dossier personnel de la Stasi", *Genèses*, Vol. 3, No. 52, 2003, pp. 119-132; J. Schmeidel, *Stasi*, London: Routledge, 2008.

[4] C.J. Bennet, "The Public Surveillance of Personal Data: A Cross-National Analysis", in D. Lyon and E. Zureik (eds), *Computers, Surveillance and Privacy*, Minneapolis, MN: University of Minnesota Press, 1996, pp. 237-259.

Financial dataveillance is the method of investigation or monitoring through the collection of financial data. The systematic use of financial data systems for law enforcement purposes is increasingly associated with specific claims of prevention. Financial dataveillance is not only used to produce inculpating evidence in order to prosecute and convict offenders, it is also used to collect confidential information and perform social network analysis in order to incapacitate suspects before they act. This proactive, intelligence-led approach of financial policing is illustrated by the transatlantic agreement in relation to the Terrorist Financing Tracking Program (TFTP) that has attracted an "unusually high level of public sensitivity", according to Europol officials.[5]

In a letter to the Joint Supervisory Body (JSB), Europol's independent data protection supervisor, Europol Director Rob Wainwright wrote: *"*Given the sensitivity of the TFTP Agreement and its importance to Europol, I attach a very high priority to ensuring Europol reaches a common understanding with the JSB on the issues raised in the Final Inspection Report. As you know some of these issues have received adverse public attention recently in a way that has undermined the reputation of Europol. On an urgent basis I wish to repair this damage and take steps to ensure that it is not repeated.*"*[6]

This paper focuses on the main controversies that have emerged since the disclosure of the US TFTP in 2006: secondary use of commercial databases for law enforcement purposes, power imbalances between sovereign entities, massive information-sharing without judicial assessment in the name of prevention, bulk personal data transfers to a third-country and the European project of a large-scale database to monitor international financial transactions.

These controversies remain highly topical from at least two perspectives. On the one hand, the implementation of the EU-US TFTP agreement is still drawing criticism while the project of a European terrorist finance tracking system is pending. On the other hand, several of the issues are echoed in the recent disclosure of American dataveillance programmes such as PRISM, which is based on the collection of personal data from users of Facebook, Google, Microsoft, Apple, Yahoo, Youtube, Paltalk, AOL and Skype in the name of the fight against terrorism.[7]

According to Tonio Borg, the Commissioner for Health and Consumer Policy, on behalf of the European Commission, "programmes such as the so-called PRISM and the laws on the basis of which such programmes are authorised potentially endanger the fundamental right to privacy and to data protection of EU citizens […] The European Commission is concerned about recent media reports that United States authorities are accessing and processing, on a large scale, the data of European Union citizens using major US online service providers".[8] Members of the European Parliament also criticised the US programme as "a major breach of trust, non-compliant with EU data protection legislation" and as a problem that is "not only about data protection, this is about democracy and the rule of law, which cannot be in line with mass surveillance of citizens around the world".[9]

Similar concerns also greeted the public disclosure in Europe of the US TFTP in 2006. However, an EU system equivalent to the TFTP was officially proposed by the European Commission a few years later, in 2011. From criticism to imitation – is this the fundamental paradox of the European Union in the field of security and surveillance?

This paper starts by summarising the basic facts of the *SWIFT affair* and the US TFTP, which is based on the secondary use of European commercial company databases. Section 2 underlines how the TFTP challenges

---

[5]Europol, "Europol activities in relation to the TFTP agreement information note to the European Parliament 1 August 2010 – 1 April 2011", The Hague, 8 April 2011, p. 11.

[6]Wainwright, R. Europol Director, "Letter to the JSB: Implementation of JSB Recommendations", The Hague, 15 March 2011.

[7]D. Bigo, et al., "Open Season for Data Fishing on the Web. The Challenges of the US PRISM Programme for the EU", CEPS Policy Brie*f*, No. 293, 2013 (www.ceps.be/book/open-season-data-fishing-web-challenges-us-prism-programme-eu).

[8]"Commission statement on 'US internet surveillance of EU citizens'", European Parliament Plenary, Strasbourg, June 2013.

[9]European Parliament, "Prism: MEPs hit out at US surveillance of people's personal data", Brussels, 11 June 2013.

the international principle of equality between sovereign entities. Section 3 argues that the main result of the TFTP agreement is less the transatlantic transfer of personal data than the removal of information-sharing practices from the judicial framework in the questionable name of a particular form of prevention. Section 4 analyses European intra-governmental and inter-institutional tensions in relation to the negotiation of the TFTP agreement. It also questions Europol's vetting role regarding US requests of SWIFT financial messages. Section 5 describes how the TFTP reflects a specific conception of *mass* intelligence that is based on the access to bulk data for targeted search purposes. Finally, Section 6 examines controversies over the current project of an EU terrorist finance tracking system (TFTS).

1. The SWIFT Affair and the Repurposing Process of Personal Data

On 23 June 2006, *New York Times* journalists disclosed the existence of the Terrorist Finance Tracking Program that was implemented by the US government in September 2001. This counter-terrorism programme is based on the access to financial data managed by the Society for Worldwide Interbank Financial Telecommunication (SWIFT).

SWIFT is "a member-owned cooperative through which the financial world conducts its business operations with speed, certainty and confidence".[10] The company provides worldwide messaging services dedicated to the facilitation of international financial transactions. According to official assessments, the SWIFT network channels about 80% of the electronic value transfers around the world.[11] In other words, SWIFT is the postal service for international finance in that the company delivers international mail (i.e. financial messages) between financial institutions. Banking actors are the main users of SWIFT services to make international electronic payments and wire transfers for their customers, such as you and me. Central bank representatives emphasise the systemic significance of SWIFT as a key infrastructure of the international financial and payment system.[12] In 2012, SWIFT processed four and half billion messages and a daily average of 20,083,128 financial messages in May 2013.[13] For each payment by a banking customer, the SWIFT message contains the amount of the transaction, the currency, the date, the name of the originator's bank and the recipient client. The message provides information about the beneficiary and the ordering customer such as complete names, account numbers, addresses, national identification numbers and other personal data.[14]

The US TFTP is based on the secondary use of SWIFT messages. Since 2001, SWIFT representatives have received US requests to provide copies of financial messages to the Treasury's Office of Foreign Assets Control (OFAC) in the name of the 'War on Terror'.[15] OFAC officials have collected, stored and analysed copies of SWIFT messages to detect and monitor terrorist-related transactions. The vast majority of collected messages have related to transactions concerning countries other than the US as well as to entities and individuals other than US organisations and US citizens. This massive access to worldwide financial

[10]See the SWIFT website (www.swift.com).

[11]Council of the European Union, "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, 28 June 2007.

[12]National Bank of Belgium, "Financial Stability Review 2005. Synthesis", June 2005, p. 14.

[13]For further information about SWIFT, see: www.swift.com/about_swift/company_information/swift_in_figures

[14]For further information, see G. Gonzalez Fuster, P. De Hert and S. Gutwirth (2008), "SWIFT and the vulnerability of transatlantic data transfers", *International Review of Law Computers & Technology*, Vol. 22, No. 1-2, pp. 191-202; A. Amicelle, "The Great Data(Bank) Robbery", *Research Questions*, No. 36, 2011; M. Wesseling, M. De Goede and L. Amoore, "Data wars beyond surveillance: Opening the black box of SWIFT", *Journal of Cultural Economy*, Vol. 5, No. 1, 2012, pp. 49-66.

[15]"The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States. OFAC acts under Presidential national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze assets under US jurisdiction". For further information, see http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx

messages was technically possible due to the fact that SWIFT ran two operating centres to deliver messaging services, one located in the Netherlands and the other located in the US. SWIFT stored all financial messages on both servers for 124 days to prevent any problem in case of disputes between financial institutions or data loss.[16] Each server held "an exact copy of the data held by the other" server to provide a backup should one of the servers crash.[17]

OFAC officials issued administrative production orders (i.e. administrative subpoenas) to the US SWIFT operating centre to collect and process data that was originally registered for commercial purposes for a short period of time. The TFTP is a clear-cut example of *secondary use* that "involves data collected for one purpose being used for an unrelated purpose without people's consent".[18] This repurposing of personal data poses questions over three interrelated relationships: the relationship between state security agencies and commercial companies that are not providers of security services; the relationship between businesses and customers; and the relationship between state representatives and populations. Finally, the repurposing poses questions over how security programmes with dataveillance capabilities affect societal structure by altering these three interrelated relationships.[19]

"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 we are watching sends receives money from another person, we know that there is 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 sympathisers 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 TFTP was just such an invisible tool".[20]

Although US Treasury representatives promoted the added value of the TFTP, the secondary use of SWIFT messages was seriously criticised, especially in the European Union. The SWIFT headquarters are located in Belgium and the company is covered by European legislation on privacy and data protection. Members of the European Parliament (MEPs) and representatives of European data protection authorities were concerned about the massive exchange of personal data (including European citizens and residents' data) between a European commercial company and a third country without any European safeguards.

2. International Relations and the Principle of Equality between Sovereign Entities

SWIFT messaging services are critical for daily European banking practices. The US interception of SWIFT messages meant that OFAC officials collected financial personal data of millions of European citizens and residents from 2001 to 2006 (the time of the *New York Times'* disclosure) without any transatlantic

[16]Article 29 Data Protection Working Party, "Opinion 10/2006 on the processing of personal data by the society for Worldwide Interbank Financial Telecommunication (SWIFT)", Brussels, 22 November 2006.

[17]European Parliament, "Public seminar 'PNR/SWIFT/Safe Harbour: Are Transatlantic Data Protected?'", Brussels, 16 March 2007.

[18]D. Solove, "I've got nothing to hide and other misunderstandings of privacy", *San Diego Law Review*, Vol. 44, No. 475, 2008, p. 770.

[19]A. Amicelle and G. Favarel-Garrigues, "Financial Surveillance: Who Cares?", *Journal of Cultural Economy*, Vol. 5, No. 1, 2012, pp. 105-124; PACT Consortium, "Discussion paper about the theoretical foundations of PACT", *The Privacy & Security Research Series*, No. 2, 2012.

[20]US Treasury Department Office of Public Affairs, "Testimony of Stuart Levey, Under Secretary, Terrorism and Financial Intelligence, US Department of the Treasury, before the House Financial Services Subcommittee on Oversight and Investigation", 7 November 2006, p. 2.

negotiation or European agreement regarding safeguards of fundamental rights.[21] Moreover, the US counter-terrorism programme challenged EU economic sovereignty. Members of the European Parliament and data protection authorities initially flagged the potential for economic and industrial espionage;[22] they were concerned that US Treasury officials could have access to strategic transactions and commercial information about European companies.

Furthermore, the TFTP challenged the principle of equality between sovereign entities, in this case between the European Union and the United States. The United States' unilateral access to international SWIFT messages illustrates current tensions in international relations regarding forms of asymmetry and domination that are related to the *information question*, i.e. "power asymmetries as a consequence of differential dissemination of information or, at least, access inequalities to information producing devices".[23]

The implementation of security programmes with global dataveillance capabilities, such as the TFTP, contributes to destabilising the principle of equality between sovereign entities. This formal equality represents a key principle of the Westphalian system as the archetype of international order. According to the classic conceptualisation of the Westphalian system, international order is based on principles of sovereignty, non-intervention, territoriality and formal equality between sovereign actors.[24] While the issue of sovereignty has been explicitly tackled in relation to the possibility of economic espionage, the TFTP also touches on other Westphalian principles, such as formal equality. The massive collection of personal data affects power relationships between sovereign entities regarding rules of information collection and information exchange about citizens.

OFAC officials collected financial messages that circulated all over the world. As a result, US officials accessed third-country citizens' personal data without the approval of these third countries' bureaucracies. Of course, Westphalian equality has always been understood as a formal principle. The process of bypassing other national bureaucracies to collect foreign individuals' information for security purposes is a traditional practice of intelligence. However, the scope of the TFTP represented a step beyond surveillance projects such as ECHELON, as it has amplified contemporaneous forms of informational domination.[25] With their exclusive access to SWIFT messages, US authorities have shaped an asymmetric relationship between the United States and other sovereign entities in relation to the growing area of financial intelligence.

This issue of equality between sovereign entities was one of the key elements of the transatlantic negotiations to reach a TFTP agreement after the media disclosure in June 2006. Although the transatlantic agreement in relation to the TFTP was signed in 2010, a so-called 'exit from the crisis' had already been found as early as the end of 2007.[26] SWIFT representatives were under pressure from the European Union

---

[21]Nevertheless, for further information about EU actors' ambiguity, see A. Amicelle and G. Favarel-Garrigues, "La lutte contre l'argent sale au prisme des libertés fondamentales : Quelles mobilisations?", *Cultures & Conflits*, No. 76, 2009, pp. 39-66.

[22]European Parliament, "European Parliament resolution on the interception of bank transfer data from the SWIFT system by the US secret services", 6 July 2006; European Parliament, "European Parliament resolution on SWIFT, the PNR agreement and the transatlantic dialogue on these issues", 14 February 2007; Commission de protection de la vie privée (Royaume de Belgique), "Avis n°37 relatif à la transmission de données à caractère personnel par la SCRL SWIFT suite aux sommations de l'UST (OFAC)", 27 Septembre 2006; Article 29 Data Protection Working Party, "Opinion 10/2006 on the processing of personal data by the society for Worldwide Interbank Financial Telecommunication (SWIFT)", 22 November 2006; European Data Protection Supervisor, "EDPS opinion on the role of the European Central Bank in the SWIFT case", Brussels, 1 February 2007.

[23]D. Linhardt, "La 'question informationnelle'. Eléments pour une sociologie politique des fichiers de police et de population en Allemagne et en France", *Déviance et Société*, Vol. 29, 2005, pp. 259.

[24]T. Lapointe, "Système de Westphalie", in A. Macleod et al. (eds), *Relations internationales: Théories et concepts*, Montréal: Athéna Editions, 2008, pp. 495-498.

[25]For further information about ECHELON, see D. Campbell, *Surveillance électronique planétaire*, Paris: Editions Allia, 2006.

[26]Article 29 Data Protection Working Party, "Press release 62nd session", Brussels, 11 October 2007, p. 1; CNIL (2007), *28e rapport d'activité*, Paris: La Documentation française, pp. 23-24; Commission de protection de la vie privée (Royaume de Belgique), "Contrôle et procédure de recommandation à l'égard de la société SWIFT scrl", Bruxelles, 9 décembre 2008.

over the communication of European bulk data to the US Treasury. As a result, they decided to modify the technical architecture of their messaging services that was based on mirror servers in the Netherlands and the United States. This modification consisted of creating a new operating centre in Switzerland to keep European financial messages within the continent. In other words, SWIFT representatives wanted to store European SWIFT messages in mirror servers in both the Netherlands and Switzerland, and no longer in the US operating centre.

To do so, they approved the division of their international messaging platform into two distinct zones. "Distributed architecture will partition messaging into two zones, the European messaging zone and the Trans-Atlantic messaging zone, with pairs of Operating Centres that store the traffic for each zone. The implementation of the messaging zones will take place by the end of 2009."[27] The European messaging zone covers the European Economic Area (EU-27, Norway, Iceland and Liechtenstein), Switzerland and other territories and dependencies of the European Union or associated with European member states. The Trans-Atlantic zone relates to the United States and its territories, and the other 180 or so SWIFT countries have been assigned to the Trans-Atlantic zone by default, though their representatives can request to be reassigned to the European zone. This element reminds us that the impact of the TFTP is not only an EU-US issue, as "more than 10,000 financial institutions and corporations in *212 countries* trust [SWIFT] every day to exchange millions of standardised financial messages".[28]

The implementation of this new distributed architecture meant that financial messages in the European zone would only be registered in the SWIFT operating centres in the Netherlands and Switzerland. Electronic traces in relation to financial transactions of the European messaging zone would remain in Europe. Consequently, OFAC officials could no longer request access to interbank messages that circulate in Europe; the US TFTP could only be based on SWIFT messages that are related to the Trans-Atlantic zone. Nevertheless, a reconfiguration of SWIFT was anticipated by US authorities to allow access to European financial transactions that are channelled through SWIFT messaging services. Transatlantic informal negotiations resumed in 2009 to allow US TFTP analysts to consult SWIFT messages unrelated to the US territory and the Trans-Atlantic zone. In July 2009, the European Commission and the Swedish presidency of the European Union were mandated to strike a new deal with the United States. The US presidential change from the Bush administration to the Obama administration has not altered its position on the TFTP.

3. Prevention as a Legitimation Narrative: Information-Sharing Practices outside the Judicial Framework

MEPs, representatives of data protection authorities and some member states' delegations (primarily Germany and Austria) criticised the idea of a transatlantic agreement that mainly aimed at ensuring the status quo regarding the TFTP.[29] The European Data Protection Supervisor (EDPS), Peter Hustinx, considered that "not enough evidence has been provided so far to justify the necessity and the proportionality of such a privacy-intrusive agreement, which in many ways overlaps with pre-existing EU and international instruments in this area".[30] Regarding pre-existing instruments, Mr. Hustinx primarily referred to the 2003

[27]SWIFT, "Distributed Architecture: Allocation of Countries to the Two Messaging Zones", 6 June 2008.

[28]See the SWIFT website at www.swift.com.

[29]*European Voice*, "Commission to seek new deal with the US on data transfers", 16 July 2009; *Le Temps*, "Les Etats-Unis obtiendraient l'accès aux données de SWIFT via la Suisse", 22 July 2009; *EU Observer*, "EU bank data move ignored legal advice", 29 July 2009; European Parliament, "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", Brussels, 3 September 2009; *European Voice*, "Pressure Grows on Opponents of Bank Transfer Data Deal", 26 November 2009.

[30]European Data Protection Supervisor, "Comments of the EDPS on different international 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, 25 January 2010.

agreement on mutual legal assistance between the European Union and the United States.[31]

However, a major difference exists between the logic of this agreement of mutual legal assistance and the logic of the envisaged TFTP agreement. The 2003 agreement fits perfectly within the legal framework of criminal justice. In other words, information exchange was mainly possible to prosecute crimes after they occur. In contrast, the TFTP is associated with a particular logic of prevention that exceeds traditional practices of criminal investigation in that it does not just aim at finding and prosecuting criminals before they reoffend. Moreover, the main aim of the TFTP promoters has been precisely to remove counter-terrorism practices from the legal framework of criminal justice in which a judicial/court order is required to access information.

The use of administrative subpoenas and programmes such as the TFTP reflects the promotion of a specific form of prevention: "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".[32] This promotion of administrative productive orders (i.e. *administrative* subpoenas without prior *judicial* oversight) for counter-terrorism purposes illustrates the legitimation narrative of the TFTP and other US security programmes with dataveillance capabilities, such as PRISM.

While prevention is clearly presented as the ultimate goal of counter-terrorism, this stance refers to a specific form of prevention that overlaps with the ambivalent appropriation of military pre-emption in the context of intelligence-led policing.[33] Here, prevention does not fit within the classic understanding of addressing the root causes of criminal or political violence. Neither is this notion of prevention associated with another traditional form of prevention, i.e. 'deterrence', as it is optimistic to expect any deterrent effect from a programme that has been conceived as an invisible and secret tool. The TFTP highlights the significance of a third, proactive meaning of prevention to 'act before the other' in order to prevent potential harmful events from happening.[34] Official justifications for accessing detailed personal data are less focused on finding evidence to prosecute and punish criminals than on amassing intelligence to pre-emptively disrupt and incapacitate suspects.[35]

---

[31]Agreement on mutual legal assistance between the European Union and the United States of America, OJ 2003, L 181/34.

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

[33]D. Grondin, "Guerre préemptive/guerre préventive", in A. Macleod et al. (eds), *Relations internationales: Théories et concepts*, Montréal: Athéna Editions, 2008, pp. 206-210; M. De Goede, "The Politics of Preemption and the War on Terror in Europe", *European Journal of International Relations*, No. 14, 2008, pp. 161-185 ; M. De Goede, "Risk, Preemption and exception in the war on terrorist financing", in L. Amoore and M. De Goede (eds), *Risk and the War on Terror*, London: Routledge, 2008, pp. 97-112.

[34]D. Bigo, L. Bonelli and T. Deltombe (eds), *Au nom du 11 septembre… Les démocraties à l'épreuve de l'antiterrorisme*, Paris: La Découverte, 2008; D. Bigo, "Globalized-In-Security: the Field and the Ban-Opticon", in N. Sakai and J. Solomon (eds), *Translation, Biopolitics, Colonial Difference*, Hong Kong: University of Hong Kong Press, 2006, pp. 109-156.

[35]This specific logic of prevention is also related to blacklisting and asset-freezing measures. See: A. Amicelle, "Désigner et geler: les listes noires de l'Union européenne", in E. Saulnier-Cassia (ed), *La lutte contre le terrorisme dans le droit et la jurisprudence de l'Union européenne*, Paris: Mission de recherche Droit et Justice, 2012; B. Hayes and G. Sullivan, "Blacklisted: Targeted sanctions, preemptive security and fundamental rights", ECCHR: 10 years after 9/11 Publication Series, 2010.

As a result, the main purpose of the transatlantic agreement on the TFTP is not the transnational communication of financial personal data, as legal instruments already exist for this. Above all, TFTP promoters have aimed to remove information-sharing practices from the *justice/judicial/penal/criminal investigation* framework and incorporate them within the logic of *security/intelligence/administrative/prevention*. This specific logic of prevention has been the main legitimation narrative of the US TFTP and the transatlantic agreement. However, this added value of the TFTP is not substantiated in any of the TFTP case examples described in official reports.[36] Every single detailed example is related to an investigation after a violent event occurred, never before.

The Norwegian case of Anders Behring Breivik on 22 July 2011 has recently been offered as a "particularly striking example" in which the TFTP was used "to fight and prevent terrorism".[37] "TFTP-based information helped Norwegian and other European investigators, including Europol, to identify within hours the channels through which Breivik collected and moved the funds that he used for the preparation of his brutal attacks. The more knowledge is gained on the financial patterns of such terrorists ('lone wolves'), the better are law enforcement and other authorities prepared to understand the thinking of such individuals and ultimately to prevent similar attacks".[38]

Although the Breivik case is used to illustrate the relevance of the TFTP, the case mainly serves to weaken the argument for the added value of the programme and its preventive legitimation. According to the official statement, the TFTP provided information about Breivik's profile (i.e. financial patterns) that can be used to monitor and prevent future similar events. While one should critically analyse this claim of the preventive ability to connect the dots of possible future events through profiling practices, we can certainly question the specific added value of the TFTP regarding access to Breivik's financial data. The investigation started after Breivik's crimes, not before; TFTP was only valuable because it was directed at a criminal event that already happened. Pre-existing legal instruments (i.e. mutual legal assistance) and law enforcement institutions (i.e. financial intelligence units) could have been used to obtain the same amount of information about Breivik's financial patterns. The TFTP brought little benefit, if any.

However, before this happens, MEPs rejected the first version of the transatlantic TFTP agreement in February 2010, and a revised version was adopted several months later with a new vetting role for Europol.[39]

4. The Transatlantic Agreement and Europol

The Rejection of the First Agreement: Intra-Governmental and Inter-Institutional Tensions

As already mentioned, MEPs criticised the new EU-US negotiations in 2009 that aimed at reaching an

---

[36]J.-L. Bruguière, "Second report on the processing of EU-originating personal data by the United-States Treasury Departement for Counter Terrorism purposes: Terrorist Finance Tracking Program", Brussels, January 2010; European Commission, "Commission Staff Working Document – Report on the second joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program", Brussels, SWD(2012) 454 final, 14 December 2012.

[37]European Commission, "Commission Staff Working Document – Report on the second joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program", Brussels, SWD(2012) 454 final, 14 December 2012, pp. 14-15.

[38]Ibid.

[39]Council of the European Union, "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, 24 June; Council of the European Union, "Signature of EU-US agreement on financial messaging data for purposes of the US Terrorist Finance Tracking Program", Brussels, 28 June 2010; European Parliament, "European Parliament legislative resolution of 8 July 2010 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, 8 July 2010 .

agreement to ensure transatlantic data transfers regardless of SWIFT's new technical architecture. A resolution was adopted at the European Parliament in September 2009 to highlight privacy and data protection concerns.[40] Moreover, MEPs were still concerned about the possibility of economic and industrial espionage and they requested additional safeguards and specific mechanisms, such as a reciprocity mechanism "obliging the competent US authorities to transfer relevant financial messaging data to the competent EU authorities, upon request". There was also no unanimous position at the Council of the European Union in October 2009, with the delegations of Austria and Germany expressing concerns about data protection safeguards. Germany was quickly identified by US authorities as the critical actor in negotiations to strike a new deal. US diplomats "were 'astonished to learn how quickly rumours about alleged US economic espionage' had taken root among German politicians who opposed the program".[41] German concerns highlighted intra-European dissensions, while US intensive lobbying of the German delegation resulted in German intra-governmental controversies.

Transatlantic negotiations in relation to the TFTP took place at the same time as Angela Merkel's re-election in September/October 2009. This re-election ended the grand coalition with the Social Democratic Party in Germany (SPD) that existed from 2005 until 2009. The new federal coalition was formed by Merkel's group in Parliament – Christian Democratic Union (CDU) and Christian Social Union (CSU) – and the Free Democratic Party (FDP). These partners did not share the same opinion of the TFTP. Several FDP leaders had already expressed their concerns when the Swedish EU presidency received the negotiated mandate. According to a US diplomatic cable disclosed by WikiLeaks, Sabine Leutheusser-Schnarrenberger (a leading figure of the FDP who became justice minister under the new coalition) "had inserted language into the CDU/CSU-FDP coalition agreement specifically addressing the TFTP negotiations and directing Germany to call upon the EU to work towards a higher level of data protection".[42]

In response to this reluctance, US authorities put pressure on the German government to support the adoption of the new TFTP agreement at the EU Council on 30 November 2009. "[US] Ambassador Murphy met with [German] Interior Minister de Maizière on November 27 and urged him to support US-EU negotiations on an interim TFTP agreement, to which de Maizière indicated that he would abstain from voting on the agenda item at the November 30 COREPER meeting. De Maizière's decision, which followed a German request to shorten the duration of the interim agreement to nine months rather than twelve, facilitated the passing of the agreement as Germany was the strongest holdout. De Maizière's decision followed two weeks of intense lobbying in Berlin, Brussels and Washington by the Embassy in Berlin, USEU, the Departments of Treasury, State and Justice and the NSC. The campaign included calls by Secretaries Clinton, Geithner, the Attorney General and the National Security Advisor to their German counterparts. State Department Counter-Terrorism Coordinator Benjamin urged support for the agreement during a two-day visit to Berlin. Ambassador Murphy twice wrote to all five relevant ministers (Interior, Justice, Finance, Chancellery, and MFA) and made repeated calls to senior decision-makers, stressing the importance of the interim agreement and the need for Germany to not block it. The DCM, Econ M/C, and staff from multiple embassy sections heavily engaged on the issue as well. De Maizière (CDU) stressed that his decision was not an easy one given that the Christian Democrat/Social Union (CDU/CSU) and Free Democratic Party (FDP) coalition had differing views on the TFTP program".[43]

On one hand, the interior minister's decision to abstain from voting was welcomed by US authorities. On the other hand, his decision created significant tensions within the German coalition. Tensions between the CDU/CSU and the FDP added to the classic struggles in Germany between interior minister and justice minister. Thomas De Maizière overruled his ministerial colleague, Sabine Leutheusser-Schnarrenberger, who complained that her views were ignored and that the decision has "upset millions of citizens of Europe".[44]

---

[40]European Parliament, "European Parliament resolution of 17 September 2009 on the envisaged international agreement to make available to the United States Treasury Department financial payment messaging data to prevent and combat terrorism and terrorist financing".

[41]"Europe Wary of US Bank Monitors", *New York Times*, 5 December 2010.

[42]*WikiLeaks,* Ambassador Kennard's meeting with Spanish Permanent Representative to the EU. Cable 02 Brussels 128.

[43]Ibid.

[44]Ibid.

The EU-US TFTP agreement also reinforced tensions between EU institutions. Indeed, the agreement was adopted at the EU Council on the last day before the implementation of the Lisbon Treaty granted the European Parliament consent over international agreements such as the TFTP. Spain took the EU presidency one month later, and the Spanish permanent representative to the EU was "very concerned that the interim agreement on TFTP was reached on the last possible day before the Lisbon Treaty came into force, which meant 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".[45] Ultimately, members of the Civil Liberties, Justice and Home Affairs Parliament Committee (LIBE) called to reject the agreement on 5 February 2010 due to concerns about data protection as well as judicial recourse and lack of EU-US reciprocity regarding security practices.[46]

The TFTP agreement came into force on 1st February and the LIBE proposal was adopted at the European Parliament on 11th February (the published vote was 378 in favour and 196 against, with 31 abstentions). The TFTP agreement was therefore invalidated only 11 days after its official entry into force. This rejection represented a milestone event, with MEPs using their veto right (attributed by the Lisbon Treaty) for the very first time. To a certain extent, the European Parliament has become a fully-fledged institutional actor regarding EU-US security matters since this point in time. A revised version of the first agreement was finally adopted by MEPs in July 2010 as a result of further negotiation and with additional safeguards.[47]

Europol's Vetting Role in Practice

Two major last-minute elements were introduced in the second TFTP agreement after MEPs' rejection of the initial deal. First, the appointment of a European overseer in the United States was presented as an additional safeguard to "ensure that the [SWIFT] provided data [for the TFTP] is only accessed in cases where there is a clear nexus to terrorism or its financing, and the search of the data is narrowly tailored".[48] An overseer was recruited on a temporary basis in 2010, and the permanent EU overseer has been in place since May 2011. He has joined the former team of 'independent overseers' who have been recruited by SWIFT representatives to audit and supervise TFTP analysts' searches and uses of financial messages.

Second, the European Union's law enforcement agency (Europol) has been designated as the public body to monitor OFAC official's requests for SWIFT data to be transmitted from Europe. Now, US Treasury officials have to obtain Europol authorisation before each transfer of financial personal data that is stored in Europe by SWIFT (in the Netherlands and Switzerland). Europol staff's mission consists of checking whether US Treasury administrative production orders are sufficiently substantiated for counter-terrorism purposes and respectful of the agreement requirements. US requests also need to be "tailored as narrowly as possible in order to minimise the amount of data requested, taking due account of past and current terrorism risk analyses focused on message types and geography as well as perceived terrorism threats and vulnerabilities, geographic, threat, and vulnerability analyses; and not seek any data relating to the Single Euro Payments

[45]Ibid.

[46]European Parliament, "SWIFT: MEPs to vote on backing or sacking EU/US data sharing deal", Brussels, 5 February 2010.

[47]Council of the European Union, "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, 24 June 2010; Council of the European Union, "Signature of EU-US agreement on financial messaging data for purposes of the US Terrorist Finance Tracking Program", Brussels, 28 June 2010 ; European Parliament, "European Parliament legislative resolution of 8 July 2010 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, 8 July 2010.

[48]European Commission, "Commission Staff Working Document – Report on the second joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program", Brussels, SWD(2012) 454 final, 14 December 2012.

Area".[49] Europol officials can block transatlantic transfers of financial personal data if they conclude that US requests do not comply with the requirements of the transatlantic agreement. To do so, a new Europol unit has been created within the Operations Department – the O9 (TFTP) unit.[50]

Europol's vetting role has modified TFTP supervision in relation to principles of necessity and proportionality of US access to messages of international financial transactions. Although SWIFT representatives claimed that they "narrowed the scope of the [US Treasury] subpoenas to a *limited* set of data", [51] Europol's check has been promoted as *the* guarantee to ensure that US requests are tailored as narrowly as possible. Moreover, Europol's new role has been presented as the official response to MEPs' request for the designation of an EU public authority with the responsibility to review demands from the US Treasury Department. However, Europol's new role has also represented a significant concession by MEP's, as Parliament resolutions called for a public *judicial* body to review US requests and not for a public *law-enforcement* body such as Europol.[52]

The choice of Europol to discharge the new vetting responsibilities has a concrete effect on the type of verification that is enforced. While a judicial body would have checked US requests based on legal criteria and a data protection body would have checked US requests from a data protection perspective, Europol analysts assess US requests "in the light of operational considerations and security needs".[53] From this perspective, the attempt to remove the TFTP and information-sharing practices from the judicial framework has been a complete success. Furthermore, Europol's so-called 'guarantee' has been seriously challenged during the very first months of implementation of the transatlantic agreement.

In March 2011, representatives of the Europol Joint Supervisory Body (JSB) detailed the main conclusions of their first review of Europol's new task.[54] The JSB president underlined that "the most important 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".[55] Europol representatives notified JSB inspectors that Europol analysts also received oral briefings from US Treasury officials to approve requests that they reviewed. JSB representatives rejected this argument because confidential oral information is, by definition, impossible to supervise.

---

[49]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, OJ 2010, L 195/5, p. 4.

[50]With reference to the TFTP agreement, Europol's responsibilities are not limited to the vetting role regarding US requests to the extent that the O9 unit can also act as recipient of US intelligence related to the TFTP (i.e. Article 9 of the agreement) as well as requester of US intelligence related to the TFTP (i.e. Article 10). For further official information, see: Europol, "Terrorist finance tracking programme (TFTP) – The EU-US TFTP Agreement. Questions and Answers", The Hague; Europol (2011), "Europol activities in relation to the TFTP agreement information note to the European Parliament 1 August 2010 – 1 April 2011", The Hague, 8 April 2011.

[51]European Parliament, "SWIFT statement: Francis Vanbever, Chief Financial Officer, Member of the Executive Committee", Brussels, 4 October 2006.

[52]European Parliament, "European Parliament resolution of 17 September 2009 on the envisaged international agreement to make available to the United States Treasury Department financial payment messaging data to prevent and combat terrorism and terrorist financing".

[53]European Commission, "Commission Staff Working Document – Report on the second joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program", Brussels, SWD(2012) 454 final, 14 December 2012, p. 7.

[54]JSB is Europol's independent data protection supervisor. For further information, see the JSB website at http://europoljsb.consilium.europa.eu/about.aspx?lang=en

[55]Joint Supervisory Body, "Terrorist Finance Tracking Program (TFTP) agreement: Europol Joint Supervisory Body inspection raises serious concerns about compliance with data protection principles", 2 March 2011, p. 2; Joint Supervisory Body, "Report of the inspection of Europol's implementation of the TFTP agreement, conducted in November 2010 by the Europol Joint Supervisory Body", Brussels, 2 March 2011.

As a result, various actors underlined what they considered to be a supervisory gap in the implementation of the transatlantic agreement on the TFTP. Following the JSB's first inspection, Europol was seriously criticised over its verification task, especially in the European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE).[56] MEPs such as Sarah Ludford stated that "entrusting this task to Europol is like putting the fox in charge of the chicken coop".[57] Although the European Commission review team published a much more positive report on the first six months of implementation of the TFTP agreement, members of the review team also supported the JSB's concerns about the opacity of US oral briefings.[58] Finally, representatives of the German delegation at the European Council were concerned about a general lack of transparency from the European Commission and Europol in relation to the TFTP.[59] Europol representatives eventually sent further information to the European Parliament one month after the JSB's critical inspection.[60]

In November 2011, JSB officials conducted their second inspection of Europol's implementation of its task under the TFTP agreement. While their general conclusions highlighted that "Europol has made some progress", they also noticed various issues regarding US requests for SWIFT data that have always been accepted by Europol.[61] They made "clear that the US must improve the information provided in the requests". They claimed that "oral information provided by the US to Europol in regular, confidential briefing sessions apparently still plays a role in the verification of the requests. More transparency by the US is needed to allow Europol to verify the requests more effectively and to allow proper internal and external supervision".[62]

Although the director of Europol denied that US requests were mainly based on oral briefings, MEPs such as Sophie In't Veld criticised Europol for granting "requests orally over the telephone. It is a complete violation of the term of the agreement".[63] This criticism did not appear in the second joint review of the implementation of the agreement published by the European Commission in December 2012. "The EU review team believes that cooperation between Europol and the Treasury has resulted in substantial improvements […] and is satisfied that this process is proceeding in compliance with the agreement".[64] Nevertheless, the existence and potential significance of US oral briefings remains a matter of controversy. Another matter of controversy is the scope of US requests and the perpetuation of bulk data transfers.

---

[56]European Parliament (Press Release), "SWIFT implementation report: MEPs raise serious data protection concerns", Brussels, 16 March 2011.

[57]Ibid.

[58]European Commission, "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, 16 March 2011.

[59]German Delegation, "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, 8 February 2011.

[60]Europol, "Europol activities in relation to the TFTP agreement information note to the European Parliament 1 August 2010 – 1 April 2011", The Hague, 8 April 2011.

[61]Joint Supervisory Body, "Terrorist Finance Tracking Program (TFTP Agreement) - Second inspection by the Europol Joint Supervisory Body", 21 March 2012.

[62]Ibid.

[63]*EU Observer*, "EU hands personal data to US authorities on daily basis", 26 June 2012.

[64]European Commission, "Commission Staff Working Document – Report on the second joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program", Brussels, SWD(2012) 454 final, 14 December 2012.

5. *Mass* Intelligence and *Targeted* Surveillance

Although US requests have to be narrowly tailored, they still result in bulk data transfers. The EU review team and JSB inspectors have both agreed that Europol has received a US request on average every month, with each request covering a period of one month.[65] "The requests – when seen as a group – therefore essentially cover a continuous time period. To be clear, this means that one consequence of the agreement, as it is currently being implemented, is that data relating to certain financial transactions are provided by the designated provider [SWIFT] to the US for a time frame containing every single day of the year, year on year".[66] Any transfer of SWIFT data from Europe to the United States requires Europol authorisation, but the scope of each transfer is still extremely broad as US requests have never been individualised since the creation of the TFTP.

OFAC officials' subpoenas have never been individualised since 2001 because SWIFT operating centres cannot technically deal with targeted queries due to the encrypted structure of each SWIFT financial message. During the period from September 2001 to June 2006 (the time of the *New York Times*' disclosure), each US request was "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 US".[67] "The SWIFT system isn't made in the way that you can say I want M. X's transfers on the 16th of November, the 8th of June and 9th of August. It's not the system, you always get a bulk".[68]

These statements remain valid today. US officials do not immediately target and collect individualised data pertaining to a specific suspect. First, they request bulk data of SWIFT messages in connection with a specific time-span (one month, on average) and specific geographic areas such as between two countries. Then, the wide range of 'subpoenaed message' is entered into a US Treasury searchable database. Finally, US TFTP analysts use their own tools to launch specific searches within the searchable, large-scale database in order to open relevant SWIFT messages.[69]

The TFTP illustrates a specific conception of intelligence that is different from a classic form of espionage that entails intensive monitoring of small groups of individuals, mostly through human means. The TFTP represents *mass* intelligence through databases and transnational communication of bulk data of personal information about millions of individuals in order to monitor terrorist suspects. This conception of intelligence involves security programmes with dataveillance capabilities to extract information from electronic traces left by individuals in their daily life. It also involves computer tools for collecting, filtering, processing, sharing and disseminating this information.

Paradoxically, *mass* intelligence is officially justified in the name of *targeted* searches. US Treasury representatives have consistently claimed that "data provided by SWIFT is searched to extract only information that is related to an identified, pre-existing terrorism investigation".[70] Despite widespread European concerns about data-mining practices, US authorities have asserted that they have never conducted any *fishing expeditions* into the US Treasury's searchable database, or any data-mining processes and automated profiling initiatives. According to US statements since 2006 until now, "no search may be conducted on data unless a TFTP investigator provides pre-existing information demonstrating a *nexus*

---

[65]Ibid.

[66]Joint Supervisory Body, "Terrorist Finance Tracking Program (TFTP Agreement) - Second inspection by the Europol Joint Supervisory Body", 21 March 2012.

[67]Article 29 Data Protection Working Party, "Opinion 10/2006 on the processing of personal data by the society for Worldwide Interbank Financial Telecommunication (SWIFT)", Brussels, 22 November 2006.

[68]Interview with European official, European Commission, Directorate General Justice, Liberty and Security, June 2008.

[69]Council of the European Union, "Information Note: EU-US agreement on the processing and transfer of financial messaging data for purposes of the US terrorist Finance Tracking Program", Brussels, November 2009.

[70]Processing of EU originating Personal Data by United States Treasury Department for Counter Terrorism Purposes — 'SWIFT', OJ 2007, C 166/18, p. 4.

between the subject of the search and terrorism or its financing".[71] The TFTP is mainly promoted as a programme to visualise "terrorist networks" through the use of pre-existing information (i.e. a terrorism nexus) about known suspects to perform social network analysis in order to map their financial connections and so their potential relationships with *unknown terrorists*.[72] From this perspective, TFTP analysts are primarily focused on known individuals who fall into this so-called *terrorism nexus*. The critical issue is less data mining and algorithmic profiling than social network analysis derived from the terrorism nexus.

In other words, the critical questions are: Who falls into the terrorism nexus as defined by US agencies, and how?[73] What is the suspicion threshold? How is social network analysis performed? To what extent do US TFTP analysts go beyond the visualisation of known (i.e. terrorism nexus) suspects' financial relationships? In other words, to what extent do they analyse the other financial relationships of people who also have financial relationships with suspects, and so on?

With regards to the period from 2001 until 2006, US Treasury representatives notified that TFTP analysts opened and analysed less than 1% of the subset of SWIFT messages that were stored in their database. This very low percentage was cited to argue that the TFTP is a targeted surveillance scheme that is based on a pre-existing terrorism nexus. However, this statistic should be viewed in relation to the total number of collected messages in order to get a clearer picture of the scope of TFTP data processing. Although no exact figure has been provided by the US authorities since 2001, SWIFT officials confirmed that they received 64 US requests from September 2001 to June 2006.[74] As already mentioned, each request covered several weeks and several geographic areas. With daily SWIFT traffic of more than ten million messages, we can easily estimate that OFAC officials collected several hundred million messages during five years. As a result, although less than 1% seems to be very low at first glance, less than 1% of several hundred million of messages still represents a huge amount of processed personal data.

The principle of bulk transfer of personal data by SWIFT to the US government has remained one of the main concerns for MEPs and representatives of the European data protection authorities. While the transfer of bulk data of millions of innocent individuals for targeted searches on terrorist suspects is currently allowed under the transatlantic agreement, European officials are discussing a *legal and technical framework for the extraction of data on EU territory*. To create this, the next step would be an EU system equivalent to the US TFTP to stop transfers of bulk data, and this is the current issue at stake.

6. From Criticism to Imitation? The Project of an EU Terrorist Finance Tracking System

"The agreement also takes into account the European Parliament's call for a "two-step approach", i.e. initially allowing for transfers of bulk data until an EU system equivalent to the TFTP is established. This will result in more targeted transfers of data in the future".[75]

The possibility of a European terrorist finance tracking system is formally included in the current transatlantic agreement. It was first introduced in September 2009 by a European Parliament resolution, which "note[d] that it may be useful for the Commission to evaluate the necessity of setting up a European

[71]The United States Department of the Treasury, "Terrorist Finance Tracking Program. Questions and Answers", 2013.

[72]J.-L. Bruguière, "Second report on the processing of EU-originating personal data by the United-States Treasury Departement for Counter Terrorism purposes: Terrorist Finance Tracking Program", Brussels, January 2010.

[73]Statewatch, "News online: EU-USA: SWIFT-TFTP Agreement Report: Second Report on the processing of EU-originating personal data by the US Treasury Department for counter-terrorism purposes", September 2010.

[74]Commission de la protection de la vie privée (Royaume de Belgique), "Dossier Technique. Affaire SWIFT: La Commission belge de la protection de la vie privée (« CPVP ») demande de la transparence", June 2007.

[75]See the website of the directorate general Home Affairs of the European Commission (http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/tftp/index_en.htm).

TFTP".[76] With this proposal, MEPs aimed at stopping transatlantic communication of bulk data by a commercial company (SWIFT) to a third country (the United States). The inclusion of this option in the five-year agreement has been presented as European Parliament victory in the name of data protection and fundamental rights. "The key to the deal for the European Parliament is the eventual elimination of 'bulk' data transfers. In exchange for backing the agreement, MEPs won an undertaking that work on setting up an EU equivalent to the US Terrorism Finance Tracking Program (TFTP), which would preclude the need for bulk data transfers, will start within 12 months. Once Europe has a system enabling it to analyse data on its own territory, it need only transfer data relating to a specific terrorist track".[77]

Various European officials, including the EU counter-terrorism coordinator, supported the Parliament's proposal to promote the creation of an equivalent EU system. However, Gilles de Kerchove supported the EU system not simply in the name of data protection, he mainly justified it as "the development of a more equal partnership with the US" regarding security and intelligence practices.[78] This illustrates again the significance of the *information question* and the critical issue of equality between sovereign entities. Regarding the project of an EU equivalent system, European security actors are less motivated by data protection concerns than the end of the US informational monopoly on international financial data for security purposes.

As a result, the initial consensus on an equivalent EU system has been highly paradoxical. The idea of setting up a European TFTP has been officially associated with MEPs' disposition to take into account data protection in particular, and fundamental rights in general. However, the official argument of data protection has made possible the idea of a security project that was unthinkable a few years ago due also to concerns over fundamental rights, i.e. the project of a supranational EU security programme to collect, centralise and monitor huge amounts of personal data in relation to international financial transactions. "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".[79] The European context has slightly changed since this interview in 2007 with the emergence of an unlikely combination of conflicting interests that support the careful study of an EU TFTS.

In 2010, the European Commission was invited to submit to the European Parliament and the Council a legal and technical framework to extract US requested data on European soil. In July 2011, three options in relation to an *EU terrorist finance tracking system* were presented in a communication from the Commission.[80] These options were focused on the operationalisation of an EU TFTS and the possible creation of an EU searchable database of SWIFT messages that can be accessed by member states' national agencies (i.e. national financial intelligence units). Each option follows the same general scheme: first, EU requests to SWIFT; second, collection and storage of requested data in a new EU large-scale database; finally, a "targeted search" of the EU database and further analysis of the search results. However, the options are very different from each other. They reflect different conceptions of European cooperation in the field of security, i.e. European integration and Europol as a European security hub vs. inter-governmentalism and national agencies as the main security actors. The European Commission's options have attracted criticism from various perspectives and various groups of actors.

The strongest criticism has been expressed by MEPs and representatives of European data protection

---

[76]European Parliament resolution of 17 September 2009 on the envisaged international agreement to make available to the United States Treasury Department financial payment messaging data to prevent and combat terrorism and terrorist financing.

[77]European Parliament (Press Release), "Parliament gives green light for SWIFT II", Brussels, 8 July 2010.

[78]Council of the European Union, "Note from the EU Counter-Terrorism Coordinator to Council/European Council: EU Counter-Terrorism Strategy – discussion paper", Brussels, 15359/1/09, 26 November 2009.

[79]Interview with European official, Council of the European Union, Brussels, December 2007.

[80]European Commission, "Communication from the Commission to the European Parliament and the Council. A European terrorist finance tracking system: available options", Brussels, COM(2011) 429 final, 13 July 2011.

authorities. They are opposed to every single option in the communication from the Commission in relation to the project of an EU TFTS. "The requirement for a prior filtering of data within the EU is supported by the EDPS [European Data Protection Supervisor], as it would prevent the sending of bulk data to a third country. However, the Communication goes beyond the acknowledged purpose of filtering data in the EU, as it clearly indicates that the 'system should not be set up just to provide relevant information to US authorities', as the authorities of the member states 'have a real interest in the results of such a system as well'". [81]

In the interests of data protection, MEPs have called for a two-step approach but their call, in effect, is to imitate the US programme that they had previously criticised. Data protection claims are paradoxically interpreted as incentives for a European security programme with dataveillance capabilities that is particularly intrusive regarding individuals' right to privacy. According to the European data protection supervisor, "the Communication therefore seems to legitimise the setting up of a whole new TFTS scheme, in an EU-specific context, on the basis of the existing TFTP agreement. In other words, the Communication seems to justify the introduction of a new system which invades the privacy of EU citizens for the benefit of the authorities of EU member states while using as a justification the assessment of the utility of a system conceived and implemented to allow the US authorities to pursue their own investigation linked to terrorism. The EDPS has strong doubts about this approach, which does not appear to respect the principles of necessity and proportionality". [82]

From this perspective, the Commission's communication can be seen as an exercise of *function creep*, i.e. "the addition of new features beyond the scope of the original project",[83] in relation to MEP's original project. Furthermore, the communication tends to promote function creep in relation to the original US TFTP. What if the scope of the EU project of TFTS is broader than that of the US programme? The Commission's communication has briefly opened this debate with the statement that "there is little doubt that such access [to financial messaging data] would also be a valuable tool for combating other forms of serious crime, in particular organised crime and money laundering". [84]

Finally, tensions between security professionals are also framed by the Commission's options, which illustrate conflicting visions of *Security Europe*. The implementation of option one or two would reinforce the significance of Europol (and Eurojust, to a lesser extent). These options promote much more centralised forms of European cooperation, with the EU TFTS database managed by Europol. With reference to the current TFTP practices, the EU review team, which is headed by a senior Commission official, clearly supports Europol as the European Union's operational hub. "The EU review team is aware that the Agreement does not contain any obligations for member states to proceed through Europol and that they continue to be able to submit requests for TFTP searches directly to the Treasury. However, in order to improve the EU's response to terrorism and its financing and to control the application of the Agreement's safeguards, it would be very useful to have Europol as the EU's single contact point or, where requests are directly submitted to the Treasury, to have the member states inform Europol of such requests in a systematic and timely manner, at least in all those cases in which the request is generated by law enforcement authorities". [85] In contrast, the third option of the communication is associated with a process of cooperation that would primarily involve national agencies (i.e. financial intelligence units) rather than Europol. National delegations, including France, support this intergovernmental option that gives the lead to national

---

[81] European Data Protection Supervisor (2011), "Comments on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 13 July 2011: "A European terrorist finance tracking system: Available options"", Brussels, 25 October 2011, p. 1.

[82] Ibid.

[83] D. Lyon (2008), *Surveillance Studies: An Overview*, Cambridge: Polity Press, 2008, p. 201.

[84] European Commission (2011), "Communication from the Commission to the European Parliament and the Council. A European terrorist finance tracking system: available options", Brussels, COM(2011) 429 final, 13 July, 2008, p. 7.

[85] European Commission, "Commission Staff Working Document – Report on the second joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program", Brussels, SWD(2012) 454 final, 14 December 2012, p. 13.

authorities rather than to Europol in operating the EU TFTS database.[86]

Once again, the *information question* plays a critical role in the three options. Here, it is not related to power relationships between sovereign entities, but to power relationships between national and supranational security agencies in Europe. The creation of the EU TFTS would represent a tremendously symbolic resource for the security agency (or agencies) that will be chosen to manage the EU large-scale database. The redistribution of power within the field of European security is one of the key controversies of this project.

Conclusion

The paper has examined the main controversies in relation to the US Terrorist Finance Tracking Program. Based on this examination, the following conclusion highlights several key findings and makes recommendations regarding the transatlantic agreement and the project of an equivalent EU system.

First of all, the rationale of the current transatlantic agreement deserves further attention. Indeed, the logic of the TFTP relegates the classic legal-criminal procedures to the service of preventive access to personal data. It circumvents the *justice/judicial/penal/criminal investigation* framework based on the *security/intelligence/administrative/prevention* rationale. While prevention is promoted as the main justification for various programmes including the TFTP, a clear-cut political debate would be welcomed in relation to the use of the multifaceted notion of 'prevention' in the field of security. The same word covers many different things.

Promoting the prevention of "security threats" through "targeted development assistance, strategies for reducing poverty, or restoration programmes for natural or manmade disasters"[87] is completely different from a posture of deterrence or the current "shift towards dataveillance, proactivity and prevention".[88] These elements are not mutually exclusive, but it seems necessary to clarify them and their hierarchy in European security strategy. While there is "an urgent need for a uniform legal definition of the concept of 'profiling'"[89], there is also a need to clarify the meaning of prevention, as this notion is used as the legitimation narrative of security-focused programmes with dataveillance capabilities. Of particular concern is the duplication and overlap of security measures in the name of the *security/intelligence/administrative/prevention* logic, although the preventive added value of the new measures is not based on evidence and has not been demonstrated in practice.

Second, Europol's vetting role constitutes a tricky compromise. It has been widely presented as a major concession by TFTP supporters to MEPs' concerns, but it can also be interpreted as a significant concession by MEPs to TFTP supporters as well. European deputies called for an EU public judicial body to check US data requests, but a law-enforcement agency has been designated. The mandatory assessment of US demands is exclusively based on operational considerations and security needs. The implementation of this verification task has emerged as a critical matter in the context of confidential oral briefings and Europol's acceptance of every single US requests of transatlantic data transfers until now.

Although the Joint Supervisory Body of Europol is involved in reviewing the practices of the Europol 09 unit, there are grounds for more inclusion of EU "freedom agencies" to reinforce transparency, accountability

---

[86]Council of the European Union, "Note from the French delegation to CATS. France's position with respect to TFTP", Brussels, 13716/11, 2 September 2011.

[87]European Parliament Committee on Civil Liberties, Justice and Home Affairs, "Report on the European Union's Internal Security Strategy" ((2010)2308(INI)), Rapporteur: Rita Borsellino, Brussels, 24 April 2012, p. 7.

[88]D. Bigo et al., "Towards a New EU Legal Framework for Data Protection and Privacy: Challenges, Principles and the Role of the European Parliament", study requested by the European Parliament's Committee on Civil Liberties, 2012 (http://www.ceps.be/book/towards-new-eu-legal-framework-data-protection-and-privacy-challenges-principles-and-role-europ).

[89]European Parliament Committee on Civil Liberties, Justice and Home Affairs (2011), "Report on the EU Counter-Terrorism Policy: main achievements and future challenges" (2010/2311(INI)), Rapporteur: Sophia In't Veld, 20 July, p. 7.

and, ultimately, trust. The inclusion of EU bodies such as the EDPS and the Article 29 Working Party[90] should be seen as an efficient way to respond to the "public sensitivity" noted by Europol officials in order to avoid further controversies. With reference to the Lisbon Treaty, the 'de-pillarisation' process and the negotiation of a new EU legal framework for data protection and privacy, the review mechanisms in place should be reconsidered. As already mentioned in other studies, "supervisory bodies within EU agencies should at the very least be organised into a network, and a common supervision system under the EDPS should be established".[91] This framework of oversight will be all the more welcome for assessing the operational move towards mass intelligence, large-scale databases and "global data transfers".[92]

Third, the project of an equivalent EU system to the US TFTP is highly paradoxical in that it imitates what has previously been harshly criticised. While the possibility of an EU system was initially justified by the European Parliament to restrict transatlantic transfers of bulk data, the current proposal extends financial dataveillance and even mentions the possibility of adding new features beyond the scope of the US programme. In other words, the call by MEPs for more data protection has led to the Commission's proposal for less privacy. A general discussion about the adequate articulation of privacy and data protection rights is all the more important to provide a proper basis for examining the project of an EU terrorist finance tracking system. Although there are various overlaps and interrelations between both rights, "much can be learned from making and ascertaining the differences in scope, rationale and logic between privacy on the one hand, and data protection on the other".[93]

The main purpose of data protection consists of regulating the processing of personal data by introducing procedural safeguards to protect fundamental rights. Data protection regulations aim at ensuring transparency and accountability for data record-holders. Those regulations are not intended to block data processing, but to guarantee its channelling and control. According to Serge Gutwirth and Paul de Hert, data protection can be understood as a "transparency tool" intended to compel data record-holders to "fair information practices" or "good practices".[94] This "transparency tool" is focused on issues of oversight and legal requirements regarding data processing. Privacy, on the other hand, can be framed as an "opacity tool" intended to establish limits regarding interference by the state and commercial actors.[95] While data protection refers to a "regulated acceptance" of legitimate data processing, privacy refers to a "prohibition" of illegitimate and excessive use of power.[96] Thus, the "opacity tool" (privacy) is focused on the "necessity" of a certain security-focused programme with surveillance capabilities in a democratic society.

The opportunity and the design of an EU TFTS should be critically discussed from this privacy perspective, at least. To what extent is EU imitation of the US TFTP necessary in European democratic society? Furthermore, the current negotiation of a new European legal framework for data protection and privacy should strongly address the issue of third-country data transfer/processing and the critical "lacuna in EU law

---

[90]Launched in 1996, the Article 29 Working Party is made up of a representative from the data protection authority of each EU member state, the European Data Protection Supervisor and the European Commission.

[91]A. Scherrer, J. Jeandesboz and E.-P. Guittet (2011), "Developing an EU Internal Security Strategy, fighting terrorism and organised crime", Study requested by the European Parliament's Committee on Civil Liberties, p. 120 (http://www.europarl.europa.eu/document/activities/cont/201206/20120627ATT47777/20120627ATT47777EN.pdf)

[92]E. Guild, "Global data transfers: the human rights implications", *INEX Policy Brief*, No. 9, 2010.

[93]S. Gutwirth and P. De Hert, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power", in E. Claes, A. Duff and S. Gutwirth (eds), *Privacy and the criminal law*, Antwerp, Oxford: Intersentia, 2006, pp. 61-104; PACT Consortium (2012), "Discussion paper about the theoretical foundations of PACT", *The Privacy & Security Research Series*, No. 2, 2012.

[94]Ibid. See also C. Bennett and C. Raab, *The governance of privacy. Policy instruments in a global perspective*, Cambridge and London: MIT Press, 2006.

[95]S. Gutwirth and P. De Hert, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power", in E. Claes, A. Duff and S. Gutwirth (eds), *Privacy and the criminal law*, Antwerp, Oxford: Intersentia,2006, pp. 61-104; R. Gellert and S. Gutwirth (forthcoming), "Beyond accountability, the return to privacy?" in D. Guagnin et al. (eds), *Managing privacy through accountability*, Basingstoke: Palgrave Macmillan.

[96]Ibid.

and policy regarding private sector and law enforcement cooperation".[97]

The fundamental paradox resulting from MEPs' intervention in the TFTP negotiation should also be emphasised. While the European Parliament now fully engages with EU-US security matters, MEPs also run the risk of further legitimising the European reproduction of US programmes that they previously denounced as problematic.

Finally, European concerns have been focused on the massive transfer of personal data (including EU citizens' data) between a European commercial company (SWIFT) and a third country (the United States). However, access to SWIFT data is not only an EU-US issue, as SWIFT messaging services are officially delivered in 212 countries. SWIFT's new technical architecture, Europol's vetting role and the project of EU equivalent system have caused a slight re-balancing in the power relationships between the European Union and the United States. However, the situation has remained unchanged regarding third countries and their citizens all over the world. Democratic debate of the TFTP and any other US security programme of global dataveillance should move beyond Euro-centrism.

[97]D. Bigo et al.,"Open Season for Data Fishing on the Web. The Challenges of the US PRISM Programme for the EU", CEPS Policy Brief, No. 293, 2013 (www.ceps.be/book/open-season-data-fishing-web-challenges-us-prism-programme-eu).

ABOUT CEPS

Founded in Brussels in 1983, the Centre for European Policy Studies (CEPS) is widely recognised as the most experienced and authoritative think tank operating in the European Union today. CEPS acts as a leading forum for debate on EU affairs, distinguished by its strong in-house research capacity, complemented by an extensive network of partner institutes throughout the world.

Goals

- Carry out state-of-the-art policy research leading to innovative solutions to the challenges facing Europe today,
- Maintain the highest standards of academic excellence and unqualified independence
- Act as a forum for discussion among all stakeholders in the European policy process, and
- Provide a regular flow of authoritative publications offering policy analysis and recommendations,

Assets

- Multidisciplinary, multinational & multicultural research team of knowledgeable analysts,
- Participation in several research networks, comprising other highly reputable research institutes from throughout Europe, to complement and consolidate CEPS' research expertise and to extend its outreach,
- An extensive membership base of some 132 Corporate Members and 118 Institutional Members, which provide expertise and practical experience and act as a sounding board for the feasibility of CEPS policy proposals.

Programme Structure

In-house Research Programmes

Economic and Social Welfare Policies
Financial Institutions and Markets
Energy and Climate Change
EU Foreign, Security and Neighbourhood Policy
Justice and Home Affairs
Politics and Institutions
Regulatory Affairs
Agricultural and Rural Policy

Independent Research Institutes managed by CEPS

European Capital Markets Institute (ECMI)
European Credit Research Institute (ECRI)

Research Networks organised by CEPS

European Climate Platform (ECP)
European Network for Better Regulation (ENBR)
European Network of Economic Policy Research Institutes (ENEPRI)
European Policy Institutes Network (EPIN)