EU-US COOPERATION IN COUNTER-TERRORISM: TIME FOR SWIFT III?

LUCA MARIA THIEME Assessor Iuris

SUBMITTED IN FULFILMENT OF REQUIREMENTS OF THE DEGREE OF

LLM (BY RESEARCH)

School of Law, College of Social Sciences

University of Glasgow

July 2018

ABSTRACT

This thesis investigates the legal compatibility of the establishment of an EU Terrorist Finance Tracking System with EU primary law.

Currently, financial intelligence capacities for counter-terrorism purposes are outsourced to the United States which run a Terrorist Finance Tracking Program in order to detect 'terrorist monies' in international bank transfers. Known as the SWIFT II Agreement, this cooperation has been praised as a valuable tool for the EU's security and condemned for its fundamental rights intrusiveness. The thesis identifies the deficiencies of the United States' practice as opposed to the black letter words of the Agreement. Analysing the latest EU case law on the rights to privacy and data protection, SWIFT II is scrutinised against the criteria set out by the Court of Justice of the European Union. It is argued that the transatlantic cooperation fails to meet the high standards stipulated by the Court in various ways.

From the entry into force of the Agreement, the set-up of a European system was considered as a desirable alternative in order to restore fundamental rights compliance. Whilst the idea was dismissed in 2013 due to its cost-intensity and impact on EU fundamental rights, it has been reanimated in light of the numerous terrorist atrocities on European soil during the last three years. However, the EU Commission is now heading for a complementary scheme to SWIFT II. It is submitted that a European equivalent to the Terrorist Finance Tracking Program can be modelled in conformity with the Court's understanding of individual privacy and data protection. However, assuming that Europol was to be tasked with its operation, the thesis supports a restrictive interpretation of EU competence in matters of police cooperation and doubts that the EU could rely on the ordinary legislative procedure to do so.

Nevertheless, it is concluded that SWIFT II is practically immune to EU legal scrutiny and will perpetuate violating the rights enshrined in primary law unless renegotiated with regard to the criteria established in EU case law.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

Many thanks are due to Iain and Moira who provided so much helpful advice and were great conversation partners throughout my time in Glasgow. I also want to thank Cansin and Denis for their solidarity and friendship and Cansin's offer to use her office most of the year. I owe my gratitude to Joanne and Jacqui for making me feel home in Glasgow from the very first day.

This adventure would not have been possible without the indulgence of my family and Andreas who gave me their unconditional support. Finally, I want to extend my gratitude to Gleiss Lutz for giving me the opportunity to 'go ahead'.

To little Susi Sunshine.

AUTHOR'S DECLARATION

'I declare that, except where explicit reference is made to the contribution of others, that this dissertation is the result of my own work, and has not been submitted for any other degree at the University of Glasgow or any other institution.'

PRINTED NAME: Luca Maria Thieme

SIGNATURE: _____

LIST OF ABBREVIATIONS

AFSJ .....Area of Freedom, Security and Justice
APA .....U.S. Administartive Procedure Act
CJEU.....Court of Justice of the European Union
DPO.....Data Protection Officer
DRI..... Case Digital Rights Ireland and Others
..... v Minister for Communications, Marine and Natural Resources and Others
ECJ .....European Court of Justice
EU..... European Union
EUCFR.....EU Charter of Fundamental Rights
ECHR ..... European Charter of Human Rights
ECtHR .....European Court of Human Rights
EDPS.....European Data Protection Supervisor
FOIA .....U.S. Freedom of Information Act
MEP..... Member of the European Parliament
EP.....European Parliament
EU TFTS.....EU Terrorist Finance Tracking System
JSB.....Europol Joint Suspervisory Body
LIBE ..... European Parliament Committee on Civil Liberties, Justice and Hime Affairs
MLA..... Mutual Legal Assistance
PNR..... Passenger Name Records
PNR Canada ..... Opinion EU-Canada PNR-Agreement
Schrems..... Case Schrems v Data Protection Commissioner
SWIFT .....Society of Worldwide Interbank Financial Telecommunications
Tele2 ..... Case Tele2 Sverige and Secretary of State for the Home Department
..... v Post- och telestyrelsen and Others
TFTP..... Terrorist Finance Tracking Program
U.S.....United States
USPA..... 1974 U.S. Privacy Act
UST ..... United States Department of the Treasury

A. INTRODUCTION

SWIFT (the *Society of Worldwide Interbank Financial Telecommunications*)[1] is the financial world's major 'post service' with nearly 30 million transactions channelled through its network per day.[2] Among those, in all probability, are terrorist monies spent on recruitment, training and equipment for future suicide attackers and foreign fighters. It is the mission of the EU – U.S. cooperation under the so-called SWIFT II Agreement[3] to identify and drain money flows of terrorist groups and their supporters by analysing suspicious SWIFT messages.

The agreement has encountered opposition from the outset for different reasons; primarily, bulk data transfers to U.S. territory have been disputed for their compatibility with European Human Rights standards on privacy and data protection. On the other hand, political stakeholders have argued that the U.S.-led analysis of financial data was a critical tool for the EU's counter-terrorism strategy to succeed.[4] The set-up of a European-led Terrorist Finance Tracking scheme has been mutually understood as a desirable alternative to SWIFT II. After the EU Commission submitted a feasibility study in 2013 which recommended not to pursue the project of a European programme in substitution of SWIFT II,[5] the idea has been reanimated in the 2016 *Action Plan on strengthening the fight against terrorism financing*.[6] It is this thesis' purpose to discuss the legality of the current agreement and assess a favourable option for a future SWIFT III.

I. Subject matter and methodology

Although the adoption and coming into force of SWIFT I and II caught the attention of politicians, media and scholars,[7] the agreement's long-term implementation and

[1] A cooperative society under Belgian law with headquarter in La Hulpe, SWIFT facilitates trans-border transactions and thus provides a critical infrastructure of the international finance industry.
[2] SWIFT, <https://www.swift.com/about-us/highlights-2017> accessed 16 April 2018.
[3] 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 (adopted 13 July 2010; entered into force 01 August 2010) [2010] OJ L195/5.
[4] For this and the previous see: EP Plenary Verbatim Record (10 February 2010) P7_CRE(2010)02-10, 158ff.
[5] Commission, A European terrorist finance tracking system (EU TFTS), COM(2013) 842 final, 34.
[6] Commission, Communication on an Action Plan for strengthening the fight against terrorist financing, COM(2016) 50 final.
[7] E.g.: Letter from Jacob Kohnstamm (Art. 29 Working Party) and Francesco Pizzetti (Working Party on Police and Justice) to Juan Fernando Lopez Aguilar (LIBE Committee)

operation has been followed less closely.[8] Against the background of growing case-law of the Court of Justice of the European Union (CJEU) on privacy and data protection from 2014 on,[9] this is somewhat surprising. As opposed to the analysis and transfer of Passenger Name Records which finally became subject of a legal opinion delivered by the Court in 2017,[10] SWIFT II has rarely been cross-checked with the newly established criteria set forth in Luxembourg case-law.[11]

An exception is the work of Mara Wesseling who, pursuing a socio-legal approach, continuously analysed the political developments in the 'SWIFT affair' from 2010 on.[12] In her latest publication on *An EU Terrorist Finance Tracking System* (EU TFTS), Wesseling raises legal questions concerning an EU scheme's concurrence with EU fundamental rights.[13] The present thesis builds on these questions assessing the compliance of SWIFT II and a potential SWIFT III scheme with the privacy and data protection standards stipulated by the CJEU. Beyond the problem of human rights compliance, the study challenges the tacit, albeit general assumption of EU competence in this matter, in order to determine if a system comparable to the U.S. programme could be established at EU level at all.

(25 June 2010); Valentina Pop 'MEP: Swift "secrecy" may hamper new data deals with US' (*euobserver*, 28 February 2011) <https://euobserver.com/institutional/31880> accessed 17 April 2018; Sylvia Kierkegaard, 'US war on terror EU SWIFT(ly) signs blank cheque on EU data' (2011) 27 Computer Law & Security R, 449ff.

[8] Apart from periodic Joint Reviews conducted by the Contracting Parties according to art.13 SWIFT II (see nos.48, 51, 54).

[9] In particular: Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Others v Minister for Communications, Marine and Natural Resources and Others* [2014] ECLI:EU:C:2014:238; Joined Cases C-203/15 and C-698/15 *Tele2 Sverige and Secretary of State for the Home Department v Post- och telestyrelsen and Others* [2016] ECLI:EU:C:2016:970; Case C-362/14 *Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650.

[10] Opinion 1/15 *EU-Canada PNR-Agreement* [2017] ECLI:EU:C:2016:656.

[11] In fact, only three publications apply the Court's rulings of 2014 until 2016 to SWIFT II: Franziska Boehm and Mark D. Cole, 'Data Retention after the Judgement of the Court of Justice of the European Union' (2014), 72ff., arguing that SWIFT II is in breach of EU fundamental rights; alike: Carolin Möller, *The Evolution of Data Protection and Privacy in the Public Security Context – An Institutional Analysis of Three EU Data Retention and Access Regimes* (PhD thesis, 2017), 175ff.; dissenting: Will R. Mbioh, 'The TFTP Agreement, Schrems Rights, and the Saugmandsgaard Requirements' (2016) 20 J Internet L 29ff.

[12] with Marieke de Goede and Louise Amoore, 'Data Wars Beyond Surveillance: Opening the black box of Swift' (2012) 5 J Cultural Economy 49; *The European Fight against Terrorism Financing, Professional Fields and New Governing Practices* (Boxpress 2013); 'Evaluation of EU measures to combat terrorist financing' (In-depth Analysis for LIBE, 2014); 'An EU Terrorist Finance Tracking System' (Occasional Paper, RUSI September 2016).

[13] *Ibid* (2016), 23f.

The analysis is based on primary sources, namely the EU treaties and the text of the current agreement, along with CJEU documents, EU policy documents, scholarly publications and other secondary sources. The overall approach remains dogmatic; nevertheless, it displays some hybrid features with law in context research as much as EU law allows for extended modes of legal exposition.[14] Moreover, analysing the agreement's implementation in reality and comparing practice with the black letter provisions, the thesis' aim is also to contribute to law reform regarding a future EU-led programme.

II. Outline of the thesis

Chapter 1 summarises the development of the EU-U.S. cooperation on SWIFT data so far, putting it into the context of transatlantic data transfers for law enforcement and counter-terrorism purposes in general. Additionally, *inter alia* building on the findings of Wesseling, data processing under the current agreement is explained in detail. In chapter 2, the stages of data processing identified in the previous chapter are scrutinised against the standard of privacy and data protection enshrined in the EU Charter of Fundamental Rights (EUCFR) as interpreted by the CJEU. Consequently, chapter 3 drafts a model of an EU TFTS coherent with the requirements outlined in chapter 2. Finally, chapter 4 answers the question if the EU could establish a programme as described in chapter 3 as an ordinary matter of shared competence in the Area of Freedom, Security and Justice. In some concluding remarks, the main options for further action are presented.

[14] The methodological pluralism (*inter alia*) coming with Europeanisation of legal-dogmatic research is described in: Jan Vranken, 'Exiting Times for Legal Scholarship' (2012) 2 Recht en Methode in onderzoek en onderwijs 42, 50f., 55ff.

B. Chapter 1: Background and operation of SWIFT II

This chapter provides factual information about the development of the EU-U.S. SWIFT cooperation and its implementation in practice today. Whilst the first section mainly focusses on the period preceding the signature of SWIFT II in 2010, the second section reconstructs its functioning on the basis of Joint Review Reports submitted by the EU Commission in accordance with the provisions of the agreement from 2011 on. It will be shown that the U.S. programme underwent a remarkable evolution from a clandestine, unilateral intelligence scheme to a transatlantic partnership. Furthermore, it is explained why critics coined it 'a fishing expedition' whereas supporters praised the programme as 'a sharp harpoon' in the fight against terrorism.[15]

I. From unilateral intelligence gathering to SWIFT II: a chronology

1. Revelation of the TFTP

In June 2006, several American newspapers revealed the existence of a secret intelligence unit of the U.S. Treasury (UST) tasked to analyse international money transfers in order to identify sources of terrorist financing and hitherto unknown associates of terrorist organisations.[16] For purposes of a Terrorist Finance Tracking Program (TFTP), the UST had subpoenaed massive amounts of financial messaging data from the U.S. SWIFT operations centre by way of monthly issued production orders without any court approval;[17] from 2002 on, TFTP investigators practically had access to the company's entire database, including data of European account holders.[18]

---

[15] Barton Gellman *et al*, 'Bank Records Secretly Tapped' (The Washington Post, 23 June 2006), citing UST Undersecretary Stuart Levey.

[16] *Ibid*; Josh Meyer and Greg Miller, 'U.S. Secretly Tracks Global Bank Data' (LA Times, 23 June 2006) <http://articles.latimes.com/2006/jun/23/nation/na-swift23>; Eric Lichtblau and James Risen, 'Bank Data Is Sifted by U.S. in Secret to Block Terror' (The NY Times, 23 June 2017) <http://www.nytimes.com/2006/06/23/washington/23intel.html?emc=eta1>; both accessed 06 March 2017.

[17] Invoking Presidential E.O. 13224 of 23 September 2001 on Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten To Commit, or Support Terrorism 66 FR 49079, in particular art.7 thereof.

[18] Cf. Lichtblau/Risen, *supra* no.16, citing a person familiar with the operation as saying: 'At first, they got everything — the entire Swift database'; according to the Belgian Data Protection Commission, Opinion No. 37/2006 of 27 September 2006 on the Transfer of Personal Data by the CSLR SWIFT by Virtue of UST (OFAC) Subpoenas (inofficial translation into English) (2006), 5, SWIFT had refused any cooperation with U.S. intelligence agencies before 9/11, but subsequently did not seek judicial redress against the broad administrative subpoenas under the TFTP.

The reaction on behalf of the European Community and its Member States was vehement and dismissive;[19] European data protection watchdogs and Parliamentarians called for an immediate termination of the programme and insisted that the U.S. comply with Mutual Legal Assistance (MLA) mechanisms in order to acquire European personal data.[20] An EU-U.S. MLA Agreement had been negotiated and signed in 2003, with a specific provision on bank information.[21] As to other data transfers for law enforcement purposes, namely of Passenger Name Records (PNR), a specific agreement had already been found[22] and was to be renewed.[23] Against this background, the entirely covert operation of the TFTP could be interpreted only as an intentional circumvention of European data protection and privacy safeguards.[24]

In order to put the ongoing bulk transfer of SWIFT data on an official basis, the UST submitted unilateral 'Representations' in July 2007,[25] basically comprising the TFTP's data protection standards (negotiated with SWIFT as early as 2003[26]).

[19] Cf. Hans-Jürgen Schlamp, 'EU to Allow US Access to Bank Transaction Data' (spiegel online, 27 November 2009) <http://www.spiegel.de/international/europe/spying-on-terrorist-cash-flows-eu-to-allow-us-access-to-bank-transaction-data-a-663846.html> accessed 02 May 2018.
[20] EP, Resolution on the interception of bank transfer data from the SWIFT system by the US secret services (P6_TA(2006)0317) [2006] OJ CE303/843; Article 29 Working Party, Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) (WP128); EDPS, Opinion on the role of the European Central Bank in the SWIFT case [2007] <https://edps.europa.eu/sites/edp/files/publication/07-02-01_opinion_ecb_role_swift_en.pdf> accessed 06 March 2017.
[21] Agreement on mutual legal assistance between the European Union and the United States of America (EU-US) (adopted 25 June 2003, entered into force 01 January 2010) [2003] OJ L181/34.
[22] Agreement between the European Community and the United States of America on the Processing and Transfer of PNR Data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection (EU-US) (adopted 28 May 2004; out of force since 30 September 2006) [2004] OJ L183/84.
[23] Due to a lack of Community competence: ECJ, Joined cases C-317/04 and C-318/04 *European Parliament v Council of the European Union and Commission of the European Communities* [2006] ECR I-04721; after an Interim Agreement came into force at the end of 2006, a second PNR-Agreement was negotiated in 2007: Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) [2007] OJ L204, 16.
[24] However, U.S. parliamentary oversight bodies were not fully put on notice of the programme; UST officials explained the high demand for secrecy essential for the TFTP's operability: The Terror Finance Tracking Program: Hearing before the Subcomm. on Oversight and Investigations of the Comm. on Financing Services, 119 Cong. 2nd Sess. (2006), Serial No.109-125 (in particular Statement of Stuart Levey).
[25] United States, Processing of EU originating Data by United States Department for Counter Terrorism Purposes - SWIFT - Terrorist Finance Tracking Program - Representations of the United States Department of the Treasury [2007] OJ C166/18.
[26] Cf. Belgian Data Protection Commission, *supra* no.18, 6f.

A major concession of the U.S. government was the nomination of an 'eminent European person' mandated to oversee the TFTP's compliance with the Representations. Appointed to this post in 2008, French judge and counter-terrorism expert Jean Louis Bruguière came to the conclusion that the TFTP ran in conformity with the safeguards and guarantees, outlining its great value in the fight against terrorism.[27]

2. SWIFT I and II

In an attempt to comply with both the U.S. subpoenas and European data protection regulations,[28] SWIFT adhered to the Safe Harbour principles in 2007.[29] At this point, SWIFT had already decided to rearrange its security structure by the end of 2009[30] and from then on to process its data separately in an European and a transatlantic zone, thus keeping EU financial data as well as SWIFT messages from Pakistan, Iraq and Sudan out of reach of UST production orders.[31] Since the company's re-architecture coincided with the EU Treaty reform, the EU Council and Commission were determined to finalize an arrangement with the U.S. on the processing of European SWIFT data before the European Parliament would gain the right of

[27] The reports were classified but leaked: Jean Louis Bruguière, Summary of the First Annual Report on the Processing of EU Originating Personal Data by the United States Treasury Department for Counter-Terrorism Purposes [2008] <http://www.statewatch.org/news/2011/apr/eu-usa-tftp-swift-1st-report-2008-judge-bruguiere.pdf>; Second Report on the Processing of EU-Originating Personal Data by the United States Treasury Department for Counter Terrorsim Purposes [2010] <http://www.statewatch.org/news/2010/aug/eu-usa-swift-2nd-bruguiere-report.pdf>; both accessed 02 May 2018.

[28] The collision of obligations in the SWIFT case is described in detail in: Patrick M. Connorton, 'Tracking Terrorist Financing Through SWIFT: When U.S. Subpoenas and Foreign Privacy Law Collide' (2007) 76 Fordham LR 283ff; however, the Belgian Data Protection Commission eventually released SWIFT from the allegation of having violated Belgian (and EU) data protection law: Decision of 9 December 2008 (free translation) <https://www.privacycommission.be/sites/privacycommission/files/documents/swift_decision_en_09_12_2008.pdf> accessed 19 April 2018.

[29] SWIFT, 'SWIFT completes transparency improvements and obtains registration for Safe Harbor' <https://www.swift.com/about-us/swift-and-data> accessed 04 April 2017; Commission, Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the U.S. Department of Commerce (2000/520/EC) [2000] OJ L215/7.

[30] SWIFT, 'SWIFT announces plans for system re-architecture' <https://www.swift.com/insights/press-releases/swift-announces-plans-for-system-re-architecture> accessed 04 April 2017; the EP had called the company to do so: Resolution on SWIFT, the PNR agreement and the transatlantic dialogue on these issues (P6_TA(2007)0039) [2007] OJ CE287/349.

[31] The installation of a common back-up centre in Switzerland made mirroring of European data to the American operations centre unnecessary: Ariadna Ripoll Servent and Alex MacKenzie, 'Is the EP Still a Data Protection Champion? The Case of SWIFT' (2011) 12 Perspectives on European Politics and Society 390, 394.

approval. An interim agreement was adopted on 30 November 2009,[32] just one day ahead of the entry into force of the Lisbon Treaty.

In comparison to the 2007 Representations, SWIFT I established a formalized procedure for U.S. data requests to be verified by governments of Belgium and the Netherlands where SWIFT's European headquarters and operations centre are located (art.4). Furthermore, the agreement established reciprocity and joined EU-U.S. review mechanisms (arts.8-10). However, SWIFT I failed to ban bulk data transfers to U.S. territory, or to provide individual rights to access or rectification, or independent oversight, or enhanced limitations to dissemination.[33] The EU Parliament rebuked the Council and Commission for their strategy and the flaws of the agreement.[34] In February 2010, due to a shift of legal opinion on the Parliament's right to participation,[35] the plenary took the chance to reject SWIFT I with the result that data transfers to the UST were blocked from then on.[36]

Since the failure to implement the interim agreement was perceived to have resulted in a severe security gap,[37] the EU urgently re-entered into negotiations with the U.S. on a long-term compromise. Hence the parties did not wait for the conclusion of a framework agreement on EU-U.S. data transfers for law enforcement

[32] 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 purposes of the Terrorist Finance Tracking Program (EU-US) (adopted 30 November 2009) [2010] OJ L8/11.

[33] EDPS, Comments 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 of 25 January 2010 <https://edps.europa.eu/sites/edp/files/publication/10-01-25_eu_us_data_exchange_en.pdf> accessed 02 May 2018.

[34] EP, 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 (P7_TA(2009)0016) [2010] OJ CE224/8.

[35] The legal services of the Council and Commission had issued a legal opinion on the matter, from: Jens Ambrock, *Die Übermittlung von SWIFT-Daten an die Terrorismusaufklärung der USA* (Duncker & Humblot 2013), 40.

[36] EP, Legislative Resolution of 11 February 2010 on the proposal for a 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 purposes of the Terrorist Finance Tracking Program (P7_TA(2010)0029) [2010] OJ C341E/100.

[37] See Remarks by Joseph Biden: EP Formal Sitting Verbatim Record (06 May 2010) P7_CRE(2010)OT-06, 41.

purposes[38] and adopted SWIFT II in July 2010.[39] SWIFT II addressed the Parliament's request for the exclusion of SEPA-data (art.4 para.2 lit.d), a narrower definition of terrorism (art.2) and the inclusion of expressly enumerated rights to access, rectification and redress (arts.14ff).[40] Nevertheless, no judicial oversight was established. As opposed to SWIFT I, Europol has been tasked with pre-approving the subpoenas (art.4 paras.3-5); additionally, monitoring the UST's processing practices has been mandated to a permanent European on-site overseer (art.12). Albeit concerns persisted as to the effectiveness of the individual rights stipulated under the agreement and its proportionality in general,[41] the Parliament approved the text, [42] but insisted that the Commission assess alternative options to bulk transfers under SWIFT II.[43]

3. Implementation

After SWIFT II had entered into force on 1 August 2010, parliamentary control of its implementation proved difficult on grounds of restricted access to information, including the identity of the EU on-site overseer and the reports on Europol's approval practice submitted by the Europol Joint Supervisory Body (JSB).[44]

---

[38] Negotiations on an 'Umbrella Agreement' started in May 2010: Commission, 'European Commission seeks high privacy standards in EU-US data protection agreement' <http://europa.eu/rapid/press-release_IP-10-609_en.htm?locale=en> accessed 06 April 2017.

[39] 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 [2010] OJ L195/3.

[40] LIBE, 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 (P7_A(2010)0224), 7f.

[41] EDPS, Opinion on the proposal for a 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 purposes of the Terrorist Finance Tracking Program (TFTP II) [2010] OJ C355/10; Letter to LIBE, *supra* no.7.

[42] EP, 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 (P7_TA(2010)0279) [2010] OJ CE351/453.

[43] EP, Resolution of 5 May 2010 on the Recommendation from the Commission to the Council to authorise the opening of negotiations for an agreement between the European Union and the United States of America to make available to the United States Treasury Department financial messaging data to prevent and combat terrorism and terrorist financing (P7_TA(2010)0143) [2010] OJ CE81/66.

[44] Pop, *supra* no.7; the complaint filed against the restriction of the report with the European Ombudsman was finally not decided upon, as the Ombudsman himself was not granted access to the documents due to the resistance of the UST: Decision of the

Moreover, the review mechanisms in place turned out to be dysfunctional. Whilst the JSB (in an official summary) concluded that all U.S. data request so far issued under SWIFT II were so broad and unclear in scope that it had been impossible for Europol to verify their compliance with the requirements set out in the agreement,[45] a Joint Review conducted according to art.12 found that Europol had exercised oversight sufficiently.[46] Remarkably, Europol had not rejected a single U.S. request. Neither did consecutive reports by the JSB[47] and the Joint Review group[48] enhance transparency; in particular, the total amount of data transferred to the UST remains secret until today.[49]

When Edward Snowden accused the NSA *inter alia* of having circumvented SWIFT II by backdoor-accessing SWIFT's networks, the Parliament called for the agreement's suspension in October 2013.[50] However, an investigation could not confirm the allegations[51] and the Council and Commission refrained from terminating or

---

European Ombudsman closing the inquiry into complaint 1148/2013/TN against the European Police Office (Europol) of 02 September 2014 <https://www.ombudsman.europa.eu/de/cases/decision.faces/de/54678/html.bookmark> accessed 06 April 2017.

[45] JSB, Report on the Inspection of Europol's Implementation of the TFTP Agreement, conducted in November 2010 <http://collections.internetmemory.org/haeu/20170706142918/http://europoljsb.europa.eu/media/111009/terrorist%20finance%20tracking%20program%20(tftp)%20inspection%20report%20-%20public%20version.pdf> accessed 02 May 2018.

[46] 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 17-18 February 2011 (Commission Staff Working Paper) SEC(2011) 438 final; eventually, a member of the European Joint Review team dissociated himself from the thoroughly positive wording of the report: Letter from Paul Breitbarth to Reinhard Priebe (14 April 2011) accessed 06 April 2017.

[47] Especially questioning the practice of bulk transfers and the lack of transparency: JSB, Europol JSB Inspects for the Second Year the Implementation of the TFTP Agreement <http://collections.internetmemory.org/haeu/20170706142918/http://europoljsb.europa.eu/media/205081/tftp%20public%20statement%20-%20final%20-%20march%202012.pdf> accessed 02 May 2018.

[48] Commission, 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 October 2012 (Commission Staff Working Document) SWD(2012) 454 final.

[49] *Ibid*, 15, the UST only indicates the trend of increase or decrease of data transferred; generally as to secrecy in the implementation of SWIFT II: Marieke de Goede and Mara Wesseling, 'Secrecy and security in transatlantic terrorism finance tracking' (2017) 39 J European Integration 253, 260ff.

[50] EP, Resolution of 23 October 2013 on the suspension of the TFTP agreement as a result of US National Security Agency surveillance (2013/2831(RSP)) [2016] OJ C208/153.

[51] Commission, Joint Review Report 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

suspending the agreement on grounds of U.S. misconduct. On the contrary, the importance of the ongoing cooperation by virtue of SWIFT II was reiterated at the end of November 2013, when the Commission issued a report on a joint evaluation of the TFTP's value under art.6 para.6 of the agreement[52] and, in parallel, a feasibility study on the establishment of an EU TFTS.[53] Whilst substituting SWIFT II with a European-led scheme was assessed as conflicting with EU Fundamental Rights and coming at a considerable expenditure, the results yielded from TFTP analyses were regarded as essential in the fight against international terrorism. Against the background of numerous terrorist incidents, among them the attack on Charlie Hebdo in January 2015, the latest Joint Review report of January 2017 upheld the conclusion that SWIFT II remained of outstanding value to the EU's counter-terrorism strategy.[54]

4. Exiting times for data protection

As opposed to SWIFT II's remarkable persistence, other EU instruments of data collection and transfer have sustained damage in the course of the NSA affair. The CJEU annulled the General Data Retention Directive in 2014 as well as the Safe Harbour scheme for commercial data transfers to the U.S. in 2015,[55] thereby putting into question draft PNR Agreements and the draft EU-U.S. Umbrella Agreement. Whilst Safe Harbour was replaced by the so-called Privacy Shield[56] and the Umbrella

---

the Terrorist Finance Tracking Program (Commission Staff Working Document) SWD(2014) 264 final, 19ff.

[52] Commission, Joint Report from the Commission and the U.S. Treasury Department regarding the value of TFTP Provided Data pursuant to Article 6 (6) of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messanging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, Annex to COM(2013) 843 final.

[53] Commission, A European terrorist finance tracking system (EU TFTS) COM(2013) 842 final.

[54] Commission, Joint Review Report 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 Commission Staff Working Document SWD(2017) 17 final.

[55] *DRI* and *Schrems*, *supra* no.9.

[56] Commission, Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield [2016] OJ L207/1; the adequacy decision based on Privacy Shield was challenged before the General Court which rejected the application as being inadmissible: Case T-670/16 *Digital Rights Ireland v. Commission* (2017) ECLI:EU:T:2017:838.

Agreement eventually entered into force in February 2017,[57] the adoption of a PNR-Agreement with Canada was stopped by the Court in summer 2017.[58]

In the meantime, the EU reformed its entire legislative framework on data protection, passing a Data Protection Regulation, a Directive on Data Processing for Law Enforcement Purposes, an EU PNR Directive[59] and a new Europol-Regulation in 2016.[60] It comes as no surprise that data processing under SWIFT II deviates from those newly established provisions in various ways. The next section will explain the regulatory framework of the agreement and its operation in practice.

II. How it works: SWIFT II

It has never been disclosed how financial data is processed in the course of SWIFT II. On the basis of the agreement's wording, official reports issued by oversight and review bodies, statements on behalf of Europol and the UST as well as various newspaper articles, the following paragraphs reconstruct the scheme's functioning in as much detail as possible. The TFTP's database ('black box')[61] and the methods applied to analyse the data stored therein form the heart of the entire process. Here, the analysis primarily builds on Wesseling's findings on the TFTP's logic and technology in order to shed light on the intelligence production by the UST. It will be shown that the provisions leave considerable discretion to the mandated agencies, and that the practice of their application might even contravene SWIFT II's wording and purpose. Before turning to the various stages of data processing

[57] Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences (adopted 02 June 2016, entered into force 01 February 2017) [2016] OJ L336/3.
[58] *PNR Canada*, *supra* no.10.
[59] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC; Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA; Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime; all published in [2016] OJ L119/1ff, 89ff, 132ff.
[60] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA [2016] OJ L135/53.
[61] The notion is taken from Wesseling *et al*, *supra* no.12, and from the Belgian Data Protection Commission, *supra* no.18, 5.

under the agreement, however, it shall be explained how SWIFT's messaging service works and why it is the most intelligible data source for the TFTP's purposes.

1. SWIFT FIN messages

As its official title reveals, SWIFT II regulates the transfer of financial messaging data; according to its Annexe, SWIFT is the solitary provider data is taken from. More precisely, it is SWIFT's core service FIN enabling the trans-border exchange of messages formatted in traditional SWIFT standard.[62]

In 2017, 7.1 billion FIN messages were sent through SWIFT's network[63] which is built in a V-structure of national concentrators (functioning as a letter box) and operations centres (comparable to postmen).[64] The sending bank generates a standardised SWIFT message comprising: an envelope ('header') *inter alia* containing the address of the sending and recipient bank and respective bank account numbers, the message type (e.g. customer fund transfer) and an authentication code; a letter ('body') with the main instructions for the transaction (amount of money, currency, value date, reference); a trailer which signals the end of the message.[65] In SWIFT's national concentration centre, the letter is encrypted and the message is deconstructed to packages. Sent to one of SWIFT's operations centres, the data packages are forwarded to the national concentrator allocated to the receiving bank as soon as the receiving bank signals receptivity. This national concentrator pieces the message together and approves its correctness, checking the authentication code of the envelope. The receiving bank decrypts the message and the same information is sent back through the network to the originator's bank. The receiving bank credits the designated amount to the beneficiary's account whereas the sending bank discounts the originator's account respectively. Through common settlement accounts, the involved banks finalise the transaction afterwards.[66] For purposes of claims management, the messages are mirrored to SWIFT's back-up centre in Switzerland where the copies are stored for 124 days.[67] This is the database of interest for the TFTP.

---

[62] Belgian Data Protection Commission, *ibid*.
[63] SWIFT, *supra* no.1.
[64] Susan V. Scott and Markos Zachariadis, *The Society for Worldwide Interbank Financial Telecommunication (SWIFT). Cooperative governance for network innovation, standards, and community* (Routledge 2014), 36.
[65] *Ibid*, 62ff.; other message types are, *inter alia*, travellers checks or precious metals and syndications.
[66] For this and the previous sentences: Ambrock, *supra* no.35, 23ff, 127ff.
[67] *Ibid*, 20ff.

2. The qualities of SWIFT data

From the perspective of intelligence and law enforcement agencies, SWIFT messages possess most convenient properties.[68] Firstly, FIN provides a large-scale database containing data on a variety of transactions between a variety of actors around the globe, most of which are communications data (names of sender and recipient, local branch of sender's bank, date and time of generation of message), giving away a lot of information on the persons involved in the transaction, for example their location at a specific moment in time.[69] Although the UST asserts that SWIFT data rarely contains sensitive information (as on sexual orientation, religious or political conviction etc., art.5 para.7), it is still possible to draw detailed conclusions on a person's private life from the messages, in particular from their reference which is also accessible to the investigators. Moreover, SWIFT data provides additional identification details of utmost relevance for counter-terrorism purposes, such as addresses, phone numbers or national ID-numbers (cf. art.5 para.7).[70]

Secondly, data processed through SWIFT's network are highly accurate and reliable,[71] for the obvious reason of the contractors' mutual interest in a smooth and successful transaction and reduction of unnecessary costs. Thirdly, FIN messages are standardised, reducing the effort of preliminary data cleansing which makes SWIFT data most valuable for automated data analysis.[72]

3. UST data requests

In order to receive data from SWIFT, the UST issues formal production orders (administrative subpoenas) to SWIFT. According to art.4 paras.1 and 2, those subpoenas must be tailored as narrowly as possible, that is to say that they have (1) to identify the requested data as clearly as possible, *inter alia* by naming specific

---

[68] Generally, see Statement of Stuart Levey, *supra* no.24, 13.
[69] Cf. Anthony Amicelle, 'The Great (Data) Bank Robbery: Terrorist Finance Tracking Program and the "SWIFT Affair"' (Centre d'études et de recherches internationales Sciences Po 2011), 10.
[70] Gellman *et al*, *supra* no.15, quoting Stuart Levey: 'The way the SWIFT data works, you would have all kinds of concrete information - addresses, phone numbers, real names, account numbers, […] the kind of actionable information that government officials can really follow up on'.
[71] Scott/Zachariadis, *supra* no.64, 65.
[72] For this and the previous, cf. Mary DeRosa, 'Data Mining and Data Analysis for Counterterrorism' (CSIS 2004) 3, 9.

data categories; (2) to clearly substantiate the necessity of the data for the purpose of the prevention, investigation, detection or prosecution of terrorism or terrorist financing; (3) to narrow down the scope of the request as far as possible by collating it with analyses of former requests and their investigative value for past and current terrorism operations, with suspected terrorist activities and with further situation analyses;[73] (4) to exclude SEPA-data.

According to Europol, the requests 'exhibit a certain level of abstraction.'[74] In practice, the production orders are issued for an average period of four weeks, comprise a list of targeted countries and denominate the categories of trans-border messages being sought.[75] The agreement merely indicates the information possibly included in the messages (art.5 para.7). SWIFT, however, would not be capable of singling out individual communications as its database is not equipped with this kind of search capacity.[76] Hence, the UST requests issued to the SWIFT company most certainly denominate mere standard FIN categories. Effectively, as observed by the JSB, the requests cover continuous money flows of entire countries.[77]

Allegedly, the UST has continuously reduced the amount of data requested by cutting down the list of identified message types and geographic regions deemed of relevance for counter-terrorism investigations.[78] To this end, the SWIFT data analysed by the TFTP are regularly audited for their investigative value.[79] Subsequently, TFTP analysts decide on the geographic and material scope of the requests and demonstrate the necessity of the requested data by providing past and current terrorism risk analyses and concrete past investigations,[80] supposedly relating to the concerned regions.

[73] See UST Representations, *supra* no.25.
[74] Europol, Europol Activities in Relation to the TFTP Agreement - Information Note to the European Parliament (1 August 2010 – 1 April 2011) (2011), 7; JSB, *supra* nos.45, 47.
[75] 2nd JSB report, *supra* no.47; Wesseling (2013), *supra* no.12, 168, assumes that Muslim countries are targeted mostly.
[76] Ambrock, *supra* no.35, 128.
[77] 2nd JSB report, *supra* no.47.
[78] Europol, *supra* no.74, 8.
[79] For this and the previous: 2nd Joint Review Report, *supra* no.48, 25.
[80] Europol, *supra* no.74, 4.

a. Approval by Europol

An exact copy of the production order with additional substantiation of its necessity is sent to Europol[81] which is in charge of pre-approving the data transfer (art.4 paras.3 and 4). The substantiation of the requests does not contain information on concrete investigations the data might be needed for, but refers to rather general threats emanating from already identified terrorists.[82]

The assessment of the requests is conducted according to the criteria set-out in art.4 para.2. However, it is Europol's understanding of art.4 para.2 that the review is of a purely operational nature. Thus, Europol cross-checks the UST's substantiating information with its own terrorism risk analyses without any legal assessment or access to the data requested.[83] By approving the requests and notifying SWIFT thereof, the production orders gain binding legal effect under European and U.S. law and thereby have to be obeyed by SWIFT which can challenge the subpoenas under U.S. law only (art.4 paras.5 and 6). Since Europol classifies all documents provided by the UST and all processes related to the requests as 'EU restricted', [84] European judicial and parliamentary oversight depends on the UST's consent to disclosure, which has not been given so far.[85]

b. Bulk transfer to UST black box

Eventually, SWIFT's back-up centre identifies bulk datasets comprising the data requested. After having transferred all data within the company's secure network to its U.S. operations centre, data are decrypted and forwarded to a UST server. For the purpose of transatlantic data transfer, art.8 of the agreement deems the UST as providing an adequate level of data protection as long as compliance with the agreement's privacy and data protection safeguards is ensured.

[81] Europol set-up a specialised 'Unit O9' tasked to implement SWIFT II and advised by Europol's Legal Affairs Unit and its DPO: *ibid*.
[82] *Ibid*; regarding those subjects and their respective networks, the UST provides additional personal data to Europol: 4th Joint Report, *supra* no.54, questionnaire no.14.
[83] Europol, *supra* no.74, 11, 8: whilst this understanding is shared by the Joint Review Group (2nd Joint Report, *supra* no.48, 6), Europol's DPO and the JSB took the position that art.4 para.2 requires an operational and legal assessment.
[84] Europol, *supra* no.74, 6.
[85] Cf. *supra* no.44.

4. Retention of data in UST black box

Bulk data provided by SWIFT are stored in the UST's searchable database. In the absence of an initial analysis regarding the data's concrete relevance for counter-terrorism purposes, all data-sets are taken into retention directly, irrespective of their sensitive nature or expectation of professional secrecy (art.5 para.7). Theoretically, the UST is obliged promptly and permanently to delete data erroneously transferred by SWIFT (art.6 para.2). However, with regard to the breadth of the requests, the transfer of unrequested data is unlikely to happen. Also, as will be explained in the consecutive paragraphs, the UST does not delete any individual datasets from the warehouse before the maximum retention period has expired.

a. Data security and integrity

The TFTP black box is subject to high security standards as stipulated in art.5 para.4: The database must provide a secure physical environment, is to be maintained with high-capacity systems and be subject to physical intrusion controls; transferred data must be stored separately from any other data and the black box shall not be interconnected with any other database. Thus, SWIFT messages cannot be cross-checked with information from other sources before being formally extracted from the black box in course of an individualised search (art.5 paras.5 and 6). The database is not connected to the Internet and furthermore secured by digital security clearances.[86] Access to stored data must be limited to TFTP analysts, technical supporters, data base managers and overseers. Moreover, data must not to be copied except for disaster recovery back-ups and are protected from any manipulation, alteration or addition in the black box.[87] Interestingly, the latter requirement prevents the UST from correcting or deleting incorrect data which are therefore merely flagged inaccurate.[88] Finally, all searches in the black box (art.5 para.6) and every onward transfer of TFTP-derived leads (art.7 lit.f) must be log-filed.

b. Retention period

The length of retention of individual datasets depends on whether the data are extracted or remain unaccessed. Extracted data are retained as long as necessary

[86] UST Representations, *supra* no.24.
[87] *Ibid*.
[88] 2nd Joint Review Report, *supra* no.48, 11f.

for the concrete investigation or prosecution they were extracted for, art.6 para.7. Non-extracted data, however, are stored up to five years in the black box, art.6 para.4.

The agreement remains indefinite as to extracted data that could not affirm any suspicion of terrorist activity whatsoever. Art.6 para.1 obliges the UST to delete any data no longer deemed necessary for counter-terrorism purposes. Whether art.6 para.1 refers only to the extracted copies or includes raw data stored in the black box, is not clear. Even if the UST would conclude that such data were of no more relevance in general, the obligation to delete is subject to technical feasibility. According to the UST, however, the administration of the black box and the management of massive amounts of data contained therein are highly complex, resulting in the UST's practice of adhering to the five year retention period apparently without exception.[89] Moreover, reviews of the appropriateness of the retention period under art.6 paras.5, 6 and art.13 repeatedly came to the conclusion that a shorter time of storage would significantly hamper the achievement of the TFTP's objective.[90]

5. At the core of the TFTP: extraction and analysis

The analysis of SWIFT data provided to the UST's black box is dealt with in art.5. Generally, para.2 legitimates processing only for the prevention, investigation, detection or prosecution of terrorism or its financing. However, it is para.3 that contains the surprising statement that '[t]he TFTP does not and shall not involve data mining or any other type of algorithmic or automated profiling or computer filtering'. On the basis of Wesseling's work, it will be demonstrated that data analysis for the purposes of the TFTP in fact does require the deployment of highly sophisticated technologies of automated processing.

a. Targeted search in the black box

Under the terms of art.5 paras.5 and 6, TFTP investigators have to articulate a concrete terrorism nexus in order to access the database for a search. Searches are conducted with a TFTP-designed search-and-retrieval software by means of which individual names or bank accounts can be run against the entire dataset.[91] According

[89] *Ibid*, 10; 3rd Joint Review Report, *supra* no.51, 15f; 4th Joint Report, *supra* no.54, 15f.
[90] *Ibid*.
[91] Cf. TFTP Value Report, *supra* no.52, 4; Belgian Data Protection Commission, *supra* no.18, 6.

to art.5 para.5, this terrorism nexus must be drawn from 'pre-existing information or evidence' giving 'a reason to believe' that the concerned person or bank account is associated with terrorist activity. Since the TFTP-derived information is not designed to serve as evidence in court proceedings ('lead purposes only', art.7 lit.c),[92] the threshold of suspicion does not necessarily amount to the legal criterion of reasonable suspicion normally applied in law enforcement operations.

Furthermore, it is not known where the name or bank account number and the respective information or evidence is taken from. Allegedly, TFTP investigators run searches on suspects' names from various secret terrorist watch lists maintained by FBI and Homeland Security comprising more than a million names, most of which are of Muslim origin.[93] How persons end up on these watch lists is subject to secrecy as well and neither exposed to legal oversight nor individual redress.[94] It cannot be ruled out that the information the listing is based on was gathered under circumstances of severe human rights violations.[95]

Search terms must be as narrowly tailored as possible and are log-filed together with the supporting information (art.5 para.6). The implementation of the criteria set out in art.5 paras.5 and 6 is subject to the oversight mechanism of art.12, that is to say that SWIFT-scrutineers and EU overseers[96] can enter the searches in real time or retrospectively, having the authority to block searches or their further analysis and dissemination because of inappropriately broad search terms or insufficient substantiating material. According to the Joint Review Reports, oversight is conducted on (nearly) all searches in the black box, resulting in the overseers blocking a minute fraction of all cases for too broad search terms.[97]

---

[92] UST Representations, *supra* no.25.
[93] Amicelle, *supra* no.69, 23; Wesseling *et al*, *supra* no.12, 55.
[94] Marieke de Goede and Gavin Sullivan, 'The politics of security lists' (2016) 34 Environment and Planning D: Society and Space 67, 73ff.
[95] *Ibid*; furthermore: Cf. John Bohannon, 'Investigating Networks: The Dark Side' (2009) 325 Science 410f.
[96] Despite art.12 provides for only one EU appointee, the UST consented to a deputy overseer: 2nd Joint Review Report, *supra* no.48, 8f.
[97] From February 2011 to September 2012, the overseers queried 791 out of 31,797 searches, of which 57 searches were blocked for overly broad search terms: 2nd Joint Review Report, *supra* no.48, 33; from October 2012 to February 2014, 621 of 22,838 searches were queried, including 30 queries for too broad search terms: 3rd Joint Review Report, *supra* no.51, 38; between March 2014 and December 2015, the overseers queried 450 from 27,095 searches, 29 of which were blocked for too broad search terms: 4th Joint Review Report, *supra* no.54, 38.

b. Extraction of contact chains

The method allegedly applied in order to extract the data from the black box is called link analysis.[98] [99] Thereby, starting from a targeted subject, a network of contacts is built, mapping associates of associates.[100] Also known as 'contact chaining', this technique of automated data analysis has been deployed by NSA investigators in the PRISM programme, going up three links from the person under suspicion.[101] Since terrorist networks are known to be organised decentrally, their associates are seldom linked directly; according to the research the TFTP's conception was probably based on, active participants are on average connected through more than four links which can be 'shortcut' to less than three by identifying complementary participants who, inter alia, provide financial funding.[102] Thus, it is plausible that the TFTP takes three to four 'hops' away from the person or bank account under suspicion.

Although the UST depicts its approach as 'extremely targeted' and only accessing data 'directly responsive' to the search term,[103] it is a known phenomenon since 1929 that every person can be connected to anybody else worldwide through six handshakes;[104] in the era of social media, it takes less than four.[105] For these indiscriminate effects, Wesseling portrays the TFTP as a 'cluster bomb'.[106]

---

[98] Meyer and Miller, *supra* no.16.

[99] A form of automated data analysis, link analysis is defined as 'subject-based […] us[ing] public records or other large collections of data to find links between a subject – a suspect, an adress, or other piece of relevant information – and other people, places or things' - DeRosa, *supra* no.72, VI; the persons (financially) associated with the subject of investigation appear as 'dots' and their interrelations, appearing as 'edges', can be qualified in terms of their intensity and centrality to the network or other criteria which might be useful for a terrorism investigation – Aparna Basu, 'Social Network Analysis: A Methodology for Studying Terrorism', in: Mrutyunjaya Panda *et al* (eds), *Social Networking: Mining, Visualization and Security* (Springer 2014), 215, 221ff.

[100] Basu, *ibid*, 219.

[101] Kenton Powell and Greg Chen, 'Three degress of separation' (The Guardian, 1 November 2013) <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1> accessed 02 May 2018; according to Wesseling (2013), *supra* no.12, 160, the CIA went up to five or six links.

[102] Basu, *supra* no.99, 225ff.

[103] UST Representations, *supra* no.25.

[104] Albert-László Barabási, 'Scale-Free Networks: A Decade and Beyond' (2009) 325 Science 412.

[105] Smriti Bhagat *et al*, 'Three and a half degrees of separation' (Facebook research, 2016) <https://research.fb.com/three-and-a-half-degrees-of-separation/> accessed 08 May 2017.

[106] Wesseling (2013), *supra* no.12, 160.

c. Why link analysis alone is not enough

However, in order to identify terrorist networks, the deployment of link analysis alone has been doubted as an appropriate investigative method.[107] Since the raw networks are based on mere financial linkage between two or more people, they necessarily contain a (supposedly high) number of false-positives. This is why the assessment of the TFTP-generated networks is the crucial part of each investigation.[108] According to the UST's Intelligence Department FinCEN, the investigative potential of link analysis is realized through the integration of (many) disparate sources of information, thus adding 'layers of understanding to the behaviour that the data represents'.[109]

This is where techniques of data mining might be combined with link analysis to improve a network's informative value[110] and reduce its noise (of false-positives).[111] As opposed to link analysis, data mining is a pattern-based method of automated data analysis using algorithms to discover useful, previously unknown knowledge hidden in large and complex datasets.[112] As long as the data's quality and the comprehensiveness of the data-mining model are adequate, the application of this technique can notably reduce the false-positive quota.[113] If the assumption of a three to four link extraction holds true, the raw networks must be considerably large and indiscriminate, requiring a time-efficient and diligent filtering method. Against this background, it can be ruled out that TFTP analysts sort out data manually.[114]

d. Quality of TFTP-derived information

How exactly TFTP analysts distinguish 'valuable' from false-positive leads is not known; it has neither been revealed how many data-sets are usually extracted from the black box nor indicated how many contacts on average are affirmed as suspicious. The UST resists disclosing any numbers arguing that a search in the black

[107] Bohannon, *supra* no.95, 410f.
[108] For this and the previous: DeRosa, *supra* no.72, 14f; Wesseling (2013), *supra* no.12, 162.
[109] UST (Financial Crimes Enforcement Network), *Feasibility of a Cross-Border Electronic Funds Transfer Reporting System under the Bank Secrecy Act* (2006), 10.
[110] Cf. Bohannon, *supra* no.95, 411.
[111] DeRosa, *supra* no.72, 11f.
[112] *Ibid*, 3.
[113] *Ibid*, 11f, 14f.
[114] Ambrock, *supra* no.35, 153ff; Wesseling (2013), *supra* no.12, 161f.; Hannah C. Bloch-Wehba, 'Global Governance in the Information Age: The Terrorist Finance Tracking Program' (2013) 45 NYUJInt'l L&P 595, 635.

box can result in multiple hits or none at all.[115] Despite art.13 para.2 declaring "the number of financial payment messages accessed" in the remit of the Joint Review, the reports merely indicate an increase or decrease of SWIFT messages provided to the UST black box during the respective review period.[116]

Nevertheless, the cooperation on the TFTP has been praised as highly valuable, filling information gaps and uncovering connections other sources would not spot.[117] According to former UST officials, the TFTP targets predominantly 'lower- and mid-level terrorists and financiers who believe they have not been detected.' '[T]racking the flow of funds, rather than seeking to disrupt them, to learn how terrorist networks are organised',[118] the programme primarily enhances mobility control of previously known suspects instead of general data driven surveillance.[119] Thus, even non-responsive searches can reveal that the suspect probably has withdrawn from official financial networks, has moved to another country or has been eliminated successfully.

6. Further usage and dissemination

Finally, it remains secret what exactly TFTP-derived information is consequently used for. Most probably, there is a certain back-flow to the terrorist watch lists, either resulting in an up- or down-listing of the person under suspicion of terrorist activity or their deletion from the list. On the basis of TFTP-derived intelligence, administrative action ranging from asset freezing up to extrajudicial detention might be initiated by the UST or other U.S. government departments.[120] Since TFTP-derived information shall serve for lead purposes only and is not designed to provide evidence in judicial proceedings, the extraction method and analysis is at no point subject to judicial review. The review mechanisms established through the agreement itself are limited either to the question of access to the black box (art.12) or to the value of the 'output' of the programme in particular cases (art.13). Only the intelligence committees of the U.S. Congress potentially have authority to exercise parliamentary control on the TFTP's analysis methods.[121]

---

[115] 4th Joint Review Report, *supra* no.54, 9.
[116] *Ibid*.
[117] Value Report, *supra* no.52, 5.
[118] For this and the previous: Meyer and Miller, surpa no.16, citing UST Undersecretary Stuart Levey.
[119] Amicelle, *supra* no.69, 10.
[120] Amicelle, *ibid*, 7f.; Wesseling (2014), *supra* no.12, 27.
[121] Generally, the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence exercise oversight on U.S. intelligence activity.

Eventually, 'leads' and 'reports' are shared with other law enforcement, public security or other counter terrorism authorities of the U.S., EU Member States or third countries, or with Europol or Eurojust or other appropriate international bodies (art.7 lit.b), possibly consisting of raw personal data or a mere summary of the analysis conducted by the TFTP beforehand.[122]

a. Reciprocity mechanisms with Europe

Data sharing with 'Europe' is basically laid down in the provisions on reciprocity (arts.9 and 10). That is to say that information can be provided spontaneously by the TFTP to Member States, Europol or Eurojust under art.9 or can be requested by the Member States, Europol or Eurojust under art.10 if they determine that there is a reason to believe that a person or entity has a nexus to terrorism or its financing. Whilst Member States' requests were rarely issued at the beginning of the agreement's implementation, their number has dramatically risen since the attacks on the headquarters of Charlie Hebdo[123] and are supposedly still increasing in light of the high frequency of terrorist incidents on European territory during the last year. According to the Joint Reviews, the UST shares single leads or whole reports comprised of multiple leads with Member States authorities and Europol on a regular basis.[124] The communication is normally channelled through Europol's single point of contact.[125] Presumably, any TFTP-derived information is classified by the UST and thus will also be classified as 'EU restricted' by Europol alike.

b. Dissemination to third countries

Dissemination to third countries, on the other hand, does not require that the authority that information is forwarded to must provide an adequate level of data protection. Only when the information shared involves a citizen or resident of a Member State is the dissemination to a third country subject to prior consent of the respective Member State, unless an existing protocol between the UST and the Member State provides general allowance or that data sharing is essential for the prevention of an immediate and serious threat to public security of the U.S., a Member State or a third country. In the latter case, the respective Member State shall be notified at the earliest opportunity (art.7 lit.d).

[122] Wesseling (2014), *supra* no.12, 26.
[123] 4th Joint Review Report, *supra* no.53, 50.
[124] For this and the previous: 4th Joint Review Report, *supra* no.54, 7.
[125] Europol, *supra* no.74, 5.

7. Exercise of individual rights

In arts.15, 16 and 18, SWIFT II provides for individual rights of the data subject. Their exercise in practice turned out to be rather challenging since, due to the UST's restrictive interpretation of the agreement, these rights apply to extracted data only and are subject to a number of derogations and limitations.

Firstly, as art.5 para.5 requires a concrete terrorism nexus to be demonstrated ahead of any access to the black box, the UST refuses to provide access to unextracted data for purposes of art.15.[126] Furthermore, the right to access can be reduced to the mere statement that the data processing has been in conformity with the provisions of the agreement (para.1). However, after data have been responsive to a search in the black box and therefore (potentially) display a terrorism nexus (though this nexus might be entirely indirect), the derogation clause of para.2 applies; thus, the exception of refusing access to information is turned to the rule. Para.2 allows for broad derogations of the right to access, *inter alia* the protection of public or national security, regularly including counter-terrorism investigations.

Secondly, the right to rectification, erasure and blocking of erroneous data or data processed in contradiction to the agreement is hampered by the strict provisions on the maintenance of the security and integrity of the database. Whilst any application under art.16 requires due substantiation (para.2)[127] which, in the absence of detailed prior access to the datasets, is already an enormous obstacle to any data subject, the UST reduces art.16 to a right to the flagging of data that shall be prevented from future processing.[128]

---

[126] 3rd Joint Review Report, *supra* no.51, 17f.

[127] The UST *inter alia* requires 'a precise identification of the record, including a description of the record, the date, and any other identifying details' and 'a statement regarding why the information is not accurate or complete, including supporting evidence', 'If the person making the request wishes to correct or add any information, the request is to contain specific proposed language for the desired correction or addition.' <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Terrorist-Finance-Tracking/Documents/Revised%20Redress%20Procedures%20for%20Web%20Posting%20(8-8-11).pdf> accessed 03 July 2018.

[128] *Supra* no.88; interestingly, 'to date, no erroneous data have been discovered' <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Terrorist-Finance-Tracking/Documents/tftp_brochure_03152016.pdf> accessed 03 June 2018.

Thirdly, art.18 para.2 does not provide for a specific right to redress but merely refers to U.S. law generally.[129] The UST's website mentions administrative and judicial redress under the Administrative Procedure Act (APA)[130] and the Freedom of Information Act (FOIA)[131].[132] With the Umbrella Agreement and the 2015 Judicial Redress Act,[133] EU citizens and rightful EU residents are furthermore granted redress rights under the 1974 U.S. Privacy Act (USPA).[134] However, apart from the problem of demonstrating legal standing before U.S. courts in secret surveillance cases,[135] the exemptions granted to law enforcement and security agencies effectively deprive data subjects of their rights altogether.[136] With the TFTP's exclusive purpose of counter-terrorism, injunctive claims are thus most likely to fail.

8. A theory-reality-gap

The foregoing paragraphs revealed several inconsistencies of the data processing by the UST in comparison to SWIFT II's wording. Nevertheless, the TFTP gradually has become an integral part of the EU's counter-terrorism policy and might even serve as a blueprint for an EU TFTS in future. What seems a paradoxical U-turn on behalf of the EU[137] might be explained by the increasing number of severe terrorist incidents on European soil since the adoption of SWIFT II.

However, whether SWIFT II indeed enhanced EU security is difficult to determine. Albeit most case studies cited in the Joint Review Reports represent post-attack

[129] Whilst art.18 para.2 also refers to the laws of the EU and its Member States, only Europol's approval of the UST requests or EU requests under art.10 could be challenged before European courts since there is no EU jurisdiction on UST data processing.
[130] 5 U.S.C. Subchapter 2.
[131] 5 U.S.C. § 552 (4) (B).
[132] UST, *supra* no.127.
[133] 5 U.S.C. 552a note.
[134] 5 U.S.C. § 552a (g)(1). Before, despite art.18 para.2 SWIFT II granting administrative and judicial redress to 'all persons', affected data subjects did still not fall in the personal scope of the Privacy Act due to art.20 para.1 SWIFT II: 'This Agreement shall not create or confer any right or benefit on any person (…)'.
[135] Neil M.Richards, 'The Dangers of Surveillance' (2013) 126 Harv LR 1934, 1962ff.; Wesseling (2014), *supra* no.12, 33.
[136] As to FOIA: UST Disclosure Services, 'Freedom of Information Act Handbook' (2010), 16ff; Bloch-Wehba, *supra* no.114, 623; as to USPA: US Federal Register Vol.79/No.71 (14 April 2014), 20971; Francesca Bignami, 'The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens' (Study for the LIBE Committee 2015), 12f.
[137] Anthony Amicelle, 'The EU's Paradoxical Efforts at Tracking the Financing of Terrorism: From criticism to imitation of dataveillance' (CEPS 2013).

investigations,[138] the TFTP's strategic approach is pre-emptive.[139] Whereas it seems generally desirable to identify and prevent terrorists from striking, the TFTP comes with the downside of collateral damage as an integral feature of the methods applied.[140] TFTP-verified suspects can be subjected to severe human rights intrusions (ranging from restraints in free-movement after a listing on a no-flight list to targeted killings);[141] those consequences are not necessarily limited to proven terrorists but may also be imposed on innocents who are affected merely for their everyday interaction with other suspects (and thus in most cases for their connection to a geographic area or religious community).

The next chapter investigates whether SWIFT II and the current practice under its regime could withstand the CJEU's scrutiny. Despite the above considerations implying that SWIFT II conflicts with several human rights guarantees, the focus of the investigation is kept on the rights to privacy and data protection under EU primary law.

[138] Wesseling (2014), *supra* no.12, 28; in the latest Joint Review Report, the statistics on leads shared with European law enforcement agencies corroborates this assumption: *supra* no.54, annex IIIC.
[139] Amicelle, *supra* no.69, 7.
[140] De Goede/Sullivan, *supra* no.94, 84 therefore coined the notion of 'collateral reality'.
[141] Wesseling (2014), *supra* no.12, 27.

C. Chapter 2: SWIFT II from CJEU perspective

This chapter shall answer the question whether SWIFT II meets the requirements established in the CJEU's recent case law on privacy and data protection. With its judgements on the EU General Data Retention Directive and respective national legislation, on the Safe Harbour scheme and the EU-Canada PNR-Agreement, the CJEU earned its reputation as a Human Rights court setting the benchmark for the regulation of new technologies in the digital age.[142] Although the focus is kept on the CJEU's landmark decisions, ECtHR case law on secret surveillance shall not remain unmentioned in the following section since the CJEU is used to referring to its Strasbourg counterpart in light of art.51 para.3 EUCFR.[143]

Firstly, the CJEU's general approach on data protection and privacy will be introduced; secondly, the CJEU's considerations on data retention, analysis and transfer are applied on SWIFT II according to the consecutive stages of data processing identified in chapter 1. Thirdly, in light of the previous findings, it will be summed up whether the UST indeed offers an adequate level of data protection as assumed in art.8 of the agreement.

I. The CJEU's approach on privacy and data protection

As opposed to the European Charter of Human Rights (ECHR),[144] art.8 EUCFR enshrines a right to data protection separate from the right to privacy found in art.7 EUCFR. Nonetheless, the CJEU rulings in *Digital Rights Ireland*, *Schrems*, *Tele 2 Sverige* and *PNR Canada* display the Court's understanding that both rights are inextricably linked and basically subject to the same interferences, justifications and safeguards.[145] Just as the ECtHR's approach on art.8 ECHR, the CJEU has been

---

[142] Cf. Federico Fabbrini, 'Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States' (2015) 28 Harv Hum Rts J 65, 81ff.

[143] *Inter alia DRI*, *supra* no.9, paras.35, 47, 54, 55: *Weber and Saravia v. Germany* ECHR 2006-XI 309, *Liberty and Others v. The United Kingdom* App. No. 58243/00 (ECtHR, 01 July 2008), *S. and Marper v. The United Kingdom* ECHR 2008-V 167, *M.K. v. France* App. No.19522/09 (ECtHR, 18 April 2013); *Tele2, ibid*, paras.119, 120: *Zakharov v. Russia* Appl. No. 47143/06 (ECtHR, 04 December 2015), *Szabó and Vissy v. Hungary* Appl. No. 37138/14 (ECtHR, 12 January 2016).

[144] In absence of a right to data protection in the Convention, the ECtHR understands data protection as subset of the right to privacy (art.8 ECHR): Nora Ni Loideain, 'Surveillance of Communications Data and Article 8 of the European Convention on Human Rights', in: Serge Gutwirth et al. (eds) *Reloading Data Protection* (Springer 2014), 183, 192f.

[145] In *DRI*, *supra* no.9, the interrelation of both rights was acknowledged by Advocate General Cruz Villalón although he kept arts.7 and 8 EUCFR separate in his Opinion, paras.54ff.

criticised for neglecting the distinct features of the right to privacy and the right to data protection which stem from their character as substantial and procedural guarantees respectively.[146] However, it is beyond this thesis' scope to discuss the interrelation of arts.7 and 8 EUCFR. The CJEU's reasoning on the draft EU-Canada PNR Agreement particularly lends itself to the legal assessment of SWIFT II; therefore, this chapter follows the CJEU's approach without taking a position as to its dogmatic persuasiveness or consistency.

1. General considerations of the Court

Generally, the Court considers every action of processing of personal data to interfere with arts.7 and 8 EUCFR, irrespective of the sensitivity of the data affected or the inconvenience caused.[147] As following from art.52 para.1 EUCFR, any interference with the essence of the rights to privacy or data protection is in breach of the Charter; this is deemed to be the case when the content of communications is accessed (art.7) or when data is processed in absence of any safeguards whatsover (art.8).[148] Furthermore, assuming a severe interference with both rights, the CJEU recognises that the mass collection and retention of metadata can be as sensitive as the processing of content data, running the risk of revealing entire personality profiles.[149]

However, neither art.7 nor art.8 provide for absolute protection;[150] the purposes of public security, in particular combatting terrorism, are objectives of general interest generally capable of justifying severe infringements as long as the measures envisaged are proportionate in order to achieve these objectives. That is to say that

---

[146] Aidan Forde, The Conceptual Relationship Between Privacy and Data Protection (2016) 1 CLR 135, 136, 143, 147ff. (inter alia with further reference to De Hert/Gutwirth and Lynskey); Gloria Gonzalez Fuster, 'Fighting for Your Right to What Exactly – The Convoluted Case Law of the EU Court of Justice on Privacy and/Or Personal Data Protection' (2014) 2 Birkbeck LR 263, 267ff.; Xavier Tracol, 'The judgment of the Grand Chamber dated 21 December 2016 in the two joint Tele2 Sverige and Watson cases: The need for a harmonised legal framework on the retention of data at EU level' (2017) 33 Computer L Security R 541, 549.

[147] *PNR Canada*, *supra* no.10, paras.122, 124; *DRI*, *supra* no.9, paras.26ff.; *Schrems*, *supra* no.9, para.87.

[148] *DRI*, *ibid*, para.39f.; *Schrems*, *ibid*, para.94; *PNR Canada*, *ibid*, para.180; interestingly, in *Tele2*, *supra* no.9, para.101, the Court only referred to content access with regard to both rights.

[149] *DRI*, *supra* no.9, paras.26ff.; *Tele2*, *supra* no.9, para.99; *PNR Canada*, *supra* no.10, paras.127f; the ECtHR has not yet acknowledged equal protection of metadata but seems to prepare for an alignment with the CJEU in that respect: *Szabó*, *supra* no.143, para.70; *Zakharov*, *supra* no.143, para.147; in the pending case of *10 Human Rights Organisations v. The United Kingdom* App. No. 8170/13, the Court will have the opportunity to do so.

[150] *PNR Canada*, *ibid*, para.136.

any limitation must not exceed the boundaries of what is appropriate and necessary.[151] Whilst the CJEU normally grants a certain margin of appreciation to the legislator when it comes to appropriateness and necessity,[152] in the context of privacy and data protection, any derogation and limitation must be strictly necessary, requiring the governing rules to be clear and precise in scope and application and to impose minimum safeguards against abuse of power.[153]

2. SWIFT data: all metadata?

SWIFT data requested and collected for purposes of the TFTP certainly enable UST analysts to draw very detailed conclusions on the account holder's activities on the basis of 'context data' of every transfer to and from the respective account(s). Whether all SWIFT data qualify as metadata, however, might be doubted. If some of the information processed by the TFTP was content rather than context data, this could provoke a violation of the essence of art.7. On the one hand, it can be argued that the transfers' reference provides some sort of content of the financial communication; on the other, EU law (including the CJEU's case law) lacks a consistent definition of metadata altogether.[154] It stands to reason to draw an analogy to the subject heading of a letter or an e-mail; here, it is also questioned whether such information can still be understood as metadata because its mere 'envelope' character cannot be decisive while revealing the underlying content of the body of the communication concerned.[155] This becomes particularly apparent with financial communications: whilst the 'body' of each SWIFT message *inter alia* contains the amount of money transferred, it is the reference line which gives away a transfer's purpose. Moreover, this information does not appear necessary for either SWIFT as messaging operator or its clients, mostly banks, to provide their respective services; rather, it merely serves as an identifier for the recipient account holder.

---

[151] *Ibid*, paras.140, 152f, 154ff.
[152] *DRI*, *supra* no.9, para.48.
[153] *DRI*, *ibid*, paras.51, 54f.; *Schrems*, *supra* no.9, paras.91f.; *Tele2*, *supra* no.9, paras. 96, 103, 109, 117; *PNR Canada*, *supra* no.10 para.140, 141.
[154] Cf. Sophie Stalla-Bourdillon *et al*, 'Metadata, Traffic Data, Communications Data, Service Use Information… What Is the Difference? Does the Difference Matter? An Interdisciplinary View from the UK', in: Serge Gutwirth *et al* (eds), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection* (Springer 2016); Loideain, *supra* no.144, 185.
[155] E.g.: Loideain, *ibid*, 199; Maria Tzanou, 'Is Data Protection the Same as Privacy? An Analysis of Telecommunications' Metadata Retention Measures' (2013) J Internet L 21, 29.

Nevertheless, the CJEU's opinion on the EU-Canada PNR Agreement suggests otherwise: As long as data collected does not typically contain private information or only reveals such information in particular circumstances and as to limited aspects of a person's private sphere, the essence of art.7 is respected.[156] As this understanding of content access is reduced to serious cases of privacy intrusions,[157] it would be unlikely for the CJEU to assume a core violation of art.7 with regard to SWIFT data because the messages' references regularly do not contain private information; where they do, the information is typically reduced to a very specific aspect of privacy.

Any infringement of the essence of art.8 is also out of the question, as it is the agreement's main purpose to establish a data protection regime, whether this regime be sufficient or not.[158] Whether SWIFT II's provisions limit the interferences with arts.7 and 8 to what is proportionate, will be investigated subsequently.

3. TFTP: an appropriate tool in counter-terrorism?

SWIFT II legitimises data processing for the prevention, investigation, detection and prosecution of terrorism or terrorist financing only (art.1). An objective of high priority, *inter alia* pursuing the protection of the rights and freedoms of others (art.6 EUCFR),[159] this purpose is capable of justifying far-reaching restrictions to the exercise of fundamental rights. Whilst SWIFT II provides a legal basis for the interferences in the course of the TFTP's operation,[160] the programme might turn out to be an inappropriate means to achieve that objective: it can be assumed that (jihadist) terrorists are likely to avoid channelling their monies through official systems but prefer alternative means of money transfer (for example the Islamic Hawala-system).[161] The CJEU, however, took the position that the suitability of a measure is not undermined by the possibility of circumventing the usage of certain

---

[156] *PNR Canada*, *supra* no.10, para.150.
[157] Boehm/Cole, *supra* no.11, 33 referring to *DRI*; however, the Court has been criticised for its distinction between content and metadata as regards the essence of privacy and data protection: Tracol, *supra* no.146, 549f.; Tuomas Ojanen, 'Making the Essence of Fundamental Rights Real: The Court of Justice of the European Union Clarifies the Structure of Fundamental Rights under the Charter' (2016) 12 EuConst 318, 327f.
[158] Dissenting: Maria Tzanou, *The Fundamental Right to Data Protection, Normative Value in the Context of Counter-Terrorism Surveillance* (Hart Publ. 2017), 211.
[159] *DRI*, *supra* no.9, para.42; *PNR Canada*, *supra* no.10, para.149
[160] Cf. *PNR Canada*, *ibid*, para.144ff. on the question whether an international agreement is a suitable legal basis in terms of art.52 EUCFR.
[161] This question was raised as early as 2006 by the U.S. House of Representatives: *supra* no.24.

technologies.[162] Moreover, when it comes to less intrusive alternatives, it can be ruled out that other means of law enforcement cooperation are indeed as efficient as SWIFT II's mechanism. Under art. 4 EU-US MLA-Agreement, requests must be individualised and based on reasonable suspicion (para.2 thereof); in order to trace the money flows of a single suspect, it might be necessary to approach several EU Member States for legal assistance, considerably delaying the acquisition of information. The TFTP's purpose to identify hitherto unknown terrorist associates would be hampered, if not entirely undermined.[163]

Thus, processing of mass SWIFT data can be deemed appropriate for counter-terrorism purposes in general. In the next section, the scheme's consecutive steps of data processing will be assessed against the Court's requirements on strict necessity.

II. From UST requests to intelligence sharing: Is SWIFT II strictly necessary to fight terrorist financing?

The criterion of strict necessity refers both to the formal quality of the law ('clear and precise rules') and the procedural safeguards provided against the abuse of power. In this respect, the CJEU criteria coincide with the legality principle applied in ECtHR case law, including the so-called *Weber criteria* for laws on secret surveillance.[164] The findings of chapter 1 already indicate that the agreement's wording is not sufficiently clear and precise. The following paragraphs will demonstrate that every single stage of data processing is likely to fall at the hurdle of strict necessity, for reasons of indefinite discretion of the UST and a lack of sufficient safeguards alike.

1. UST requests: general data retention?

The bulk transfers of European SWIFT data to the UST have been a thorn in EU data protectionists' sides from the beginning of negotiations on a cooperational agreement with the U.S. Whereas SWIFT I expressly allowed for bulk data to be provided to the UST,[165] the wording of SWIFT II neither bans nor approves mass data

[162] *DRI*, *supra* no.9, para.48.
[163] Dissenting: Tzanou, *supra* no.158, 209.
[164] *Schrems*, *supra* no.9, Opinion of AG Bot, para.193; *Weber*, *supra* no.143, paras.84ff., 94.
[165] Art.4 para.6 SWIFT I read as follows: 'If the Designated Provider is not able to identify and produce the specific data that would respond to the request because of technical reasons, all potentially relevant data shall be transmitted in bulk (…)'.

transfers. Although it has never been confirmed how many data are transferred on average, Europol's JSB observed that financial flows of entire countries are continually subject to the UST's requests. In light of the five year retention period, this practice of bulk transfers might amount to general data retention.

The Court's annulment of the General Data Retention Directive was interpreted differently, as to whether the verdict meant that any system of general data retention, irrespective of the safeguards provided, would violate arts.7 and 8 EUCFR.[166] The ruling in *Tele2 Sverige* spells out that indiscriminate (strategic) data collection and retention of commercial data for preventive purposes is in breach of the Charter. For the objective of crime prevention, only targeted data retention might concur with EU Fundamental Rights and must be limited to what is absolutely necessary regarding the data categories concerned, the means of communication included, the groups of persons affected and the length of retention, thereby establishing a certain link between the objective pursued and the data processed.[167] Art.4 paras.1 and 2 on first sight seem to adhere to these criteria by limiting the scope of the UST requests *inter alia* to specific geographic areas, time periods and data categories to be denominated. Nevertheless, these provisions might not lay down sufficiently clearly and precisely what exactly is to be understood by that and thus might not exclude general retention of all FIN data processed through SWIFT's network. Moreover, it is questionable if SWIFT II provides sufficient safeguards enabling the affected data subjects to protect their data efficiently.

Since the retention of SWIFT data will be examined as a separate interference with the rights under arts.7 and 8 EUCFR at a later stage, it only shall be stressed at this point that a retention period of five years considerably increases the amount of data stored in the black box. In fact, if financial data of a period of multiple years were analysed, they could reveal personality profiles more precisely than air travelling data retained for the same period (even if collected globally). The

[166] The Directive failed to comply with the Charter for its blanket nature; however, it was doubted whether the intention of the ruling was to allow for targeted data retention only: cf. Maria Helen Murphy, 'Algorithmic surveillance: the collection conundrum' (2017) Int'l RL, Computers & Techn 31, 225, 233f.
[167] *Tele2*, *supra* no.9, paras.108ff; confirmed in *PNR Canada*, *supra* no.10, paras.190ff.; with a critical stance on the judgement's restrictive approach: Iain Cameron, 'Balancing data protection and law enforcement needs: Tele2 Sverige and Watson' (2017) 54 CMLR 1467, 1481f.

following examination of affected data categories, persons and means of communication shall take this into consideration.

a. Data categories collected

Firstly, SWIFT II remains unclear as to which data categories are liable to processing by the UST. In the context of PNR data, the CJEU did not accept incomprehensive descriptions of data categories.[168] As elaborated above, art.5 para.7 does not list specific FIN message types but merely indicates the information which can be derived from requested FIN data in a non-exhaustive manner. The data categories this information is drawn from, however, are not identified in the agreement. Moreover, the range of personal information accessible to TFTP investigators is possibly much wider than art.5 para.7 suggests.[169] This lack of definition is neither remedied by art.1 para.1 also referring generally to 'financial transfers and related data', nor by art.6 para.2 obliging the UST to immediately delete non-requested data without clarifying which data can be rightfully requested in the first place.

Furthermore, SWIFT II does not establish any particular safeguards for sensitive data. In *PNR Canada*, the Court required an extraordinarily high level of justification for processing sensitive data in order to comply with arts.7, 8 and 21 EUCFR because of the inherent risk of stigmatisation of data subjects concerned.[170] However, it can be left unanswered here if the exclusive purpose of counter-terrorism could serve as a sufficient objective in this regard.[171] As art.5 para.7 states that sensitive data were highly unlikely to result from the requests, the TFTP's functioning evidently does not depend on the processing of sensitive information in any way. Still, it cannot be ruled out that sensitive information is contained in the SWIFT messages. From this perspective, it is difficult to see why the processing of sensitive data is not banned from the outset[172] or at least restricted after transfer by rigid masking or express deletion requirements. Against the background of (presumably) mostly Muslim countries being targeted by the UST requests,[173] any misuse of SWIFT data

[168] *PNR Canada*, *ibid*, para.160.
[169] For instance, 'sometimes even bills of lading': 2nd Joint Review Report, 38 (Annex IV).
[170] *PNR Canada*, *supra* no.10, paras.141, 164ff.
[171] *Ibid*, the Court dissented: 'Having regard to the risk of data being processed contrary to Article 21 of the Charter, a transfer of sensitive data requires […] grounds other than the protection of public security against terrorism and serious transnational crime'.
[172] By analogy for the Umbrella-Agreement: EDPS, Opinion 1/2016, <https://edps.europa.eu/sites/edp/files/publication/16-02-12_eu-us_umbrella_agreement_en.pdf> accessed 06 July 2018, para.36 with further references.
[173] Wesseling (2013), *supra* no.12, 168.

for ‘religious’ or ‘ethnic profiling’ should be prevented by appropriate safeguards in order to comply with the principle of non-discrimination. On the contrary, art.5 para.7 treats sensitive data equally to other SWIFT data, thereby violating arts.7 and 8 EUCFR and art.21 EUCFR respectively.

These shortcomings are best demonstrated with regard to information potentially derived from reference information: Whilst art.5 para.7 does not mention this data category at all, it is suggested here that the transaction’s reference is the most likely to contain sensitive data since it gives away the transaction’s purpose, for example a donation to a sectarian charity. In the aftermath of 9/11, Muslim charities were under particular focus of U.S. counter-terrorism investigations.[174] In that regard, it can be assumed that the agreement’s wording is misleading to say the least, when emphasising that sensitive data is extracted only in exceptional circumstances.[175]

A similar argument can be made for the absence of protection for data subject to professional secrecy. Although personal data concerning the work of journalists or the privileged relationship between client and attorney do not fall under the definition of sensitive data,[176] they require no less rigid safeguards in order to protect the rights enshrined under art.11 EUCFR.[177] It is not improbable that such data could be derived from trans-border transactions in course of international mandates or journalistic investigations. Nevertheless, the agreement remains tacit as to the processing of those data categories, let alone as to the specific safeguards applicable.

Whilst terrorist financiers most probably disguise their transfers’ purposes, innocent account holders could protect their sensitive information more efficiently if they were aware of the full range of data collected by the UST or if processing of sensitive and similar data was interdicted generally. Conclusively, the agreement neither lays down sufficiently clear and precise rules on the data categories processed nor

[174] See: Marieke de Goede, *Speculative Security: The Politics of Pursuing Terrorist Monies* (University of Minnesota Press 2012), 125ff.
[175] The UST Representations called it ‘highly unusual for SWIFT records to include sensitive data’.
[176] Cf. art.10 Directive (EU) 2016/680 on special categories of personal data.
[177] *DRI*, *supra* no.9, paras.56ff. where the question of professional secrecy is elaborated with regard to the groups of persons affected by data collection.

minimum safeguards for the processing of particularly sensitive categories of personal data.

b. Persons and providers affected

Secondly, suggesting a character of general rather than targeted data retention, the number of affected data subjects is supposedly extraordinarily high. According to art.4, UST requests are supposed to identify certain geographic areas and time periods associated to terrorist activity. It can be doubted, however, whether the risk analyses the requests are based on establish a sufficient link between the persons affected and the TFTP's objective. As observed by Europol's JSB, the production orders' broadness indicates otherwise.

However, the Court's notion of 'targeted data retention' should not be equated with the requirement of an individualised suspicion necessary to take data into storage in the first place:[178] The existence of an indirect link is a satisfactory threshold; this link can be of geographical or temporal nature.[179] The *PNR Canada* opinion confirmed that an initial mass retention of data on probably unsuspicious persons does not constitute an *a priori* violation of the Charter if otherwise the identification of unknown security risks through techniques of automated analysis would be rendered impossible.[180] It is exactly the TFTP's purpose to detect new terrorism suspects by sophisticated processing of data stemming from regions associated with an increased terrorism risk. Thus far, the acquisition and storage of financial data concerning entire countries matches the Court's criterion of targeted data retention.

Furthermore, the data requested by the UST represent a mere small fraction of the total amount of SWIFT messages generated in SWIFT's European processing zone. The fact that SWIFT's FIN network provides a messaging service for trans-border money flows, whilst inner-national transfers are communicated through domestic clearing houses, leads to the exclusion of most everyday transactions as they are

[178] For instance Alexander Roßnagel, 'Neue Maßstäbe für den Datenschutz in Europa aus dem EuGH-Urteil zur Vorratsdatenspeicherung' (2014) MMR 372, 375f. concluded that only 'quick freeze' could be compliant with the Court's understanding of lawful data retention.
[179] *Tele2*, *supra* no.9, 108ff; Aqilah Sandhu, ‚Anmerkung zum Urteil des EuGH vom 21.12.2016 in der Rs. C-203/15 (Tele2)' (2017) 52 Europarecht 453, 462f., points out that the threshold of individual/reasonable suspicion can only apply at the second stage of processing for purposes of consulting the data retained.
[180] *PNR Canada*, *supra* no.10, paras.187, 196.

(generally speaking) unlikely to require cross-border remittances. A major percentage of those transfers is furthermore excluded by art.4 para.2 lit.d prohibiting the UST to seek SEPA data (also communicated in SWIFT FIN standard). Persons making payments in Euro are not liable to data collection,[181] thus protecting a considerabe number of cross-border travellers, entrepreneurs and employees.

Consequently, the data collection under SWIFT II seems hardly comparable with measures envisaged under the former Data Retention Directive which basically subjected the entire European population to communications surveillance.[182] This is confirmed by the fact that, apart from SWIFT-generated data, no other financial communication service is targeted by the agreement. Irrespective of SWIFT's factual monopoly regarding trans-border interbank financial transfer messages, alternative and growing services, for example in the e-money business (PayPal), are not data sources for the TFTP.

Hence, it is arguable that SWIFT II is sufficiently precise and clear regarding the means of communication and persons affected by enumerating designated providers and limiting the data of interest to geographic areas associated with a certain level of terrorist threat. Nonetheless, the Court asks for sufficient safeguards ensuring the efficient protection of data subjects and preventing the abuse of power. Here, the agreement's mandate to Europol to conduct oversight on the requests appears to have several weaknesses in breach of art.8 para.3 EUCFR.

c. Europol approval: a sufficient safeguard against abuse of power?

The European Courts show a clear preference for judicial control of governmental access to personal data;[183] however, neither the ECtHR nor the CJEU insist on prior authorisation by a judicial authority under all circumstances. Whilst the Strasbourg Court in its latest decision requires a court approval ahead of data transfers to other countries,[184] the CJEU did not apply this hurdle to PNR-transfers to Canada which are neither authorised by a judge nor another supervisory body.[185]

[181] As the implementation of the SEPA-standard across Europe took considerably longer than expected when SWIFT II had been adopted, the TFTP could request inner-european payments until 2016: cf. Ambrock, *supra* no.35, 74.
[182] *DRI*, *supra* no.9, para.56.
[183] As to the ECtHR: Murphy, *supra* no.166, 231f.
[184] *Szabó*, *supra* no.143, paras.77ff.
[185] Cf. *PNR Canada*, *supra* no.10, para.193.

In context of SWIFT II, however, the Parties apparently saw the necessity of an *ex ante* oversight mechanism[186] which consequently must meet the requirements established in European case law:[187] Irrespective of the (non-)judicial character of the authority, any supervisory body must provide sufficient independence, impartiality and proper procedure. Europol's clear interest in smooth cooperation with the UST under the agreement[188] is difficult to reconcile with the need of impartiality: according to art.10, Europol can request the conduct of TFTP searches on its own behalf and has done so in multiple cases since SWIFT II's entry into force in summer 2010.[189] Apprehensions were confirmed when the former JSB observed that not a single UST request was rejected by Europol despite the subpoenas' level of abstraction hampering any assessment against the criteria set out in art.4 para.1 and 2.

Apart from Europol's overly tolerant attitude towards this abstraction, its purely operational assessment of the requests, irrespective of their legal compliance with the agreement, casts further doubt on the effectiveness of the procedure. If Europol is deemed to be fulfilling the mandate under art.8 para.3 EUCFR, it is primarily tasked to safeguard the legal requirements emanating from art.8 paras.1 and 2 EUCFR.[190] ECtHR case law on secret surveillance measures affirms that for purposes of prior or subsequent oversight, the authority's scope of review must comprise the factual and legal aspects of the respective operation.[191] An operational assessment might serve as an additional layer of control, however, it cannot replace legal scrutiny altogether. The abstract character of non-individual requests cannot lead to the conclusion that effective judicial or administrative oversight is superfluous; on the contrary, if the high level of abstraction hampers supervision, the requests must be rejected.

---

[186] The *ex ante* approval by an EU institution was urged by MEPs after rejection of SWIFT I; however, under art.4 paras.3-5 SWIFT I, an authority of the Member States hosting SWIFT's headquarter and its European server (Netherlands and Belgium) would have been charged with the provision of SWIFT data on the basis of MLA Agreements, thereby in fact conducting an assessment under national data protection law.
[187] *PNR Canada*, *supra* no.10, paras.228f. and *Schrems*, *supra* no.9, para.41 referring to C-288/12 *Commission v. Hungary* [2014] ECLI:EU:C:2014:237, para.48 and C-518/07 *Commission v. Germany* [2010] ECLI:EU:C:2010:125, para.25; *Zakharov*, *supra* no.143, para.258, 275; *Szabó*, *supra* no.139 para.77, 80.
[188] Cf. EDPS, *supra* no.41.
[189] For instance, according to the 4th Joint Review Report, Europol initiated 74 requests on own behalf and transmitted 120 Member States requests during the review period 2014/2015: *supra* no.54, 7.
[190] *PNR Canada*, *supra* no.9, para.228.
[191] *Zakharov*, *supra* no.143, paras.260ff.

d. Limited ex-post legal scrutiny

Europol's failure in interpreting the standard of oversight laid down in art.4 paras.1-4 is hardly remedied by further provisions of the agreement: the production order itself and its binding legal effect (remarkably, under EU and U.S. law) can be challenged by SWIFT only and exclusively before U.S. courts; against administrative subpoenas, however, the review is limited to the question of reasonability[192] irrespective of the requirements stipulated in the agreement.

Theoretically, Europol's approval decision is subject to administrative and judicial review, art.18 para.2 providing 'any person who considers his or her data to have been processed in breach of the agreement [with the right to] effective […] redress […] in accordance with the laws of the European Union, its Member States and the United States, respectively'. As to administrative redress, the new 2016 Europol Directive mandates the EDPS with handling individual complaints concerning alleged data protection breaches of Europol (art.47 and art.43 para.2 lit.a thereof). As opposed to the former JSB, the EDPS is vested with the authority to interdict any acts of data processing in contradiction of the Regulation and other EU data protection rules (art.43 para.2 lit.c, para.3 lit.f) and with the right to escalate a case to the CJEU (art.43 para.3 lit.h). However, since 1 May 2017 (when the Regulation became effective) the EDPS apparently has not raised the issue of Europol's approval practice despite the JSB's previous reports.[193] Whilst the new Europol Regulation thus could fill the gap of administrative redress on European behalf, the practice to be established by the EDPS in overseeing Europol will demonstrate whether the Regulation can serve as a sufficient safeguard for the purposes of SWIFT II.

As to judicial redress, every act of an EU agency can be challenged before the CJEU according to art.263 paras.1 and 4 TFEU.[194] However, it cannot be predicted if the Court could finally provide effective protection to the data subjects due to the UST's lack of consent to disclosure:[195] The so-called principle of originator's control would most probably prevent Europol from disclosing the documents substantiating

[192] Bignami, *supra* no.136, 16.
[193] EDPS, *Annual Report 2017* (2018) <https://edps.europa.eu/sites/edp/files/publication/18-03-15_annual_report_2017_en.pdf> accessed 22 June 2018, 22ff.
[194] The question of admissibility will be elaborated in the concluding chapter.
[195] This happened before when the UST refused consenting to disclosure of the JSB reports: *supra* no.44.

the requests. As a rigid principle of European law and a core value of Europol,[196] the principle of originator's control hardly allows any balancing with the individual rights in question; as a result, the Court possibly would lack the factual basis[197] to assess Europol's approval against the criteria described above. Without having a say on the classification of documents by the UST in the first place, however, it is difficult to see how Europol could be held responsible for adhering to its confidentiality obligations under the Europol Regulation.[198]

In light of these considerations, it is a major flaw of SWIFT II not to provide for an EU mechanism for individual redress,[199] leaving the agreement with insufficient safeguards for the protection of data subjects from UST data requests incompatible with the limitations set out in art.4 paras.1 and 2.

2. Data retention in the black box

Whilst the bulk transfer of financial messaging data from SWIFT to the UST thus can qualify as a measure of targeted data retention which does not *a priori* violate arts.7 and 8 EUCFR, SWIFT II 's data retention period of five years is a considerable long time and might lead to a very precise picture of a person's personal life and how it has changed. In several reviews, the UST repeatedly took the position that the retention cannot be shortened generally because 35-45 percent of the data identified as crucial for their investigations had been retained for three years or longer.[200]

a. Five years of retention: five years of suspicion

In *Digital Rights Ireland*, the Court found a maximum retention of three years incompatible with arts.7 and 8 EUCFR stressing that the length of retention must result from objective criteria.[201] According to the Court's reasoning in *Tele2 Sverige*

---

[196] Artur Gruszczak, *Intelligence Security in the European Union* (Palgrave Macmillan 2016), 256f.; the principle of originator's control is enshrined in art.19 paras.1 and 2 Europol-Regulation; the handling of EU-restricted documents is regulated on the basis of art.67 para.2.
[197] For this and the previous: V. Abazi, 'The future of Europol's parliamentary oversight: a great leap forward?' (2014) 15 German LJ 1121, 1123, 1126ff. with further references.
[198] The Venice Commission, Report on the Democratic Oversight of Signals Intelligence Agencies (CDL-AD(2015)011), paras.13, 125 therefore suggests that this principle should not apply to oversight bodies generally.
[199] Bloch-Wehba, *supra* no.114, 623.
[200] TFTP Value Report, *supra* no.52, 11ff.
[201] *DRI*, *supra* no,9, para.65.

and reaffirmed in its opinion on the *PNR Canada* Agreement,[202] the provisions on the retention period have to be clear and precise, establishing a certain link to the objective pursued. However, the mere average lifespan of international [terrorist] networks and the complexity of investigations cannot serve as an objective criterion demonstrating a sufficient link between data of generally unsuspicious persons and the purpose of combatting terrorism.[203] Hence, the argument that a considerable amount of long-term stored data has proven useful for the TFTP's operation cannot *per se* justify the five year retention period. In particular, the retention period must mirror the usefulness of the respective data categories for the investigative purposes[204] and generally differentiate between suspicious and unsuspicious persons.[205]

The retention under the TFTP scheme does not vary as to different data categories which are equally stored for five years irrespective of their average exploitability for the investigations. Whilst it shall not be guessed here what data categories might be dispensable before the five year period expires, any partial deletion from or masking of the datasets would supposedly contradict the UST's interpretation of the strict integrity requirements set out in art.5 para.4 prohibiting any alteration or manipulation of data. For this reason, the UST refuses to delete erroneous data despite art.17 para.1 expressly referring to 'supplementation, deletion or correction' in order to maintain the accuracy of the data received. Although the Court repeatedly pointed out the importance of safeguards on data integrity and confidentiality,[206] those provisions however primarily aim at preventing any misuse of data and thereby can hardly serve as an objective criterion in order to extend the retention period of data categories which are no longer of use for counter-terrorism investigations; this would result in the paradoxical outcome of data being exposed to an even greater risk of misuse.

For the five years of storage, SWIFT data transferred to the UST are maintained in a general status of suspicion unless extracted from the black box. It becomes clear from the Court's case law that for ongoing storage, the 'Agreement must continue

[202] *Tele2*, *supra* no.9, para.188; *PNR Canada*, *supra* no.10, paras.191, 209 which accepted a five year period for data of persons who were found suspicious after initial data analysis or evidence collected until departure.
[203] *PNR Canada*, *ibid*, para.205.
[204] *DRI*, *supra* no.9, para.65.
[205] *PNR Canada*, *supra* no.10, paras.204ff.
[206] *DRI*, *supra* no.9, para.66; *Tele2*, *supra* no.9, para.122

to satisfy the objective criteria which established the connection between the personal data to be retained and the purpose pursued'.[207] Consequently, an ongoing threat assessment with regards to data categories, geographic area and time period equivalent to the initial assessment as laid down in art.4 paras.1 and 2 is required. Theoretically, this is exactly what is supposed to happen under art.6 para.1 stating that 'the U.S. Treasury Department shall undertake an ongoing and at least annual evaluation to identify non-extracted data that are no longer necessary to combat terrorism or its financing'. In fact, however, the UST does not delete any data before the retention period expires due to technical obstacles. The CJEU stressed that all technical and organisational measures have to be taken in order to reduce the risks of data misuse irrespective of economic interests.[208] This argument can be applied here by analogy as, eventually, it is cost-intensity caused by the complexity of the database hampering the UST from deleting unnecessary data. In this regard, art.6 para.1 leaves too much discretion to the executive when obliging the UST to delete 'as soon as technologically feasible'.

Even if the deletion indeed proved technically undoable (which should provoke the question if data should be retained in the black box at all), the UST is apparently capable of at least flagging erroneous datasets in order to prevent them from further usage. It is difficult to understand why this should not apply to data understood as being no longer necessary for counter-terrorism purposes. Apparently, despite the existence of direct EU oversight according to art.12 and repeated reviews under art.13, this weakness in the retention scheme has not been tackled so far.

To sum up, the retention period is not based on objective criteria and the agreement lacks suffiently clear rules as to the UST's obligation to delete data which are deemed as no longer necessary for the achievement of the TFTP's objectives.

b. No individual rights for ex ante unsuspicious persons

Due to the UST's restrictive interpretation of SWIFT II, enforcing individual rights is not possible before personal data are extracted from the black box. Paradoxically,

[207] *PNR Canada*, *supra* no.10, para.191.
[208] *DRI*, *supra* no.9, para.67; in this regard, the Court's reasoning goes beyond the standard established by Directive (EU) 2016/680 which obliges the controller to implement technical and organisational measures with due (but not exclusive) regard to the costs coming with it (recital 53 thereof).

data subjects cannot rely on their individual rights to access, deletion, rectification, blocking or redress in order to have their datasets erased from the black box or otherwise prevented from processing in the first place.

Whilst the Joint Review Group has accepted this practice so far, it is at odds with the CJEU's longstanding case law. As the Court had pointed out as early as 2009, the right to privacy 'means that the data subject may be certain that his personal data are processed in a correct and lawful manner, that is to say, in particular, that the basic data regarding him are accurate'.[209] Consequently, access (and consecutive rights) must generally be provided at any stage of data processing in order to prevent the authorities relying on incorrect or unnecessary data. Moreover, limiting individual rights to extracted data is not compliant with SWIFT II's clear intention to enhance the rights of individual data subjects. This is mirrored in the preamble, emphasising effective protection of privacy and personal data,[210] as well as in the existence of a right to rectification or deletion which is practically rendered invalid if incorrect or unnecessary data had to be extracted and analysed beforehand. The UST's interpretation (based on art.5 paras.2, 4 lit.c, 5 and 6) reducing access to counter-terrorism investigations demonstrates incoherent rules and safeguards governing the access to the black box or the UST's lack of commitment to fundamental rights protection. Either alternative constitutes a violation of arts.7 and 8 EUCFR.

c. Retention of extracted data

Regarding extracted data, it was observed in chapter 1 that the agreement remains indefinite as to the handling of information on data subjects who were relieved of the general suspicion of terrorist activity. In its *PNR Canada* opinion, the CJEU stressed that a long-term storage of data concerning persons who were not identified as being potential suspects after an initial data analysis violates arts.7 and 8 EUCFR.[211] In case of PNR data, the datasets transferred to third country border control agencies are profiled automatically at the time of arrival and departure. Therefore, the Court considers any retention beyond this point in breach of the Charter if the data were not responsive to the profiling algorithms. In specific cases,

[209] Case C-553/07 *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer* (2009) ECLI:EU:C:2009:293, para.49.
[210] Recitals 6, 7, 8, 13, 14 and 16.
[211] *PNR Canada*, *supra* no.10, paras.204ff.; similar: ECtHR, *supra* no.143, in *S. and Marper*, paras.122ff., and *M.K.*, para.39.

however, when objective evidence suggests that certain air passengers may pose a further security risk, storage and use of their data beyond departure are permissible if based on objective criteria (supposedly: reasonable suspicion) and if subsequent access is subject to prior approval by a judicial or independent administrative body following a reasoned request on behalf of the investigating authority.[212]

It stands to reason to draw an analogy to the extraction and analysis of SWIFT data for the detection of so far unknown terrorist associates. Whilst the TFTP's approach is based on a different technology of analysis, the extraction process serves the same objective, namely to either confirm or refute a potential terrorism nexus. As soon as no link could be confirmed, the data subjects concerned cannot be treated equally to persons who are proven to have a terrorism nexus or persons whose data has not yet undergone analysis. The mere possibility that a terrorism nexus might be revealed in other contexts cannot serve as an argument to keep their financial data retained in the black box as if they have not been queried at all. Against the background of the UST's refusal to delete any data before expiry of the retention period, datasets concerned could (at least) be flagged to signal their status of minor suspicion. Without referring to the handling of data of *ex post* unsuspicious persons at any point, however, art.6 para.7 does not lay down sufficiently clear and precise rules and appropriate safeguards when it comes to retention of extracted data.

d. Data extracted, individual rights derogated?

As much as the agreement's provisions on individual rights fail to achieve any protection for 'unsuspicious' data subjects, they prove inefficient in practice when it comes to persons whose data are extracted from the black box. This is mostly due to deficiencies in the right to access enshrined in art.15. As the CJEU held in its *PNR Canada* opinion, rules must be laid down in a clear and precise manner on the substantial and procedural requirements of the access, including the nature of information that may be disclosed, the persons to whom such disclosure may be made and if the disclosure is subject to prior authorisation of a court or an administrative body. Furthermore, any derogation from the right to access must be limited to what is strictly necessary by clearly defining the legitimate objectives which can serve as justification for the denial of disclosure. [213]

[212] *PNR Canada*, *ibid*, paras.207f.
[213] For this and the previous: *Ibid*, paras.216f.

Whilst access under art.15 theoretically implies 'disclosure of personal data' (para.2), it can be assumed that data subjects are merely provided with a 'confirmation that their rights have been respected' in course of TFTP data processing (para.1). In the latter case, however, data subjects cannot derive if their data were transferred to the black box nor if data were accessed at all. Resulting from paras.2 and 3, access to datasets can be (partly) restricted or (entirely) refused for 'reasonable' grounds under national law. Without enumerating the corresponding limitations applicable under U.S. law, para.2 solely refers to the safeguarding of the prevention, detection, investigation or prosecution of criminal offences, public security and national security. Apart from the low threshold of reasonableness and the broad understanding of the notion of national security in the U.S.,[214] the general reference to 'criminal offences' is at odds with the TFTP's limited purpose of counter-terrorism. Even if interpreted narrowly as including only the prevention, detection, investigation or prosecution of terrorism and terrorist financing, the U.S. definition of terrorism is much wider than the definition found in art.2 SWIFT II. It was exactly this divergence that prompted EU negotiators to insist on a narrower definition of terrorism and terrorism financing as found in Council Framework Decision 2002/475/JHA and the 3rd EU Anti-Money-Laundering Directive.[215] Against this background, the objectives allowing for derogations from the right to access are not clearly defined.[216]

Moreover, according to the UST Representations, data extracted from the black box is understood to be directly linked to a terrorism suspect. Hence, the mere extraction is sufficient to justify any limitation of access under art.45 para.2. Although every restriction or refusal has to be explained in writing (para.3), it can be ruled out that this information gives away any indication as to the circumstances of the extraction in order not to undermine the derogation altogether.[217] Without

[214] By analogy for the Umbrella-Agreement: Douwe Korff, 'EU-US Umbrella Data Protection Agreement: Detailed analysis by Douwe Korff' (14 October 2015) <https://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/> accessed 21 November 2017, at II.iv.
[215] Council Framework Decision of 13 June 2002 on combating terrorism (2002) OJ L164/3; Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (2005) OJ L309/15.
[216] See, by analogy, Opinion of AG Bot in *Schrems*, *supra* no.9, paras.162ff.; Korff, *supra* no.214, at II.iii.
[217] See the UST's response to Cristina Blasi Casagran, 'Global Data Protection in the Field of Law Enforcement' (Routledge 2016), 99 who was neither confirmed nor denied of the existence of any responsive records because 'the disclosure of such information could identify subjects of ongoing counter-terrorism investigations or harm national security'.

disclosure of the data extracted, however, the right to access finally loses its function as 'door opener' for other individual rights, namely the right to rectification, erasure and blocking. As stated in art.16 para.2, any application for rectification, erasure or blocking shall be duly substantiated. The respective UST guidelines impose an extraordinarily high threshold,[218] in fact rendering any application inadmissible without prior knowledge of the exact datasets.

Nevertheless, access, rectification, erasure and blocking are not placed under sufficient oversight mechanisms: the on-site EU scrutineers (art.12) are not mandated to supervise the UST's concurrence with arts.15 and 16. The Joint Reviews under art.13 so far only focussed on the identification procedure for data subjects applying for access, deletion or rectification and on the provision of further information on the UST's website with regard to the limits of rectification of data.[219] The national data protection authorities mentioned in arts.15 and 16 merely act as postmen, transmitting the applicants' documents to the UST, helping to translate and to verify their identity.[220] Thus, the assessment of the requests is solely handled by the UST's Privacy Officer whose decision is subject to administrative redess under APA, FOIA and USPA.

However, these redress mechanisms cannot sufficiently remedy the shortcomings either. Whilst the right to deletion of unlawfully processed records is not provided for, access and amendment lawsuits require a detailed description of the records concerned.[221] Furthermore, under the USPA, non-EU citizens and residents are still excluded from personal scope; for instance, Syrian refugees[222] who are particularly prone to be affected by the TFTP requests and searches. Generally, however, it must be observed that access and rectification can be excluded altogether or the burden of proof shifted to the claimant due to far reaching exemptions and privileges granted to U.S. law enforcement and security agencies (applicable to the UST).[223] From a CJEU-perspective, this is not satisfactory: effective remedy must be

[218] *Supra* no.127.
[219] 2nd Joint Review Report, *supra* no.48, 11f.; 3rd Joint Review Report, *supra* no.51, 17ff.; 4th Joint Review Report, *supra* no.54, 16ff.
[220] Letter to LIBE, *supra* no.7, 5.
[221] FOIA: 5 U.S.C. 552 (3) (A), (B); for USPA see U.S. Department of Justice <https://www.justice.gov/opcl/civil-remedies> accessed 07 June 2018.
[222] Korff, *supra* no.214, at II.ii.
[223] FOIA: 5 U.S.C. 552 (b); USPA: 5 U.S.C. 552a (j) and (k).

available to any person irrespective of citizenship as neither arts.7 and 8 EUCFR nor art.47 EUCFR are limited in personal scope.[224]

Furthermore, leaving the data subject with the burden of providing evidence that his or her data is processed by the UST without any hold against the agency conflicts with the CJEU's understanding that every person has a right to notification. If individuals were informed of the extraction of their personal data, they could seek judicial redress more easily. With this argument, the ECtHR considers the right to notification dispensable only if access to judicial redress is not dependent on the possession of the facts proving or concretely suggesting that the claimant has been subjected to secret surveillance.[225] The CJEU goes even further and asks for a general right to notification. It held that mere transparency clauses obliging the data controller to make available general information on the respective programme by publication of FAQs on government websites was not sufficient to ensure that every person affected can eventually exercise his or her rights to access, rectification and redress in order to prevent or remedy data misuse. However, the Court acknowledges the risk of jeopardising the investigations carried out by the authorities and accepts a pending of notification as long as (absolutely) necessary for the achievement of this objective.[226] Although this allows for a considerable number of derogations, the threshold of necessity is much stricter than mere reasonableness[227] (as found in art.15 para.2 of the agreement restricting the right of access). SWIFT II, however, does not provide for a right to notification at any point of data processing.

To sum up, the agreement falls short of providing efficient individual rights to the data subjects affected.

3. Extraction from the black box and analysis

As observed in chapter 1, the extraction process from the black box is not clearly portrayed in the agreement and still remains opaque today. The discretion granted to the UST for this stage of processing of SWIFT data is at odds with the Court's general considerations on clarity and precision of the legal basis concerned. It will

[224] cf. *PNR Canada*, *supra* no.10, 226f.
[225] *Zakharov*, *supra* no.143, paras.234, 290ff.
[226] *PNR Canada*, *supra* no.10, para.218; *Tele2*, *supra* no.9, para.121.
[227] Korff, *supra* no.214, as to the rights of access, administrative and judicial redress under the Umbrella-Agreement.

be argued that the existent rules on TFTP investigators' access to the black box neither determine the occasions of data usage by the UST in a foreseeable manner nor impose efficient safeguards against abuse. Whilst the analysis focusses on art.5 para.6, the Court's findings on profiling algorithms are briefly discussed afterwards with regard to SWIFT II's ban on automated processing.

a. Rules governing the access to the black box

According to the Court, the use of retained personal data must continue to satisfy objective criteria establishing a link to the purpose pursued.[228] Substantially, access should be limited to data of persons who are under reasonable suspicion of criminal conduct. Only for national security purposes, access to data of unsuspicious persons can be justified if it is likely that the information derived might contribute substantially to the success of investigations.[229] From a procedural perspective, any access requires prior approval by a court or independent administrative body following a reasoned request substantiated by sufficient evidence,[230] except for cases of urgency when an *ex post* approval is inevitable.[231]

Substantially, art.5 para.6 stipulating that each individual search 'shall be narrowly tailored, shall demonstrate a reason to believe that the subject of the search has a nexus to terrorism or its financing' does not meet these requirements. Albeit every search is conducted on a name or bank account believed to be associated with terrorist activity, the vast majority of data subjects whose data are extracted from the black box are perfectly innocent. Yet under the assumption that TFTP-searches pursue the objective of national security, the level of suspicion with regard to the names or bank accounts run against the database and the information provided in order to substantiate the terrorism-nexus certainly do not amount to reasonable suspicion of terrorist activity. Even if the CJEU might accept a lower threshold,[232] art.5 para.6 neither defines whether 'a reason to believe' is to be based on a legal or an operational assessment nor does the agreement provide any further

[228] *Tele2*, *supra* no.9, para.119; *PNR Canada*, *supra* no.10, paras.190ff.
[229] *Tele2*, *ibid*; the notion of national security is somewhat ambiguous in EU primary law – according to the CJEU's case law on public security derogations from market freedoms, however, the term's meaning is far narrower than under U.S. law (see E.II).
[230] *PNR Canada*, *supra* no.10, paras. 200ff.
[231] *Tele2*, *supra* no.9, para.120.
[232] The ECtHR apparently did when it coined the notion of 'individual suspicion': *Szabó and Vissy*, *supra* no.143, para.71.

explanation; generally, the wording suggests a very low standard.[233] Neither can it be derived what is to constitute a nexus to terrorism[234] and if a mere remote, purely indirect nexus (for example: geographic proximity) is sufficient to run a search on the concerned person. Evidently, a terrorism nexus does not necessarily amount to terrorist activity as defined in art.2. In combination with the low standard of suspicion, art.5 para.6 is hardly suitable to narrow down the searches efficiently.
The absence of a Human Rights clause aggravates these findings: the UST's alleged practice of taking information from U.S. security lists is not mirrored in the wording of the agreement. Here, the prohibition of reliance on any names or supplementary information gathered under severe violation of human rights, especially under deployment of torture, could prevent the perpetuation of those infringements. *Vice versa*, the agreement lacks a necessary safeguard prohibiting the further use of TFTP-derived data for purposes in breach of essential human rights standards, especially extrajudicial detention. [235]

As to procedural safeguards, the on-site oversight according to art.12 does not amount to a general *ex ante* approval of all the searches run in the black box, nor is it entirely clear if it is conducted on legal or operational criteria due to the opacity of the access requirements stemming from art.5 paras.5 and 6. Bearing in mind the potentially high number of false-positives resulting from a search in conformity with the criteria set out in art.5 paras.5 and 6, an *a priori* review of the search requests however seems inevitable in order to prevent any chance of an inappropriate search. This *ex ante* approval might not necessarily require a court warrant but must be based on legal criteria and has to be conducted by an independent (administrative) body. Supposedly, qualification and seniority of EU overseers is similar to the Eminent Person who was appointed to oversee the UST's compliance with the Representations, that is to say judges or lawyers with a special background in counter-terrorism. However, this assumption cannot be derived from the agreement's wording; since they team-up with the so-called SWIFT scrutineers whose background is not known at all, the agreement does not require an assessment comparable to judicial approval.

[233] Michael Palmisano, 'The Surveillance Cold War: Recent Decisions of the European Court of Human Rights and their Application to Mass Surveillance in the United States and Russia' (2017) 20 Gouzaga JInt'l L 75, 81.
[234]Amicelle, *supra* no.69, 21.
[235] For the whole paragraph, by analogy: Korff, *supra* no.214, at II.ii.

Consequently, arts.5 and 12 do not provide sufficient substantial and procedural safeguards ensuring the use of SWIFT data is compliant with arts.7 and 8 EUCFR.

b. Extraction and analysis of SWIFT networks

With its deliberations on automated processing, the *PNR Canada* opinion breaks legal ground beyond the well-established guarantee that no adverse decision shall be taken on the basis of automated data analysis only. Whilst the Court accepts the need for a computer-based analysis of mass data, it requires sufficient safeguards hedging the increased risks coming with automated analysis. Since the interference with arts.7 and 8 EUCFR essentially depends on the algorithms applied, the pre-established models and criteria should be specific, reliable and non-discriminatory, eventually arriving at results amounting to reasonable suspicion. Data-bases used for cross-checking, on the other hand, should serve the same objectives as the automated data analysis and provide high reliability and up-to-date information. Here, the Court tolerates soft-oversight mechanisms in the course of joint reviews.[236]

It cannot be answered here if the technique of link analysis deployed by the TFTP and the external databases consulted therefore satisfy these requirements. In light of the findings of chapter 1, however, the agreement's ban on automated processing in art.5 para.3 is at odds with the Court's general considerations on legal clarity and instead should comprise a clause prohibiting the UST, or any other authority provided with TFTP-derived data, from taking any decision affecting the person concerned solely on the basis of automated analysis. Furthermore, art.13 apparently excludes the methods of analysis applied by the TFTP from the Joint Review and thereby leaves it to the exclusive discretion of the UST if the number of links constituting a network, the algorithms applied in order to qualify the network and the databases consulted are appropriate to the common objective pursued. Thereby, it clearly fails to comply with the requirements set forth by the Court.

4. Dissemination of leads

As acknowledged by the ECtHR lately, data sharing is a useful tool for purposes of international cooperation in combatting terrorism.[237] This is mirrored in SWIFT II's

[236] *PNR Canada*, *supra* no.10, paras.168ff.
[237] *Szabó*, *supra* no.143, para.78.

provisions on reciprocity and onward transfer. Whilst it already has been pointed out in chapter 1 that the agreement does not specify whether the information, leads and reports disseminated contain raw SWIFT data, extracted networks, mere names or threat analyses on identified terrorism suspects, the safeguards provided for data sharing miss the high standards stipulated by the CJEU:

The Court clearly identifies the loss of control on personal data as being the major risk of data sharing with third parties. In order to ensure minimal safeguards for data that is disclosed to third country authorities, an adequate level of data protection must be ensured. This either requires an adequacy decision issued by the Commission or a specific agreement with the third country authority receiving the data. However, any discretionary power of the disseminating authority as to adequate protection and urgency procedures must be ruled out.[238]

As opposed to this case law, art.7 on onward transfers does not require the existence of an adequate level of protection offered by the third country to where the data is transferred; theoretically, the UST could share personal data with every authority mandated with counter-terrorism as it pleases, that is to say in particular with intelligence services of third countries. This is particularly problematic in light of the absence of a Human Rights clause.[239] The reservation of prior EU consent is limited to the case in which personal data of EU citizens or residents is involved, despite arts.7 and 8 CFR granting protection to every person when his or her personal SWIFT data is transferred from the EU to a third country. Moreover, in cases of immediate threat or existing protocols, consent is not required at all and the UST must merely notify the dissemination afterwards. Whilst the Court pointed out that notification must be provided to every data subject individually,[240] SWIFT II lacks a provision on notification altogether.

Remarkably, the UST has so far relied on existing protocols for all transfers to third countries.[241] However, it is not clear which protocols are referred to and if they establish similar safeguards as an EU-third country agreement on data sharing for law enforcement purposes; in fact, is is questionable if those protocols could

[238] *PNR Canada*, *supra* no.10, paras.213f.
[239] Korff, *supra* no.214, at II.i.
[240] *Supra* no.226.
[241] 2nd Joint Review Report, *supra* no.48, 23; 3rd Joint Review Report, *supra* no.51, 26; 4th Joint Review Report, *supra* no.54, 26.

constitute a legal basis in the understanding of the CJEU at all.[242] Furthermore, after the annulment of Safe Harbour and before the EU-U.S. Umbrella Agreement entered into force in 2017, it could not be assumed that other U.S. law enforcement agencies and counter terrorism authorities ensured adequacy either. When it comes to international organisations, it is entirely in the UST's discretion if those, for instance Interpol, ensure an adequate level of protection. Art.7 lit.e, requiring the UST to oblige the third party to delete the information as soon as no longer necessary for the purpose it was shared for, does not remedy these weaknesses because of the lack of enforcement capacities on behalf of the UST or the EU.

Turning to the reciprocity mechanism, it is questionable which rules exactly apply to the Member States' authorities, Eurojust and Europol requesting searches by the UST. Art.10 does not refer to art.5 paras.5 and 6; instead, the enumerated institutions shall 'determine' if there is a reason to believe that a person has a nexus to terrorism. The notions of reasonable belief and terrorism nexus might be interpreted differently from Member State to Member State as the agreement does not lay down sufficiently clearly what is meant therewith. Furthermore, when TFTP-derived information is shared with EU and Member States' institutions under arts.9 and 10, it will probably be shielded entirely from any legal or democratic oversight due to the UST's classification practice; thus, access is restricted despite the fact that, at least in case of art.10, potentially all data processed (including the raw SWIFT data and the information provided to substantiate the requests) originates from Europe.

To conclude, SWIFT II does not lay down sufficiently clear and precise rules regarding the data shared with EU and Member States' institutions nor does it establish efficient safeguards for ensuring an adequate level of protection when it comes to third country authorities.

III. No adequate level of data protection under SWIFT II

The above examination of the SWIFT II Agreement demonstrates the lack of adequate protection provided by the UST contrary to the adequacy statement of art.8. It has been shown that every stage of data processing displays severe deficiencies in the protection of privacy and personal data: (1) The transfer of SWIFT

[242] Korff, *supra* no.214, at II.iii.

data from European territory to the UST is not governed by clear and precise rules regarding the concerned data categories, lacks safeguards for sensitive data as well as data subject to professional secrecy and is neither placed under independent and efficient oversight. (2) The retention period for unextracted data is not based on objective criteria whilst the agreement fails to lay down sufficiently clear and precise rules on the retention and deletion of extracted data from the black box; furthermore, individual rights to access, rectification, deletion and redress are rendered ineffective by indefinite derogation clauses and overly restrictive interpretation on behalf of the UST. (3) As to the use of SWIFT data by the UST, the agreement does neither clearly define the threshold for accessing the black box nor does it impose sufficient restrictions and oversight on the analysis of the extracted data. (4) When it comes to the dissemination of TFTP-derived information, it is not clear exactly which personal data can be shared with third parties, nor is the disclosure accompanied with sufficient safeguards ensuring an adequate level of data protection. (5) SWIFT II finally does not comprise a right to notification of data subjects.

However, art.8 constitutes a *de facto* adequacy decision[243] with the consequence that neither SWIFT nor European Data Protection Authorities nor affected data subjects can refuse data transfer to the U.S. unless the decision is withdrawn or invalidated. As opposed to 'ordinary' adequacy decisions issued by the Commission (as in the *Schrems* case), the provision of art.8 contained in an international agreement is hardly impugnable for its legal superiority to EU secondary law.[244]

From that angle, it is remarkable that SWIFT II was cited as an example for extraterritorial application of EU law[245] and as 'an improvement' due to the Parliament's persistence.[246] In the cold light of day, the agreement rather appears to be a Pyrrhic victory, keeping the EU in a position of a 'norm taker' of U.S. interests.[247] If an EU TFTS would remedy that situation and how it could be designed to meet the requirements of CJEU case law shall be answered in the next chapter.

[243] By analogy: EP Legal Service, Legal Opinion on EU-US Umbrella agreement concerning the protection of personal data and cooperation between law enforcement authorities in the EU and the US, Doc.no. SJ-0784/15 (2016), paras.17ff.
[244] *Ibid*, 21ff.
[245] *Inter alia*: Yuko Suda, 'Transatlantic Politics of Data Transfer: Extraterritoriality, Counter-Extraterritoriality and Counter-Terrorism' (2013) 51 JCMS 772, 781.
[246] Rapporteur Alvaro in: LIBE, *supra* no.40.
[247] Very fiercly so: Kierkegaard, *supra* no.7; by analogy to the PNR Agreement: Javier Argomaniz, 'The Passenger Name Records Agreement and the European Union

Internalisation of U.S. Border Security Norms' (2009) 31 Journal of European Integration 119ff.

D. Chapter 3: SWIFT III – the EU TFTS coordination and analytical service?

Turning to a future EU TFTS, this chapter departs from the current agreement's provision on an 'equivalent EU system' intended to substitute bulk transfers with pre-filtered data subsets. On the basis of EU Commission preparatory publications, it will be shown that the EU again performed a U-turn, suddenly calling for a system complementary to SWIFT II. Even more ambitious than a substitutional scheme, the design of an EU TFTS running parallel to the SWIFT II cooperation must fit into the strengthened EU data protection framework of 2016. Although it does not seem inaccordable with the standards set out by the CJEU, both the U.S. and European data protection watchdogs will have strong reservations as to the scheme's compliance with their respective interests.

I. Art.11 SWIFT II as a manifestation of EU fundamental rights commitment

Together with the exclusion of SEPA-data from UST requests, art.11 of the current agreement was perceived as the major negotiation success on behalf of the Parliament.[248] It was the Parliamentarians' desire to replace the transmission of mass SWIFT data with a system allowing the extraction of individual datasets on European territory and to provide the UST therewith. Bulk transfers should remain only a preliminary but necessary evil until fundamental rights compliance could be restored in course of custom-building counter-terrorism capacities in the near future. [249] The U.S. committed to support and cooperate on an equivalent EU system (para.2) and the Commission was tasked to carry out a feasibility study as soon as possible (para.1). The outcome was however rather biased:

In a preliminary paper from 2011, models of hybrid EU and national cooperation were assessed as preferable policy options compared to fully centralised or fully decentralised systems. The reason was threefold: to run the system successfully, input of national intelligence was deemed essential; on the other hand, only a centralised European unit was assumed suitable both to effectively 'connect the dots' across inner-European borders and to secure a strict and uniform implementation of European data protection standards.[250] In the Commission's final communication from 2013, a so-called 'EU TFTS coordination and analytical service' was understood to be the most advantageous as well as highly centralised hybrid

[248] Marieke de Goede, 'The SWIFT Affair and the Global Politics of European Security' (2012) 50 JCMS 214, 224f.
[249] For this and the previous: Wesseling (2016), *supra* no.12, 11.
[250] For this and the previous: Commission, A European terrorist finance tracking system: available options COM(2011) 429 final, 4ff.

model.[251] In this scenario, a central TFTS unit at EU level, preferably situated at Europol, would be tasked with the collection, retention, extraction and analysis of SWIFT data. Member States could opt to either request searches to be run on their behalf or conduct their own searches in the database.[252]

Eventually, the Commission refrained from putting forward a legislative proposal. Compared to maintaining SWIFT II, they came to the conclusion that it was difficult to justify the added value of an EU TFTS. On the one hand, an EU TFTS would still provoke considerable fundamental rights challenges; on the other, any system was estimated as highly cost-intensive. Moreover, Member States' law enforcement agencies were increasingly making use on the reciprocity mechanism and apparently lost interest in substituting SWIFT II with a European system.[253]

II. From ambition to reality: The call for a 'genuine Security Union'

From 2015 on, numerous terrorist atrocities on European soil have urged the EU to 'do everything necessary to support the Member States in ensuring internal security and fighting terrorism'. [254] The Commission delivered an agenda for building up an 'effective and genuine Security Union' in line with the Stockholm and Post Stockholm Programme in order to enhance the internal security of the European Union and its Member States.[255]

In the Commission's counter-terrorism strategy, combatting terrorist financing continues to be a priority of which the EU-US TFTP mechanism forms an important part. After Charlie Hebdo in January 2015, EU requests under the reciprocity clause immediately doubled and kept rising.[256] Moreover, it transpired that on the eve of the assaults, most attackers were known to national law enforcement and intelligence agencies but neither their expenditures nor their movements across Europe came to light due to a lack of intelligence sharing.[257] The 'SEPA-gap' of

[251] 2013 TFTS Study, *supra* no.5, 19ff.
[252] For this and the previous: 2011 TFTS preliminary study, *supra* no.250, 9f.
[253] For the entire paragraph: 2013 TFTS Study,*supra* no.5, 34.
[254] European Council, *Bratislava Declaration* (16 September 2016) Decl. 517/16.
[255] Commission, European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union COM (2016) 230 final.
[256] *Supra* no.123.
[257] Cf. Commission, Roadmap: A possible European system complementing the existing EU-US TFTP agreement (2016) <http://ec.europa.eu/smart-regulation/roadmaps/docs/2016_home_191_system_complementing_tftp__en.pdf> accessed 07 June 2018.

SWIFT II apparently had turned into a security risk; after the Brussels bombings in March 2016, conservative MEPs supported the Commission's idea of a 'complementary' EU TFTS.[258] A reconsideration of available options was announced for December 2016. However, the goal was no longer to replace the current SWIFT II scheme but to run a parallel system on European financial messages.[259] The publication has been continually postponed. Irrespective of the outcome, the EU already has made another remarkable U-turn in the SWIFT-affair.

III. Main drivers for a complementary system

Notwithstanding the reassessment's objective of identifying available options, it can be assumed that the reasons for excluding purely national as well as purely centralised models are still valid. Moreover, among the hybrid options preferred in 2013,[260] a centralised unit tasked with requesting, collecting, searching and analysing the data promises exactly what has been missing on the European level so far, which is reliable information sharing. However, back in 2013, the Commission had already pointed out that the U.S. TFTP mechanism did 'not fully represent EU interests'.[261] There are four main drivers which continue to be decisive in tailoring a European-oriented system:

1. SEPA-data and other financial services

In the course of the analysis of the 2015 and 2016 attacks launched in Europe, planning and effectuating terrorist plots proved by no means as cost intensive as 9/11 had been; hardly any international money transfers of a significant amount were necessary beforehand.[262] Hence the main purpose of an EU TFTS will be the closure of the SEPA-gap arising from art.4 para.2 lit.d SWIFT II. As early as 2011, it was considered reaching beyond SWIFT and including other European financial services into the list of designated providers.[263] Since SWIFT communications in SEPA standard amount only to a small percentage of all payments denominated in Euros,

---

[258] EU Parliament Plenary Verbatim Record (12 April 2016) P8_CRE-REV(2016)04-12 (9), contribution of MEP Weber: 'And we need more. […] We have no TFTP in the European Union. […] We need more commitment on this.'
[259] For this and the previous: 2016 Action Plan, *supra* no.6.
[260] Besides the 'coordination and analytical service', the Commission had presented the option of an 'extraction service' lacking analytical capacities and an upgrade of the Financial Intelligence Unit Platform responsible for merely issuing requests to the Designated Providers: 2013 TFTS Study, *supra* no.5, 14ff.
[261] *Ibid*, 6.
[262] Cf. *Supra* no.257.
[263] 2011 TFTS preliminary study, *supra* no.250, 7f.

(Pan)European automated clearing houses, domestic in-house payment systems and e-money businesses (to mention but a few examples) could be added to the scope of an EU TFTS, in order to provide law enforcement services with a more comprehensive picture of money flow.[264] However, this would lead to a considerable growth of the amount of data collected and could push the system over the edge of operability.[265] Moreover, the inclusion of further services would require considerable data cleansing efforts, whereas it is the high standardisation of the SWIFT-datasets that makes them highly accessible for search, retrieval and analysis. In any case, the expansion of collected data to further providers would go hand in hand with a significant increase in costs. [266]

2. Terrorism and other criminal offences

Whilst the TFTP's purpose is strictly limited to counter-terrorism, the Commission had already considered an expansion to other forms of organised crime in 2013 since different forms of criminality often go hand in hand.[267] In fact, most perpetrators in Europe had criminal records, *inter alia* in drugs dealing, robbery and counterfeit-trading. Experts therefore recommend widening financial monitoring to an 'all-streams approach', [268] including petty crime along with organised crime.[269] However, apart from massive implications for the compliance with fundamental rights resulting from a broader approach, this would also cause a series of rather technical problems: the TFTP is designed to map terrorist networks instead of 'ordinary' crime structures; it remains to be seen if the UST can provide the EU with the necessary know-how. Even if such a capacity building on behalf of the EU was deemed desirable and feasible, this could undermine the complementarity with the TFTP.[270]

---

[264] 2013 TFTS Study, *supra* no.5, 6, 37; Wesseling (2016), *supra* no.12, 14f.
[265] Remarkably, the vast amount of data to be collected served as an argument against the establishment of a centralised EU PNRS because of the high possibility of system crashes, 24/7 operation and a lack of expertise on Union level: Commission, Impact Assessment accompanying the Proposal for a European Parliament and Council Directive on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (Staff Working Paper) SEC (2011) 132 final, 31.
[266] For this and the previous: *supra* no.257.
[267] 2013 TFTS Study, *supra* no.5, 35.
[268] Rajan Basra *et al*, 'Criminal Pasts, Terrorist Futures: European Jihadists and the New Crime-Terror Nexus' (ICSR 2016), 48.
[269] Florence Gaub and Julia Lisiecka, 'The crime-terrorism nexus', EUISS Brief Issue 10/2017.
[270] *Ibid.*

3. Europol's enhanced role in counter-terrorism

The Commission had pointed out that the most convenient, smooth and expeditious implementation of an EU TFTS should be secured within existing structures on the EU level.[271] Experienced in cooperation with the UST and hosting the EU Counter-Terrorism Centre, Europol arguably is the best equipped Union agency to be tasked with the EU TFTS coordination and analytical service. Conversely, Europol could benefit from being commissioned with operating the EU TFTS. The agency was often criticised as hardly living up to its mandate as an information hub because it could not provide assistance to the Member States with analysis based on original intelligence. The reason for this was depicted as 'Europol's chicken-egg-dilemma'[272]: since Europol only has the authority and capability of collecting intelligence from open sources, it relies on national agencies' goodwill to share their raw data and intelligence at European level.[273] However, national counter-terrorism agencies proved particularly reluctant to share their intelligence at all, on the one hand because of the sensitivity of the information for the Member States' national security, on the other because of a lack of trust.[274] The new Europol Regulation has strengthened Europol's position considerably by obliging the Member States to provide personal data and information to Europol's databases (art.7 paras. 6f., recital 13). [275] Additionally, awarding Europol with the task of collecting and analysing European financial messaging data could mitigate the (continuing) dilemma of national agencies being both Europol's provider and customer of intelligence: so far, no Member State has built up the necessary capacities to monitor financial transactions on a large scale; the prospect of being provided with original financial intelligence from Europol could serve as an incentive for the Member States' counter-terrorism agencies to share further data with Europol and finally upgrade the agency to an equal partner in counter-terrorism.

---

[271] 2011 TFTS preliminary study, *supra* no.250, 6.
[272] Oldrich Bures, 'Europol's Counter-terrorism Role: A Chicken-Egg Dilemma' in Christian Kaunert and Sarah Léonard (eds), *European Security, Terrorism and Intelligence: Tackling New Security Challenges in Europe* (Palgrave Macmillan 2013), 65ff.
[273] Björn Müller-Wille, 'The Effect of International Terrorism on EU Intelligence Co-operation' (2008) 46 JCMS 49, 54ff.
[274] *ibid*; John D. Occhipinti, 'Still Moving Toward a European FBI? Re-Examining the Politics of EU Police Cooperation' (2015) 30 Intelligence and National Security 234, 245f.
[275] According to Europol's 2017 Activity Report, the database activity increased significantly: Europol, 2017 Consolidated Annual Activity Report (Public Version 2018), 16ff.

4. Ensuring U.S. support

Finally, a crucial point for building up the capacities for an EU TFTS is U.S. support with knowledge and experience. This might come at the cost of significant compromises. Two main conditions of U.S. cooperation in matters of a European equivalent are, firstly, that any European system would not require substantial alterations of the SWIFT II Agreement and, secondly, that the EU TFTS would allow for efficient and expeditous data sharing by way of a reciprocity mechanism.[276] Whether reciprocity with the U.S. can be secured by a provision similar to art.9 and 10 SWIFT II or if the U.S. will insist on direct access to the system (for instance through on-site U.S. officials) remains to be seen. However, the mere reluctance of the U.S. to adjust the current agreement – in contradiction to their commitment under art.11 – is the final nail in the coffin of the EU TFTS' original purpose of ending bulk transfers to the UST.

IV. Drafting an EU TFTS

In light of the foregoing and the observations of chapter 2, the following paragraphs will depict a draft EU TFTS coordination and analytical service in compliance with European case law. If the system were to be run by Europol, it should fit into the data processing provisions contained in the new Europol-Regulation and, as far as Member States are concerned, comply with the new Data Protection Directive for law enforcement purposes.

As pointed out by Wesseling, any proposal for an EU TFTS must answer the following legal questions:[277]

Would the establishment of an EU TFTS end up in blanket data retention, that is to say mass surveillance?

Is an EU TFTS necessary and proportionate as to:

- the alternative of merely strengthening existing schemes of financial intelligence cooperation in the EU?
- the problem of technically narrowing down data requests and transfers from the designated providers?
- the inclusion of criminal offences beyond terrorism and terrorist financing?

[276] Wesseling (2016), *supra* no.12, 16.
[277] *Ibid*, 23ff.

Would an EU TFTS be liable to different layers of oversight and how can democratic and judicial oversight be ensured in particular? Can the oversight bodies effectively support affected individuals in enforcing their fundamental rights?

The next paragraphs will answer these questions according to the stages of data processing as found in chapter 1 and 2. However, this thesis' scope is still limited to a rough draft of a possible EU system and cannot achieve the detail of a feasibilty study, let alone a legislative proposal. Therefore, where questions remain open, it will be pointed out.

1. Requests for financial messaging data

In any event, the Europol TFTS Unit must have the authority to issue legally binding requests to the designated data providers[278] in order to ensure a constant and reliable supply of data to the searchable data base. Otherwise, data retrieval would not only depend on the Member States' willingness to provide financial data to Europol but also on 27 different law enforcement and data protection regimes (irrespective of the harmonisations introduced by the Data Protection Directive). Consequently, Europol is to be regarded as the data controller responsible for the compliance with data protection safeguards.

An extension of the requests to other designated providers and to purely national transfers is particularly problematic with regard to the CJEU's findings in *Digital Rights Ireland* and *Tele2 Sverige* as to the incompatibility of arts.7 and 8 EUCFR with blanket data collection for preventive purposes: effectively, every personal activity accompanied by money transfers could be subjected to monitoring, thus interfering with the right to privacy and data protection of – potentially – the entire European population. This would go beyond even what the General Data Retention Directive would have provided for since the financial activities liable to collection do not necessarily coincide with a communication between different persons. However, as it cannot be assumed that other financial messaging providers have implemented into their systems the functionality of targeted searches, the requests would identically end up in bulk transfers to Europol, despite utmost diligence in narrowing down the requests' substantial scope.[279] Still, the majority of datasets

[278] Necessary amendments of the Europol Regulation are discussed in chapter 4 (E.).
[279] The preparation of threat assessments, strategic analyses and general situation reports is one of Europol's core competences under the Regulation (art.4 para.1 lit.f, art.18

would belong to entirely unsuspicious persons. This is at odds with the rulings of the Court. Thus, an EU TFTS should be limited either to (European) cross-border money flows or to financial communications sent through SWIFT's network (including those of national clearing houses who use SWIFT's network and standard for their purposes).

As to the inclusion of further criminal offences, the severe interference coming with the data collection described in the previous paragraph requires a high level of justification. Counter-terrorism being the objective pursued, any criminal conduct targeted with the requests must typically accompany the financing of terrorism. Whilst this does not necessarily rule out low-level and petty crimes in the first place, any such offence must be committed within or contribute to a terrorist structure, that is to say display a more or less organised character. Otherwise, the core approach of mapping terrorist networks in order to identify so-far unknown terrorism suspects could be undermined, possibly prompting the Court to question the measures' coherence. It shall not be suggested here which criminal offences meet these criteria. The EU TFTS' legal basis, however, must lay down precisely the criminal conduct that establishes 'a terrorism nexus' and that can be targeted with the data requests (and the searches respectively).[280]

With regard to the necessary safeguards, the Europol Regulation already provides for an increased protection of affected persons. Art.30 imposes restrictions on the processing of sensitive data (para.2), particularly obligating Europol to transparency (para.6, art.31 para.3).[281] However, rules on the processing of data concerning the client-attorney-privilege are absent. Furthermore, it is still questionable if such data is necessary at all for the purposes of the TFTS and if processing could be entirely prevented (as in art.13 para.4 EUPNR Directive). The EU TFTS legal basis therefore should comprise a provision on the handling of sensitive data, in particular regarding data security and automated processing (first and foremost: a prohibition of automated racial profiling).[282]

---

para.2 lit.b, c); thus, the agency should be sufficiently equipped to collate the requests with geographical risk and threat information.

[280] Cf. *DRI*, *supra* no.9, para.60.

[281] However, it provides for less safeguards than Directive (EU) 2016/680: Céline C. Cocq, 'EU Data Protection Rules Applying to Law Enforcement Activities: Towards an Harmonised Legal Framework?' (2016) 7 NJECL 263, 268f.

[282] Art.30 para.4 Europol Regulation remains rather superficial as to automated profiling in comparison to art.11 paras.2 and 3 Directive (EU) 2016/680.

Additionally, the Regulation establishes a comprehensive oversight procedure under the responsibility of the EDPS. Being vested with far reaching powers,[283] *inter alia* to advise Europol in cases of individual rights violations and to eventually impose a ban on processing activities (art.43 para.3), the EDPS can ensure that his or her legal opinion as to the validity of the requests will prevail. To the benefit of affected data subjects, the EDPS is also mandated with the handling of individual complaints. For the complaint to the EDPS and further judicial redress (to the CJEU, art.48), data subjects are not required to provide evidence of their victim status in cases of secret surveillance (here: the fact that Europol's requests result in the collection of the applicant's data).[284]

However, *ex ante* oversight is limited to the consultation procedure of art.39 when the introduction of new data processing activities depends on the EDPS' prior consent. Thus, an approval mechanism with regard to the requests still has to be implemented. Since the EDPS is predominantly focussed on *ex post* supervision, the authority of monthly pre-approving Europol requests would entirely change the system of oversight and possibly overstretch the EDPS' mandate. Preferably, a different oversight body could be tasked with *ex ante* assessment; if so, this body has to provide for sufficient independence of the law enforcement community in general and Europol in particular and to ensure a legal assessment of the requests as much as an expeditious procedure. Although Eurojust was suggested to be a more suitable oversight body than Europol for purposes of SWIFT II,[285] it remains questionable if the agency responsible for the enhancement of transnational criminal prosecution can be regarded as sufficiently impartial to supervise Europol. Generally, Eurojust and Europol established an intense and complex cooperation in

[283] The mandate of the EDPS and the provision of intrusive investigative powers was criticised conflicting with the EDPS' lack of experience in the field of law enforcement and the need for flexibility in data processing for Europol's purposes: Cristina Blasi Casagran, 'The New Europol Legal Framework: Implications for EU Exchanges of Information in the Field of Law Enforcement', in: Maria O'Neill and Ken Swinton (eds.), *Challenges and Critiques of the EU Internal Security Strategy* (Cambridge Scholars 2017), 149, 164; in this respect, the Regulation goes far beyond the Directive (EU) 2016/680, the latter leaving utmost discretion to the Member States as to the appropriate powers awarded to data protection authorities.
[284] Maria Tzanou, 'European Regulation of Transatlantic Data Transfers and Online Surveillance' (2017) 17 HRLR 545, 550 with reference to *Schrems*, *supra* no.9, para.87, *DRI*, *supra* no.9, para.33 and Joined Cases C 465/00, C 138/01 and C 139/01 *Österreichischer Rundfunk and Others* [2003] ECR I-4989, para.75; Valsamis Mitsilegas, 'Surveillance and Digital Privacy' (2016) 47 Colum HRLR 1, 20f, 23f.
[285] Letter to LIBE, *supra* no.7, Attachment p.5.

criminal matters,[286] whilst in particular, Eurojust is also eligible to data requests to the U.S. under art.10 SWIFT II and might come into conflict of interest when approving production orders. What is left are (judicial) warrants issued by national courts, for instance where the designated providers are based. Whether this is a feasible solution cannot be answered here. However, it appears compliant with the Court's case law to merely impose judicial oversight ahead of access to the datasets collected as long as the safeguards for the retention of requested data are sufficiently robust.[287]

2. Data retention: the EU TFTS black box

Within a short period of time, an enormous amount of personal data can be expected to be transferred from the designated providers' systems directly to the searchable database. Similar to its U.S. counterpart, Europol therefore must provide for a secure environment, in particular ensuring data integrity. However, this must not conflict with individual rights to access, rectification, deletion and blocking.

Data integrity and security being a core principle of the Europol Regulation (art.28 para.1 lit.f), Europol is obliged to implement appropriate technical and organisational safeguards in order to prevent data from unlawful access, destruction, dissemination or alteration (art.32); the sub-guarantees listed in art.32 para.2 are comprehensive, their design has to enhance oversight and the protection of individual rights in particular ('privacy by design', art.33).[288] Moreover, whilst art.39 requires the EDPS' placet to the technical and organisational measures before the system goes operational, the maintenance of protocols and documentation of automated processing activities according to art.40 enables the EDPS to meticulously trace back every activity in the database for a period of three years. In case of security breaches, Europol is obliged to proactively provide information

[286] Anne Weyemberg *et al*, 'Competition or Cooperation? State of Play and Future Perspectives on the Relations Between Europol, Eurojust and the European Judicial Network' (2015) 6 NJECL 258, 267ff.

[287] Dissenting: EDPS, EDPS comments on the Communication from the Commission to the European Parliament and the Council on a European Terrorist Finance Tracking System (TFTS) and on the Commission Staff Working Document - Impact Assessment accompanying the Communication from the Commission to the European Parliament and the Council on a European Terrorist Finance Tracking System (TFTS) (2014) <https://edps.europa.eu/sites/edp/files/publication/14-04-17_tfts_comments_en.pdf> accessed 23 June 2018.

[288] Still, with regard to the concept of privacy by design, the Regulation fails to further indicate the technical and organisational requirements and remains rather opaque: Casagran, *supra* no.283, 165ff.

to the EDPS, the national data protection authorities and the affected individuals (arts.34 and 35). Thus, with regards to data integrity and security, the Regulation provides for a satisfactory level of protection.

However, despite the new Europol Regulation introducing the model of integrated data management departing from Europol's previous data bases and files in order to achieve increased interoperability and availability,[289] for purposes of the EU TFTS, the U.S. approach of a stand-alone database should be maintained. Here, costs could be reduced by involving the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice ('eu LISA') in the maintenance of the database on behalf of Europol. eu LISA was established with the mandate to administer the major European databases VIS, SIS II and EURODAC without having the authority to operate the systems under any circumstances.[290] eu LISA's strict data protection regime could thus add another layer of protection to the data stored in the 'TFTS black box'.

Still, in the Court's view, the length of the data retention period is decisive for the severity of the interference with arts.7 and 8 EUCFR. Art.31 of the Regulation provides for an average retention of three years and an option of prolongation up to six years (and beyond) in case of substantiated necessity (to be documented). Despite art.31 para.3 imposing increased oversight on the storage of sensitive data and art.31 para.6 deliminating any alternative to deletion to exactly numerated cases, a blanket retention for a period of three years is likely to come in conflict with the Court's requirements on the sufficient link between the data subjects concerned and the objective pursued when data are retained irrespective of initial suspicion. In this regard, the model laid down in the EU PNR Directive[291] obliging the involved agencies to gradually depersonalise the datasets might serve as a suitable safeguard.[292] Thus, Europol could handle datasets according to their status

[289] As to the advantages and pitfalls coming with this structural change, see: F. Coudert, 'The Europol Regulation and Purpose Limitation: From the "Silo-Based Approach" to… What Exactly?' (2017) 3 EDPL 313ff.
[290] Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (2011) OJ L 286/1.
[291] *Supra* no.59, art.12.
[292] However, the EDPS raised concerns as to appropriateness and necessity of the five year retention period found in the EUPNR Directive (despite masking of datasets): Opinion 5/2015, <https://edps.europa.eu/sites/edp/files/publication/15-09-24_pnr_en.pdf> accessed 01 May 2018, para.24.

of suspicion (which is a general obligation under art.30 para.1 of the Regulation). As to personal data accessed that could not confirm any suspicion whatsoever, the consequence must be the deletion from the database which is to be secured by appropriate technical and organisational measures according to arts.32 and 33.

Currently, the rights of data subjects are tailored for Europol's established informational structure building on data transfers from the Member States, presupposing that the individual will apply for access, rectification or erasure on a national level (art.37). Thus, the legal basis of an EU TFTS has to provide for individual rights directly against Europol as data controller; arts.12 to 16 of Directive (EU) 2016/680 could serve as suitable model for this purpose, including the right to notification (art.13 para.2) and respective derogation clauses (in order to avoid obstruction or prejudice of national law enforcement inquiries, investigations and proceedings and to protect national and public security: arts.13 para.3, 15, 16 para.4).[293] In any case, the EDPS will have oversight on Europol's handling of applications (art.43 para.2 lit.c) and decide upon respective complaints (art.43 para.2 lit.a, art.47) in cooperation with the national data protection authorities with regard to the interpretation of the derogation clauses (art.44f.).

3. Extraction and analysis

According to the 2013 TFTS study, searches to extract data from the database shall be conducted by Europol and Member State representatives alike. Due to the strict security requirements, remote access is to be avoided. Consequently, trained Europol staff and seconded national officals must operate the database on-site (cf. art.6 para.8 EUPNR Directive). The extraction process will most likely be based on the U.S. search-and-retrieval software especially designed for TFTP purposes, that is to say that searches can only be run on individual names or account numbers.

Before a search can be initiated, the investigators have to substantiate suspicion of the targeted person committing or preparing one of the offences liable to the EU TFTS scheme. Whether the threshold necessarily requires reasonable suspicion might be doubted in light of the ECtHR's decision in *Szabó and Vissy*, whereas for purposes of counter-terrorism 'individual suspicion' can be regarded as a

[293] Although the derogation clauses under Directive (EU) 2016/680 are criticised for their broadness, their application is guided by the principle of proportionality which is not expressly mirrored in the Europol Regulation: Cocq, *supra* no.281, 272f.; furthermore, the CJEU's understanding of 'public security' is comparatively restrictive: Case C-145/09 *Land Baden-Württemberg v Panagiotis Tsakouridis* (2010) ECLI:EU:C:2010:708, paras.39ff.

satisfactory safeguard.[294] However, since the notion of 'individual suspicion' is not clear as to its meaning, the legal basis should spell out what is to be understood therewith. In that regard, *ex ante* judicial approval of the searches seems particularly desireable in order to ensure a profound legal interpretation of the access requirements. At this stage of processing, the individuals and bank accounts targeted can be attributed to the national jurisdiction of a Member State and judges can assess the requests on the basis of concrete information provided for substantiation. However, it might be practicable to allocate jurisdiction to a singular national court. In any case, the EDPS and the national data protection authorities will conduct *ex post* oversight on the implementation in practice. Nevertheless, the fact that the EDPS under the Regulation is granted far more powers than most national data protection authorities[295] might hamper the uniform implementation of the advice given. Again, this demonstrates the necessity of *ex ante* judicial approval of every search conducted in the database.

Data extracted will finally be analysed by Europol and national counter-terrorism experts. For this purpose, on-site presence is not necessary, albeit the transfer of the raw networks alone might lead to bulk transmission after all. Although the Europol Regulation contains a Human Rights clause (art.23 para.9) and a (general) ban on purely automated decision making on basis of sensitive data (art.30 para.4; cf. art.10 of the Data Protection Directive), the legal basis for the EU TFTS must go further and indicate the intrusiveness of the techniques applied by denominating the forms of automated data analysis deployed, their overall logic and the additional sources consulted to collate analysis results. That is to say: the fact that the EU TFTS will be based on link analysis including a definition thereof, the maximum number of 'hops' to be taken and the data bases used to generate suspicion in the first place and to cross-check the results of the extraction have to be laid down by law. Whilst the EDPS is already to be consulted beforehand under art.39, a soft oversight mechanism has to be established in order to ensure the state-of-the-art quality of the system. Here, the Europol Data Protection Board under art.44f. might serve as a suitable forum.

[294] *Supra* no.143, para.71.
[295] *Supra* no.283.

4. Data sharing with the U.S.

As to a reciprocity mechanism with the U.S., the new Umbrella-Agreement is supposed to establish an adequate level of data protection for transatlantic data transfers for law enforcement purposes. Since the agreement itself does not build a legal basis for data sharing but imposes a framework of minimum safeguards to be fulfilled in every context, the U.S. and the EU would still have to agree on a cooperation under the EU TFTS. Irrespective of whether this cooperation will be modeled on the current reciprocity clauses, it has been doubted that Umbrella indeed ensures adequate protection to data subjects affected by data transfers.[296] It is outside the remit of this thesis to assess Umbrella's compliance with the criteria deriving from CJEU-case law on arts.7 and 8 EUCFR. There are however two minimum oversight conditions to be provided for in a future EU TFTS/SWIFT III that will be hard to compromise on with the U.S.:

Firstly, and in line with the ECtHR's finding in *Szabó and Vissy*,[297] *ex ante* judicial approval should also be obligatory for U.S. search requests as mere *ex post* (judical) oversight might be hampered by the principle of originator's control. The U.S.' need for secrecy can be met by appropriate procedural safeguards, in particular *in camera* proceedings.

Secondly, any data shared with the UST must not be disseminated to other U.S. or third country agencies without prior approval by Europol (however, urgency procedures should be implemented). All transfers, requests for dissemination and cases of urgency shall be duly documented on behalf of Europol and made accessible to the EDPS (who is allowed to access EU restricted information under the Regulation). Thus, in case of mishandling, the EDPS could at least effectuate his power to impose a preliminary ban on further transfers to the UST.

5. EU TFTS without alternative?

Notwithstanding the foregoing, the set-up of an EU TFTS would add another layer of surveillance to the EU realm. EU data protection watchdogs repeatedly pointed out that a mere 'added value' for EU counter-terrorism was an insufficient justification for an EU TFTS;[298] in particular, the Article 29 Working Party 'would

[296] Korff, *supra* no.214.
[297] *Supra* no.184.
[298] EDPS, *supra* no.287.

find it difficult to accept any justification which allows the continuation of the US-TFTP agreement in parallel with the establishment of an EU TFTS'.[299] However, the last impact assessment put into question whether less intrusive means of financial intelligence are as efficient as an EU TFTS.[300] Remarkably, instead of publishing the announced paper on a complementary EU TFTS, the Commission focussed on strengthening the EU Financial Intelligence Unit Platform in its October 2017 progress report.[301] Again, this rather appears to be a complementary approach to a future EU TFTS and neither does it come without data protection concerns.[302]

However, the establishment of a system described in this chapter does not only challenge individual rights. Neither is it obvious that the EU could act on the basis of its ordinary competence and procedure. Therefore, the last chapter will investigate whether EU primary law provides for sufficient EU powers.

[299] Letter from Jacob Kohnstamm to Cecilia Malmström (29 September 2011) <file:///C:/Users/HP/Downloads/20110929_letter_to_commission_tfts_en.pdf> accessed 23 June 2018.
[300] 2013 TFTS Study, *supra* no.5, 29.
[301] Commission, Eleventh progress report towards an effective and genuine Security Union, COM (2017) 608 final, 5f.
[302] In particular regarding the oversight structure of FIUs: *supra* no.299.

E. Chapter 4: A question of competence

So far, the EU's competence to establish an EU TFTS has been understood as a matter of shared competence in the Area of Freedom, Security and Justice (AFSJ) according to arts.82 and 87 TFEU.[303] Respectively, it was art.87 TFEU in connection with art.216 TFEU which served as legal basis for SWIFT II. However, the question of competence should be dealt with increased attention. The CJEU's case law on the distribution of competences with regard to police cooperation was rather inconsistent before the Lisbon Treaty came into force.[304] The *PNR Canada* case was the first opportunity for the Court to rule on the post-Lisbon competences on data protection in the context of counter-terrorism and it found the legal basis chosen (arts.82 and 87 TFEU) incorrect, for falling short of art.16 para.2 TFEU.[305]

This chapter will put the Commission's assumption of competence into question, firstly, by demonstrating that with respect to Europol, primary law is far from clear as to which investigative powers can be conferred to the agency. Secondly, it will be argued that the security terminology of the treaties suggests a restrictive interpretation. Thirdly, it is concluded that the EU TFTS requires reliance on the flexibility clause resulting in a different legal procedure.

I. art.88 TFEU: the Europol legal basis

If Europol indeed was tasked with requesting financial data from designated providers, this would require the power to directly retrieve personal data from databases held by private parties for commercial purposes. Under the Europol Regulation, however, Europol is forbidden to collect any personal data unless it has been transferred by a Member State, Union body, third state or international organisation or can be directly retrieved from publicly accessible sources (art.17 paras.1 and 2). Affirmed in art.26 paras.1, 2 and 9, Europol is interdicted from any contact with private parties in order to retrieve personal data, including data retrieval with the consent of the concerned data subject. The Regulation would preclude Europol from issuing subpoenas or any other kind of requests to designated providers. Thus, this power has to be conferred to Europol in order to set up an EU TFTS as described in the previous chapter.

---

[303] 2013 TFTS Study, *supra* no.5, 15.
[304] *EU-US PNR 2006*, *supra* no.23; Case C-301/06 *Ireland v European Parliament and Council of the European Union* (2009) ECLI:EU:C:2009:68 on the 2006 Data Retention Directive.
[305] *PNR Canada*, *supra* no.10, paras.76ff., 95ff.

Any alterations to Europol's legal framework must concur with the procedural and substantial provisions set out in art.88 TFEU.[306] The Lisbon Treaty significantly amended art.88 with the aim of upgrading Europol from a mere assistant agency to a partner with the Member States' law enforcement services.[307] Whilst Europol's core mandate as information hub is mirrored in art.88 para.2 lit.a stating that 'the collection, storage, processing, analysis and exchange of information, in particular that forwarded by the authorities of the Member States or third countries or bodies' is a task subject to the ordinary legislative procedure, para.3 clarifies that '[any] operational action by Europol must be carried out in liaison and in agreement with the […] Member States whose territory is concerned' and that '[the] application of coercive measures shall be exclusive responsibility of the competent national authorities'.

1. Production orders within the remit of Europol's data collection mandate?

Issuing data requests to designated providers on first sight appears in perfect compliance with Europol's 'collection' capacity mentioned in art.88 para.2 lit.a TFEU. The non-exhaustive enumeration of the data sources allows for a broad understanding of the provision, that is to say the power to retrieve data indirectly from other law enforcement authorities and directly from private parties. On the other hand, this might contravene para.3 interdicting Europol from applying coercive measures while executing its tasks.[308] Literally, subpoenas incorporate a coercive element. However, systematically, the exclusion of coercive measures refers to operational actions[309] that are distinct from data processing generally, although both forms of police activity are often closely connected.[310] In fact, data

[306] Steve Peers, *EU justice and home affairs law* (3rd edn, Oxford University Press 2011), 877; eventually, art.87 para.2 lit.a in connection with art.88 para.2 lit.a TFEU would build a joint legal basis (together with art.16 TFEU).
[307] *Ibid*, 871f.
[308] Bettina Schöndorf-Haubold, 'Europäisches Sicherheitsverwaltungsrecht, § 35', in: Jörg Philipp Terhechte (ed.), *Verwaltungsrecht in der Europäischen Union* (Nomos 2011), 1212, 1231.
[309] Operational cooperation is understood as any 'action related to concrete cases/events/crisis/phenomena that require a trans-national approach whereby all the concerned authorities of the Member States' competent at national level collaborate with each other and with the competent Union bodies': Council, 'Discussion paper on the future Standing Committee on Internal Security (COSI) - Constitutional Treaty, art.III-261; 21/02/2005' doc.6626/05, para.15; Oliver Dörr, 'AEUV Art. 276 [Unzuständigkeit des EuGH für mitgliedstaatliche Polizeimaßnahmen]' in: Eberhard Grabitz et al. (eds), *Das Recht der Europäischen Union* (60th EL October 2016), para.13.
[310] Cf. Peers, *supra* no.306, 876 with reference to the distinction between art.87 para.2 and para.3 TFEU.

collection by law enforcement agencies might cross the line from informational to operational activity.

2. Production orders: 'the operational level of intelligence'[311] kept to the Member States?

Albeit Europol is eligible to take part in operational action according to art.88 para.2 lit.b and para.3 sentence 1 TFEU, for example in Joint Investigation Teams, it is limited to merely supportive action. As soon as any contribution requires the application of coercive powers, these are exclusively reserved to the respective national authorities. Coercive measures include, *inter alia*, the powers to arrest a person, to search a person or a location[312] as well as to covertly observe a person by telephone surveillance or eavesdropping.[313] The latter examples demonstrate that art.88 para.3 sentence 2 TFEU might very well exclude certain methods of information gathering.[314] However, the legal background of the exclusion of coercive measures from Europol's powers is contentious:

a. The State monopoly of force

The exclusion could aim at protecting the Member States' monopoly of the legitimate use of force.[315] Art.88 para.3 TFEU is generally understood as a specific application of the general rule found in art.72 TFEU[316] according to which the exercise of the national responsibilities in maintaining law and order and internal security shall not be impeded by the fifth title of the TFEU. However, it remains indefinite as to which powers exactly flow from the monopoly of force. It is widely agreed that immediate physical force traditionally is at the heart of the monopoly; [317] however, this does not explain why Europol is excluded from eavesdropping and

[311] Taken from: Kristof Clerix, 'Ilkka Salmi, the EU's spymaster' <https://www.mo.be/en/interview/ilkka-salmi-eu-s-007> accessed 29 June 2017, quoting the director of INTCEN (EEA intelligence hub) as saying: '[We are] not an operational agency. We do not have a collection capability. […] We do not carry out clandestine operations. The operational level of intelligence is the Member States' responsibility'.
[312] Elena Spaeth, 'AEUV Artikel 88 (ex-Artikel 30 EUV) [Europol]', in: Hans von der Groeben *et al* (eds), *Europäisches Unionsrecht* (7th edn, C.H. Beck 2015), para.3.
[313] Knut Amelung, 'Zwangsbefugnisse für Europol?', in: Jürgen Wolter *et al* (eds), *Alternativentwurf Europol und europäischer Datenschutz* (C.F. Müller 2008), 233, 240.
[314] Cf. Nicholas Grief, 'EU law and security' (2007) 32 ELR 752, 759ff.
[315] Peter-Christian Müller-Graf, 'Artikel 72 AEUV [Nicht berührte Zuständigkeiten der Mitgliedstaaten]', in: Matthias Pechstein *et al* (eds), *Frankfurter Kommentar zu EUV, GRC und AEUV* (Mohr Siebeck 2017), para.3.
[316] Peers, *supra* no.306, 55.
[317] Cf. Christian Callies, 'Die Europäisierung der Staatsaufgabe Sicherheit unter den Rahmenbedingungen des freiheitichen Rechtsstaats', in: Erwin Müller and Patricia

communications surveillance.[318] Unsurprisingly, definitions of the boundaries vary and may even include mere announcements of the application of (physical) force in order to achieve obedience to a legal duty.[319] Assuming that the monopoly of the use of force comprises coercion of any kind, direct or indirect, the conferral of investigative competences to the Commission in matters of competition law (art.105 TFEU)[320] would apparently intrude on the preserved area of sovereignty. Conclusively, in order to shape the scope of art.88 para.3 sentence 2 TFEU, the institution of the state monopoly of force appears too vague after all.[321]

b. Interference with Fundamental Rights: a national prerogative?

Another reason for limiting Europol's powers in information gathering might be the intrusiveness of secret surveillance to the fundamental rights of the concerned persons, requiring a high level of justification that should be reserved to the special relationship between the Member States and their individuals.[322] Undeniably, coercive and clandestine police action interferes severely with individual rights; as elaborated in chapter 3, the production orders would amount to considerable human rights intrusions for the data subjects affected. Nevertheless, other methods and stages of data processing are not necessarily less intrusive, especially if conducted on a large scale, but are certainly in the remit of Europol, which is clearly demonstrated in the new Europol Regulation. Thus, the particular relevance of fundamental rights is a coincidental but not exclusive feature of coercive measures and can neither define the line between art.88 para.2 lit.a and para.3 when it comes to data retrieval.

Therefore, the following paragraphs will take a general look at the distribution of competences in the AFSJ in order to figure out whether art.88 para.2 lit.a TFEU is open to a broad or narrow interpretation.

Schneider (eds), *Die Europäische Union im Kampf gegen den Terrorismus: Sicherheit vs. Freiheit?* (Nomos 2006), 83, 89.

[318] Amelung, *supra* no.313, 240, 248.

[319] Stephan Bittner, 'Zwangsmittel im Recht der Europäischen Union: Geteilte Rechtsmacht in Europa', in: Manfred Zuleeg (ed), *Europa als Raum der Freiheit, der Sicherheit und des Rechts* (Nomos 2007), 9, 10ff.

[320] Amelung, *supra* no.313, 241f.

[321] *Ibid*, 248.

[322] Cf. Anna Jonsson Cornell, 'EU Police Cooperation Post-Lisbon' in: Maria Bergström and Cornell (eds), *European Police and Criminal Law Co-operation* (Hart Publ. 2014), 147, 150f.

II. EU competences in the AFSJ: security (terminology) in the making

With the Lisbon Treaty, the AFSJ was fully integrated into the European Union's supranational policies as a matter of shared competence between the Union and the Member States. This comes with the effect of 'pre-emptive Union action', meaning that so long and so far as the Union exercises its competence, the Member States are excluded from legislative action (art.2 para.2 TFEU). This also holds true for the previous 'third pillar' of police and justice cooperation in criminal matters (chapters 4 and 5 of Title V) which now form equal part of the AFSJ, besides policies on border checks, asylum and immigration (chapter 2) and judicial cooperation in civil matters (chapter 3). However, chapters 4 and 5 kept a number of exceptional provisions, e.g. art.82 para.2, 3 and art.83 para.2, 3 TFEU providing for what is referred to as 'emergency-brake clauses' when it comes to the approximation of substantive and procedural criminal law. These particularities apparently correlate to the Member States' prior responsibility for 'internal security' as mirrored in art.72 TFEU.

Moreover, the Treaty Reform introduced the notion of 'national security' in art.73 TFEU and art.4 para.2 sentences 2 and 3 TEU. Whilst the former somewhat nebulously states that *'[it] shall be open to Member States to organise between themselves and under their responsibility such forms of cooperation and coordination as they deem appropriate between the competent departments of their administrations responsible for safeguarding national security*', art.4 para.2 TEU seems to fundamentally delineate Union policy from the purely national realm:

> *'The Union shall respect the equality of Member States before the Treaties as well as their national identities […]. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State.'*

The meaning of 'national security' as distinct from 'internal security' is far from clear.[323] The Court has not yet had the chance to deliver its understanding of the

[323] Grief, *supra* no.314, 754ff.; a good summary on the (inconsistent) security terminology of the Treaties can be found in: Gloria Gonzalez Fuster *et al*, 'Discussion paper on legal approaches to security, privacy and personal data protection' (PRISMS Deliverable 5.1, 2013), 3ff.

security terminology used in the Treaties.[324] The strong wording suggests that the Member States wanted to restrain the EU in security matters. If so, the Union competences within the AFSJ, including art.88 para.2 lit.a TFEU, might require a restrictive interpretation.

1. Background of 'Christophersen Clause'

Originally stemming from the context of complementary competences (now art.6 TFEU), art.4 para.2 TEU was introduced as a general rule regarding the distribution of competences between the Union and the Member States. Instead of enumerating negative competences deemed not to be conferred to the Union, the responsible Committee[325] decided to reinforce the principle of respect of the national identities (now: sentences 1 and 2) to prevent the EU from silently extending its competences beyond the wording of the Treaties.[326] Interestingly, it was no later than at the Convent of Europe when the term 'national security' replaced 'internal security' in sentence 2 and that sentence 3 was added.[327] Together with art.73 TFEU, art.4 para.2 was included in the texts upon request from the UK government[328] and welcomed by the Member States who allegedly wanted to prevent the Union from further encroaching on their security competences in the context of counter-terrorism.[329]

What can be derived from the evolution of art.4 para.2 TEU and arts.72, 73 TFEU was subject to controversy, first and foremost in respect of the applicability of EU

[324] As to derogations from the market freedoms, the Court defined the term of 'public security': Tsakouridis, *supra* no.293; however, this is little helpful for the delineation of competences: Alicia Hinarejos, 'Law and order and internal security provisions in the Area of Freedom, Security and Justice: before and after Lisbon', in: Christina Eckes and Theodore Konstadinides, *Crime within the Area of Freedom, Security and Justice* (Cambridge University Press 2011), 249ff.
[325] Headed by the former Danish Prime Minister and EU-Commissioner Henning Christophersen.
[326] For this and the previous: Barbara Guastaferro, 'Beyond the Exceptionalism of Constitutional Conflicts: The Ordinary Functions of the Identity Clause' (2012) 31 YEL 263, 271ff.
[327] Christian Calliess *et al*, 'EU-Vertrag (Lissabon) Art.4 [Zuständigkeiten der Union, nationale Identität, loyale Zusammenarbeit]', in: Callies and Matthias Ruffert (eds), *EUV/AEUV* (5th edn, C.H. Beck 2016), para.6 no.17.
[328] Jean-Claude Piris, *The Lisbon Treaty: a legal and political analysis* (Cambridge University Press 2010), 191; lateron, the UK government explained that the meaning of 'national security' was identical to what formely had been the 'internal security of each Member State' but constantly had caused confusion with the notion of 'internal security of the Union': House of Lords, The Treaty of Lisbon: An Impact Assessment. Volume I: Report (2008), 157f.
[329] Walter Obwexer, 'EUV Artikel 4 [Zuständigkeiten der Union]', in: von der Groeben *et al*, *supra* no.312, para.46.

fundamental rights and the consequences for the NSA affair.[330] However, as will be shown in the subsequent parapgraphs, the arguments issued are no less relevant for the delineation of competences in the AFSJ.

2. No restraint in matters of security?

According to Peers, neither the new provisions on 'national security' nor art.72 TFEU on 'internal security' impose any general reservations on EU competences in the AFSJ. Otherwise, there was no need of express procedural or substantial exceptions (e.g. the emergency brake clauses or art.79 para.5 TFEU). If any, restrictions were to be interpreted narrowly, irrespective of Art.4 para.2 TEU which could not be more specific than art.72 TFEU for its nearly identical wording and the fact that it merely commands the Union's '*respect*' for the Member States.[331] On the other hand, Art.73 TFEU could neither restrain Union competence since it addresses only the Member States which shall not be excluded from further action.[332]

Following Peers' approach, art.88 para.2 lit.a TFEU is open to broad interpretation whilst the exclusion of coercive measures – as an exception to the rule – must be understood narrowly. Consequently, Europol could be provided with further data retrieval capacities in order to establish an EU TFTS. However, denying any impact of art.4 para.2 TEU on the distribution of competences between the Union and the Member States regarding security sensitive issues conflicts with its wording and systematic position: Whilst sentence 3 is unbiased in declaring national security to remain 'the sole responsibility of the Member States', art.4 para.2 TEU clearly finds itself in the context of conferral of competences. Its preceding paragraph rephrases the principle of conferral as to the competences which (exclusively) remain with the Member States; art.5 TEU sets out the principles of conferral, subsidiarity and proportionality; art.3 TEU dealing with the Union's objectives closes noting that 'the Union shall pursue its objectives by appropriate means commensurate with the competences which are conferred upon it in the Treaties' (para.6). This is

[330] Pars pro toto: Douwe Korff, 'Expert Opinion prepared for the Committee of Inquiry of the Bundestag into the "5Eyes" global surveillance systems revealed by Edward Snowden' (Committee Hearing of 5 June 2014) <https://www.bundestag.de/blob/282874/8f5bae2c8f01cdabd37c746f98509253/mat_a_sv-4-3_korff-pdf-data.pdf> accessed 06 July 2018, 35ff.

[331] Similar: Armin von Bogdandy and Stephan Schill, 'EUV Art. 4 Prinzipien der föderativen Grundstruktur', in: Grabitz *et al*, *supra* no.309, para.35; Obwexer, *supra* no.329, para.52; Volker Röben, 'AEUV Art.72 Nationale Zuständigkeiten' in Eberhard Grabitz *et al* (eds), *Das Recht der Europäischen Union* (61st edn, C.H. Beck 2017), para.16.

[332] For the entire paragraph: Peers, no.306, 54ff.

furthermore backed up by the provision's intention to render a negative catalogue of competences superfluous.[333]

3. National security: a domaine reservée?

Müller-Graff takes the opposite position to *Peers*, concluding that art.72 TFEU and art.4 para.2 sentence 2, 3 TEU guard the Member States' *domaine reservée*. Consequently, EU competences within the AFSJ were to be interpreted restrictively.[334] He understands 'internal security' as a subset of 'national security', *inter alia* protecting the state monopoly of force. At the most, Member States could be urged to execute their reserved competences in security matters in loyalty to the Union as emphasised in art.4 para.3 TEU.[335]

Accordingly, art.88 para.2 lit.a TFEU required a narrow reading with the consequence that Europol could not be tasked with data collection further than indirect retrieval. However, Müller-Graff's approach does not credit the fact that a multitude of competences were conferred to the EU in the field of internal security for legislative action. It is now in the Union's competences to build up a considerable body of substantial and procedural criminal law (arts.82, 83 TFEU) and – prospectively – prosecution capacities (art.86 TFEU). Admittedly, these competences depend on unanimity in the Council but they are not excluded from EU policy *a priori*. The set-up of Frontex on the basis of art.77 para.2 lit.b, c and d TFEU gives evidence of the Union's far reaching powers in matters of border control.[336] Furthermore, derogative clauses referring to 'public security' (e.g. art.36 TFEU) or 'essential interests of [the Member States'] security' (e.g. art.347 TFEU) demonstrate that the Member States are not entirely free from European regulation while executing their responsibilities in internal and national security.[337]

---

[333] For this and the previous: cf. Guastaferro, *supra* no.326, 271ff.
[334] Consenting as to the restrictive interpretation of EU competences: Stephan Breitenmoser and Robert Weyeneth, 'AEUV Artikel 72', in: von der Groeben *et al*, *supra* no.312, paras.4ff.; Calliess *et al*, *supra* no.327, para.21.
[335] For the entire paragraph: Müller-Graf, *supra* no.315, paras.1ff.
[336] Although exercise of coercive powers is under supervision of the Host Member State and only permissible within the boundaries of respective national law: Jorrit J. Rijpma, 'Frontex and the European System of Border Guards. The future of European Border Management', in: Maria Fletcher *et al* (eds), *The European Union as an Area Freedom, Security and Justice* (Routledge 2017), 217, 237f.
[337] Hermann-Josef Blanke, 'Article 4 [The Relations Between the EU and the Member States]', in: Blanke and Stelio Mangiameli, *The Treaty on European Union (TEU): a commentary* (Springer 2013), paras.77ff.

4. Relative competence in security matters?

Möstl pursues a significantly different approach interpreting art.72 TFEU as a provision of 'relative' competence. Pointing at the provision's wording that merely prevents the Member States from being 'affected' in their responsibility on internal security, art.72 TFEU primarily preserved the Member States' margin of appreciation as to their appropriate level of security, regardless of the minimum level flowing from EU action. Since the AFSJ aimed at a high level of security,[338] art.72 TFEU simply clarified that Union action was deemed to complement the Member States' action where necessary; however, the EU should neither substitute the Member States' role nor exclude any further measures being taken at national level.[339]

Under this assumption and against the background that the Member States have not built up their own capacities for large scale financial monitoring, art.88 para.2 lit.a TFEU could serve as a legal basis for tasking Europol with the EU TFTS. Nevertheless, interpreting art.72 TFEU as a provision basically leading to parallel competences of the Union and the Member States in the field of internal security appears incoherent with the system on shared competences set out in art.2 para.2 and art.4 TFEU. Where the TFEU wishes to prevent the pre-emption of Member State competences, it says so expressly (e.g. art.4 paras.3 and 4 TFEU). Introducing the category of 'relative competence' (as distinguished from 'parallel') rather adds to the complexity of the security terminology used in the Treaties.

5. Intelligence agencies: The clue to the puzzle?

Remarkably, it is widely agreed that intelligence agencies are beyond EU policies and competences because they operate at the very heart of national security as laid down in art.4 para.2 TEU.[340] If given an institutional meaning rather than a functional interpretation,[341] 'national security' would primarily restrain the EU to

[338] See: art.67 para.3 TFEU.
[339] For this and the previous as to the identical worded predecessor: Markus Möstl, *Die staatliche Garantie für die öffentliche Sicherheit und Ordnung: Sicherheitsgewährleistung im Verfassungsstaat, im Bundesstaat und in der Europäischen Union* (Mohr Siebeck 2002), 601ff.; ‚Grundfragen Europäischer Polizeilicher Kooperation, in: Dieter Kugelmann (ed) *Migration, Datenübermittlung und Cybersicherheit* (Nomos 2016), 9, 14f.
[340] European Union Agency for Fundamental Rights (FRA), *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Mapping Member States' legal frameworks* (2015), 6f.
[341] Heinrich Amadeus Wolff, 'BDSG 2018 § 45 Anwendungsbereich', in: Wolff and Stefan Brink (eds), *BeckOK Datenschutzrecht* (24th edn, C.H. Beck 2018), para.20f.

(partly) accroach on the business of national intelligence services through wide effectuation of its competences.[342] Symptomatically, there is neither an 'EU intelligence service' existent under the current EU framework[343] nor a definition of intelligence services found in the Treaties altogether. Irrespective of the variety of intelligence agencies in the Member States, it can be summed up that their mandate is focused on data collection (of any kind) and analysis whilst lacking further operational powers.[344] Thus, regularly collecting the same information while pursuing different purposes, intelligence services work in parallel to national law enforcement agencies.

Whereas this parallelism is not continued at EU level, Europol is also tasked with 'data processing' but limited as to operational powers. With Europol's focus on transnational crime in general and counter-terrorism in particular, its field of action is likely to collide with the national intelligence agencies. It comes as no surprise that Europol must not require the Member States to 'disclose information relating to organisations or specific intelligence activities in the field of national security' (art.7 para.7 lit.c Europol Regulation).[345] In a general manner, this is corroborated in Declarations nos.20 and 21 to the Lisbon Treaty as to the impact of EU data protection rules on matters of national security and in the police sector, suggesting that the AFSJ 'is not a normal area of law where the general framework of data protection applies'.[346] Therefore, it is this thesis' stance that with regards to data collection for security purposes, the Treaties preserve the Member States' prerogative of first access to data in order to ensure the institutional protection of intelligence services. This prerogative must not be undermined by an extensive interpretation of art.88 para.2 lit.a TFEU. An exception is only compliant with EU primary law where Member States could not claim any exclusivity whatsoever, that

[342] Hansjörg Geiger, 'Rechtliche Grenzen der Europäisierung nachrichtendienstlicher Aufgaben', in: Thomas Jäger and Anna Daun (eds), *Geheimdienste in Europa Transformation, Kooperation und Kontrolle* (VS Verlag 2009), 240, 244.
[343] INTCEN is no operational service but merely provides analyses and policy recommendations which are based on the national intelligence services' strategic information: Mai'a K. Davis Cross, 'A European Transgovernmental Intelligence Network and the Role of IntCen' (2013) 14 Perspectives on European Politics and Society 388, 393.
[344] FRA, *supra* no.340, 27.
[345] Mirroring the CJEU's understanding of 'state security': Case C-300/11 *ZZ v Secretary of State for the Home Department* (2013) ECLI:EU:C:2013:363, para.66.
[346] Julia Ballaschk, 'In the Unseen Realm: Transnational Intelligence Sharing in the European Union – Challenges to Fundamental Rights and Democratic Legitimacy' (2015) Stan JInt'l L 19, 29.

is to say where data is openly accessible to anyone, mirrored in art.17 para.2 Europol Regulation.

This finding is affirmed in art.73 TFEU which was introduced alongside of art.4 para.2 TEU into the body of primary law. Referring to the '*competent departments of [the Member States'] administrations responsible for safeguarding national security*', the provision expressly displays an institutional understanding of 'national security'. There is no reason apparent suggesting that the notion of national security was used differently in art.4 TEU and art.73 TFEU, although art.73 TFEU confusingly declares cooperation and coordination on these matters 'open to the Member States'. Some authors derive from this wording that the Treaties grant the Member States the opportunity to conclude bilateral agreements on internal security cooperation (e.g. for Transnational Police Units);[347] others understand art.73 TFEU to exclude the pre-emptive effect of art.2 para.2 TFEU.[348] However, the wording might be simply misleading[349] since the Member States have never been excluded from security cooperation beyond the AFSJ – irrespective of the competences conferred upon the Union in (internal) security matters.[350]

Hence, primary law suggests the understanding that Europol's competences in data collection must be handled restrictively, preventing the EU from conferring further powers of direct data retrieval to the agency for purposes of an EU TFTS on the basis of art.88 para.2 lit.a TFEU. Nevertheless, the flexibility clause might offer an alternative legal basis if the Council can agree on the EU TFTS unanimously.

III. Effectuating the flexibility clause

The Commission already indicated that implementing the vision of a Security Union could require the effectuation of art.352 TFEU.[351] Art.352 TFEU sets out four explicit substantive requirements which must be met in order to serve as a legal basis for the EU TFTS.

---

[347] Müller-Graff, 'Artikel 73 AEUV [Zusammenarbeit der Mitgliedstaaten in eigener Verantwortung]', in: Pechstein *et al*, *supra* no.315, paras.2f.; Möstl, *supra* no.339, 17f.
[348] Cf. Matthias Rossi, 'AEUV Art.73 [Zusammenarbeit der Mitgliedstaaten]', in: Calliess/Ruffert, *supra* no.327, para.2.
[349] Marcel Kau, 'Justice and Home Affairs in the European Constitutional Process – Keeping the Faith and Substance of the Constitution', in: Stafan Griller/Jacques Ziller (eds), *The Lisbon Treaty* (Springer 2008), 223, 229.
[350] As to the mere declaratory nature: Müller-Graff, *supra* no.347, para.1.
[351] European Political Strategy Centre, *'Towards a "Security Union" - Bolstering the EU's Counter-Terrorism Response'* EPSC Strategic Notes 12/2016, 2.

Firstly, the flexibility clause can be relied upon only with the aim of attaining a policy objective contained in the Treaties. For the establishment of an EU TFTS, it is primarily the objective of prevention and persecution of terrorism mirrored in art.88 para.1 TFEU outlining Europol's mission to strengthen the Member States' action and art.222 TFEU concerning the prevention of terrorist attacks[352] pursued when invoking art.352 TFEU.

Secondly, the EU must lack the competence that shall be drawn from art.352 TFEU. A lack of competence is not reduced to the case that the Treaties do not provide any competence on the matter at all; if primary law contains a competence which either falls short of the objectives to be achieved therewith or which is unclear in scope, art.352 TFEU can be applied in connection with the respective provision.[353] As demonstrated in the previous paragraphs, it is at least unclear if art.88 para.2 lit.a TFEU provides Europol with the necessary competence of direct data retrieval. Due to the flexibility clause's exceptionality, every means of interpretation has to be exhausted beforehand, including an *effet utile* interpretation or applying the implied powers doctrine.[354] Albeit art.67 para.3 TFEU stipulates the objective of a 'high level of security' within Europe, *effet utile* would conflict with the previous finding that EU competences in the AFSJ have to be interpreted restrictively unless the wording suggests otherwise.[355] As opposed to art.77 para.2 lit. d TFEU on the establishment of an integrated border control system, art.88 para.2 lit.a TFEU does not permit 'any measure' but indicates the nature of the data sources in order to achieve the task of data collection. Moreover, as observed by Herlin-Karnell, a 'focus on security in combination with the effectiveness mantra constitutes a particularly dangerous combination'.[356] Against this background, there is no room for *effet utile*.

Neither could extended powers over data retrieval be inferred from the implied powers doctrine that merely justifies the implementation of measures inevitable to exercise conferred powers (so-called 'narrow approach') or defined tasks ('wider

[352] *Ibid*.
[353] ECJ, Case C-8/73 *Hauptzollamt Bremerhaven v. Massey-Ferguson* ECR 897, para.4; however, the complementary application of art.352 TFEU is contentious: Rossi, 'AEUV Art. 352 [Flexibilitätsklausel]', in: Calliess/Ruffert, *supra* no.327, paras.66ff.
[354] *Ibid*, paras.61ff.
[355] Calliess *et al*, *supra* no.334.
[356] Ester Herlin-Karnell, *The constitutional dimension of European criminal law* (Hart Publ. 2012), 85.

approach') in a reasonable and efficient manner.[357] Direct access to data subjects is not necessary for Europol in order to fulfil its task of data collection generally, nor is there any other power conferred to Europol which could not be exercised without direct data retrieval.[358]

Thirdly, Union action must be necessary to achieve the treaty objective. That is to say that primary law has to display a discrepancy between the competences conferred to the Union and the objectives set out in the Treaties; the Commission and Council can claim a margin of (political) appreciation when it comes to qualifying whether this discrepancy is tolerable or not.[359] Against the background of the horrific attacks during the last two years alone and the assumption that homegrown terrorists and foreign fighters who returned to Europe pose an increased security risk to the safety of European people, it seems unlikely that the Court would put the Commission's assessment into question that vesting Europol with further data retrieval competences is necessary for the set up an EU TFTS.[360]

Fourthly, the competence to be derived from art.352 TFEU must not exceed the framework of the policies defined in the Treaties in order to attain the objective. Seemingly a rather redundant requirement, not all of the Treaties' policies are open to the flexibility clause: in matters of Common Foreign and Security Policy (CFSP), art.352 para.4 TFEU excludes the clause's applicability. Moreover, the invocation of art.352 TFEU must respect the concerned policy's distinct character; therefore, it can be questioned if the flexibility clause can be effectuated at all within the AFSJ.[361] From the clearly defined exclusion of CFSP issues, however, it can be deduced contrariwise that the AFSJ shall not be immune to art.352 TFEU. Nonetheless, the provisions mirroring the Member States' special status and primary responsibilities regarding the maintenance of internal and national security must

[357] Lorna Woods *et al*, *Steiner & Woods EU law* (13th edn, Oxford University Press 2017), 68f.
[358] In fact, art.88 TFEU does not refer to any concrete powers at all since para.2 merely enumerates tasks.
[359] T. C. Hartley, *The foundations of European Union law: an introduction to the constitutional and administrative law of the European Union* (7th edn, Oxford University Press 2010), 112f.
[360] Europol, *TESAT European Union Terrorism Situation and Trend Report 2017*, 10ff.; cf. European Political Strategy Centre, *supra* no.351, 7: 'In the framework of the area of freedom, security and justice Article 68, 74, 75, 77, 83, 84 and 87 TFEU comprise certain European competences that allow for (limited) action to prevent terrorism. These enable the EU to establish measures with regard to capital movements and payments (…)'.
[361] Calliess *et al*, *supra* no.334.

not be circumvented by relying on the flexibility clause.[362] This is where the CJEU clarified beforehand that the flexibility clause cannot substitute formal amendments to the Treaties. Whilst the red line between minor adjustments and major changes of primary law tends to blur, the Court stated that art.352 TFEU did not provide the Union with *Kompetenz-Kompetenz*.[363]

However, the establishment of an EU TFTS is unlikely to generally undermine the Member States' prerogative in internal or national security. The fact that the Member States so far could not build up the capacities to extensively monitor financial communications within their respective territories indicates otherwise. As long as Europol's powers on information gathering are not extended to generally retrieve personal data directly[364], the legal boundaries set out by arts.72, 73 TFEU and art.4 para.2 sentences 2, 3 TEU are still observed. Thus, a formal amendment of the Treaties is unnecessary in order to set up an EU TFTS.

To sum up, the flexibility clause provides a suitable legal basis for the establishment of an EU TFTS (together with art.87 para.2 and art.16 TFEU). However, the implementation of security sensitive measures without express legal basis in primary law seems to confirm the exact concerns raised by the German Constitutional Court towards silent amendments of the Treaties lacking sufficient national democratic legitimation and undermining the Member States' sovereignty.[365] Against this background, unanimous decision finding in the Council is all but certain.

[362] For this and the previous: Rossi, *supra* no.353, para.42.
[363] ECJ, Opinion 2/94, *Accession of EC to ECHR* (1996) ECLI:EU:C:1996:140, para.30.
[364] Cf. Schöndorf-Haubold, *supra* no.308, 1259.
[365] BVerfGE 123, 267, 394f; the Court's 'anxiety towards integration' was criticised, e.g.: Daniela Winkler, 'Vergangenheit und Zukunft der Flexibilitätsklausel im Spannungsfeld von unionalem Integrations- und mitgliedstaatlichem Souveränitätsanspruch - Eine Analyse von Artikel 352 AEUV unter dem Eindruck des BVerfG-Urteils zu "Lissabon"' (2011) Europarecht 384ff.

F. CONCLUSION

The investigation has shown that the current SWIFT II scheme constitutes multiple violations of EU fundamental rights. Nevertheless, political stakeholders are not willing to replace transatlantic bulk transfers with a more targeted mechanism, let alone to end the intelligence cooperation with the U.S. under SWIFT II altogether. Albeit the agreement was intended to remain in force until 2015 (art.23 para.2), the EU did not take the chance to re-enter into negotiations in order to tackle the weaknesses outlined in chapter 2.[366] Instead, SWIFT II has been automatically extended year-on-year. If any SWIFT III was to come, it would establish a complementary cooperation on European financial data under an EU TFTS. Such a system is not *a priori* inaccordable with the rights to privacy and data protection, but has to meet the strict criteria established in CJEU case law. In fact, the Court has again demonstrated in its latest opinion on the EU Canada PNR Agreement that it does not shy back from taking on the role of a 'co-legislator'; this will make negotiations with the U.S. even more challenging.[367] Furthermore, an EU TFTS cannot be established on the basis of qualified majority voting but requires unanimity in the Council.

Nevertheless, an EU TFTS and SWIFT III would not remedy the continuous violation of European fundamental rights inherent to SWIFT II. Despite the Lisbon Treaty having established CJEU jurisdiction in matters of the AFSJ (art.276 TFEU), SWIFT II is *de facto* immune due to the exceptional legal character of international agreements in EU law:

Generally, the judicial review of international agreements is limited to the *ex ante* mechanism of art.218 para.9 TFEU. This procedure was used in case of the PNR Canada Agreement and is aimed at preventing the EU from entering international obligations contrary to EU internal standards as well as from damaging international relations. Evidently, the Court cannot be asked to give an opinion on SWIFT II after its entry into force in 2010. Nevertheless, even at the later stage of implementation, an international agreement can be scrutinised by the Court. According to arts.263f. TFEU, the Court can annul EU legislative acts and acts of the Council *ex post* if they fail to comply with primary law. Here, the acts of adoption as well as the Council's

[366] Apparently, the Article 29 Working Party was expecting a renewal: Letter from Isabelle Falque-Pierrotin to Rihards Kozlovskis (23 March 2015).
[367] By analogy: Hielke Hijmans, 'PNR Agreement EU-Canada Scrutinised: CJEU Gives Very Precise Guidance to Negotiators' (2017) 3 EDPL 406, 410.

negotiation mandate for the Commission could be subject to the Court's jurisdiction. However, any action of annulment would be inadmissible due to the limited application period of two months from the publication of the agreement's wording in 2010 (art.263 para.6).

As pointed out before, action of annulment could also be filed against Europol's monthly approvals (as well as the EDPS' rejection of an individual complaint, respectively).[368] Assuming that the Court could scrutinise the SWIFT II Agreement regarding its conformity with European fundamental rights (despite the principle of originator's control), any decision of annulment would be limited to the impugned Europol decision but could not affect the validity of the agreement itself. In fact, if Europol was prevented from issuing any further approval, it would end the data transfer immediately but at the same time possibly constitute a breach of the agreement on behalf of the EU (art.21). The same applies to bans of processing issued by the EDPS in effectuation of the oversight competences in art.43 Europol Regulation.

Therefore, art.265 TFEU might be an available option, basically imposing similar admissibility requirements as art. 263 paras.1 and 4 TFEU but focussing on the Commission's failure to terminate the agreement according to art.21 para.2 or to renegotiate the cooperation under art.23 para.2. It could be argued here that the general discretion of the Commission regarding external action is reduced because of the severe infringements of arts.7 and 8 CFR resulting from the TFTP's practice. Despite scholars suggested that the Court might be apprehensive to interfere with the Commission's perorogative as to 'political questions',[369] the *EU Canada PNR* opinion seems to prove the opposite.

However, it appears unlikely that the Agreement could be suspended immediately on grounds of breach of contract on behalf of the UST (art.21 para.1) referring to the UST's restrictive interpretation of individual rights; the EU was informed about this since the second Joint Review in 2014 and should have been aware of it well

[368] According to art.263 para.5 TFEU in connection with art.47 Europol Regulation, administrative redress with the EDPS is to be exhausted before filing a case to the Court: cf. Möstl, *supra* no.347, 33 as to the former JSB.
[369] Elaine Fahey, 'Challenging EU-US PNR and SWIFT law before the Court of Justice of the European Union', in: Patryk Pawlak (ed), *The EU-US Security and Justice Agenda in Action* (ISS 2011), 55ff.

before because the UST Representations from 2007 already displayed the UST's particular understanding of access and rectification rights. Consequently, respective claims would *venire contra factum proprium*. The Agreement still could be terminated according to art.21 para.2 requiring a notification of the U.S. six months in advance. In any case, however, data transferred to the U.S. so far could be further processed under the conditions of SWIFT II as stipulated in art.21 para.4 thereof.

Thus, the situation for affected individuals remains extremely unsatisfactory. If an EU TFTS/SWIFT III as described in chapter 3 could serve as an example of 'best practice', prompting the U.S. to adjust SWIFT II accordingly, is rather doubtful. Whilst it certainly would upgrade the EU as a counter-terrorism actor, its effectiveness in enhancing EU security is as uncertain as the TFTP's. On the other hand, it would contribute to the growing Panopticon people in Europe are exposed to at the national and the European level. Therefore, as the EDPS pointed out repeatedly,[370] the case still has to be demonstrated.

[370] *Supra* no.287.

BIBLIOGRAPHY

Books and Chapters

Ambrock, Jens, *Die Übermittlung von SWIFT-Daten an die Terrorismusaufklärung der USA* (Berlin, Duncker & Humblot, 2013)

Amelung, Knut, 'Zwangsbefugnisse für Europol?", in: Hans Hilger, Josef Ruthig, Wolf-Rüdiger Schenke, Jürgen Wolter, Mark A. Zöller (eds), *Alternativentwurf Europol und europäischer Datenschutz* (Heidelberg, C.F. Müller, 2008)

Basu, Aparna, 'Social Network Analysis: A Methodology for Studying Terrorism', in: Mrutyunjaya Panda, Satchidananda Dehuri and Gi-Nam Wang (eds), *Social Networking: Mining, Visualization and Security* (Springer International Publ., 2014), 215-242

Bittner, Stephan, 'Zwangsmittel im Recht der Europäischen Union: Geteilte Rechtsmacht in Europa', in: Manfred Zuleeg (ed), *Europa als Raum der Freiheit, der Sicherheit und des Rechts* (Baden-Baden, Nomos, 2007), 9-24

Blanke, Hermann-Josef and Mangiameli, Stelio (eds) *The Treaty on European Union (TEU): a commentary* (Heidelberg New York Dordrecht London, Springer, 2013)

Bonfanti, Matteo E., 'Collecting and Sharing Intelligence on Foreign Fighters in the EU and its Member States: Existing Tools, Limitations and Opportunities", in: Andrea de Gutty, Francesca Capone and Christophe Paulussen (eds), *Foreign Fighters under International Law and Beyond* (T.M.C. Asser Press 2016), 333-353

Bures, Oldrich, 'Europol's Counter-terrorism Role: A Chicken-Egg Dilemma', in: Christian Kaunert and Sarah Léonard (eds), *European Security, Terrorism and Intelligence: Tackling New Security Challenges in Europe* (Palgrave Macmillan, 2013), 65-95

Callies, Christian, 'Die Europäisierung der Staatsaufgabe Sicherheit unter den Rahmenbedingungen des freiheitichen Rechtsstaats', in: Erwin Müller and Patricia Schneider (eds), *Die Europäische Union im Kampf gegen den Terrorismus: Sicherheit vs. Freiheit?* (Baden-Baden, Nomos, 2006), 83ff.

Callies, Christian and Ruffert, Matthias (eds), *EUV/AEUV* (5th edn, München, C.H. Beck, 2016), thereof

- Callies 'EU-Vertrag (Lissabon) Art. 4 [Zuständigkeiten der Union, nationale Identität, loyale Zusammenarbeit]'

- Rossi, Matthias, 'AEUV Art.73 [Zusammenarbeit der Mitgliedstaaten]'

- Rossi, Matthias, 'AEUV Art.352 [Flexibilitätsklausel]'

Casagran, Cristina Blasi, *Global Data Protection in the Field of Law Enforcement* (London New York, Routledge, 2016)

- 'The New Europol Legal Framework: Implications for EU Exchanges of Information in the Field of Law Enforcement', in: Maria O'Neill and Ken Swinton (eds.), *Challenges and Critiques of the EU Internal Security Strategy* (Cambridge, Cambridge Scholars, 2017), 149-169

Fahey, Elaine, 'Challenging EU-US PNR and SWIFT law before the Court of Justice of the European Union', in: Patryk Pawlak (ed), *The EU-US Security and Justice Agenda in Action* (ISS, 2011), 55-66

Fahey, Elaine and Curtin, Deidre (eds), *A transatlantic community of law: legal perspectives on the relationship between the EU and US legal orders* (Cambridge, Cambridge University Press, 2014), thereof:

- Santos Vara, Juan, 'Transatlantic counterterrorism cooperation agreements on the transfer of personal data. A test for democratic accountability in the EU', 256-288

- Mitsilegas, Valsamis, 'Transatlantic counterterrorism cooperation and European values. The elusive quest for coherence', 289-315

Hansjörg Geiger, 'Rechtliche Grenzen der Europäisierung nachrichtendienstlicher Aufgaben' in: Thomas Jäger and Anna Daun (eds), *Geheimdienste in Europa Transformation, Kooperation und Kontrolle* (Wiesbaden, VS Verlag, 2009), 240-264

de Goede, *Marieke, Speculative Security: The Politics of Pursuing Terrorist Monies* (Minneapolis London, University of Minnesota Press, 2012)

Grabitz, Eberhard, Hilf, Meinhard and Nettesheim, Martin (ed), *Das Recht der Europäischen Union: EUV/AEUV* (60th edn, München, C.H. Beck, 2016), thereof:

- von Bogdandy, Armin and Schill, Stephan, 'EUV Art. 4 Prinzipien der föderativen Grundstruktur' (31 EL 2013)

- Oliver Dörr, 'AEUV Art. 276 [Unzuständigkeit des EuGH für mitgliedstaatliche Polizeimaßnahmen]' (60 EL 2016)

Grabitz, Eberhard, Hilf, Meinhard and Nettesheim, Martin (ed), *Das Recht der Europäischen Union: EUV/AEUV* (61st edn, München, C.H. Beck, 2017), thereof:

- Röben, Volker, 'AEUV Art. 72 Nationale Zuständigkeiten'

von der Groeben, Hans, Schware, Jürgen and Hatje, Armin, *Europäisches Unionsrecht* (7th edn, München, C.H. Beck 2015), thereof:

- Obwexer, Walter, 'EUV Artikel 4 [Zuständigkeiten der Union]'
- Breitenmoser, Stephan and Weyeneth, Robert, 'AEUV Artikel 72'
- Spaeth, Elena, 'AEUV Artikel 88 (ex-Artikel 30 EUV) [Europol]'

Gruszczak, Artur, *Intelligence Security in the European Union* (London, Palgrave Macmillan, 2016)

Hartley, T. C., *The foundations of European Union law: an introduction to the constitutional and administrative law of the European Union* (7th edn, Oxford, Oxford University Press, 2010)

Ester Herlin-Karnell, *The constitutional dimension of European criminal law* (Oxford and Portland, Oregon, Hart Publ., 2012)

Hinarejos, Alicia, 'Law and order and internal security provisions in the Area of Freedom, Security and Justice: before and after Lisbon', in: Christina Eckes and Theodore Konstadinides, *Crime within the Area of Freedom, Security and Justice* (Cambridge, Cambridge University Press, 2011), 249-271

Kau, Marcel, 'Justice and Home Affairs in the European Constitutional Process – Keeping the Faith and Substance of the Constitution', in: Stafan Griller and Jacques Ziller (eds), *The Lisbon Treaty* (Springer 2008), 223-234

Loideain, Nora Ni, 'Surveillance of Communications Data and Article 8 of the European Convention on Human Rights', in: Serge Gutwirth, Ronald Leenes and Paul de Hert (eds) *Reloading Data Protection* (Dordrecht Heidelberg London New York, Springer, 2014), 183-209

Mitsilegas, Valsamis, *EU Criminal Law after Lisbon. Rights, Trust and the Transformation of Justice in Europe* (Hart Publ., 2016)

Möller, Carolin, *The Evolution of Data Protection and Privacy in the Public Security Context – An Institutional Analysis of Three EU Data Retention and Access Regimes* (PhD thesis, 2017)

Möstl, Markus, *Die staatliche Garantie für die öffentliche Sicherheit und Ordnung: Sicherheitsgewährleistung im Verfassungsstaat, im Bundesstaat und in der Europäischen Union* (Tübingen, Mohr Siebeck, 2002)

- 'Grundfragen Europäischer Polizeilicher Kooperation', in: Dieter Kugelmann (ed) *Migration, Datenübermittlung und Cybersicherheit* (Baden-Baden, Nomos, 2016), 9-36

Pechstein, Matthias, Häde, Uwe and Nowak, Carsten (eds), *Frankfurter Kommentar zu EUV, GRC und AEUV* (Tübingen, Mohr Siebeck, 2017), thereof:

- Müller-Graf, Peter-Christian, 'Artikel 72 AEUV [Nicht berührte Zuständigkeiten der Mitgliedtstaaten]'

- Müller-Graf, Peter-Christian, 'Artikel 73 AEUV [Zusammenarbeit der Mitgliedstaaten in eigener Verantwortung]'

Peers, Steve, *EU justice and home affairs law* (3rd edn, Oxford, Oxford University Press 2011)

Piris, Jean-Claude, *The Lisbon Treaty: a legal and political analysis* (Cambridge, Cambridge University Press, 2010)

Rijpma, Jorrit J., 'Frontex and the European System of Border Guards. The future of European Border Management', in: Maria Fletcher, Ester Herlin-Karnell and Claudio Matera (eds), *The European Union as an Area Freedom, Security and Justice* (Routledge 2017), 217ff.

Schöndorf-Haubold, Bettina, 'Europäisches Sicherheitsverwaltungsrecht, § 35', in: Jörg Philipp Terhechte (ed.), *Verwaltungsrecht in der Europäischen Union* (Baden-Baden, Nomos, 2011), 1212ff.

Scott, Susan V. and Zachariadis, Markos, *The Society for Worldwide Interbank Financial Telecommunication (SWIFT). Cooperative governance for network innovation, standards, and community* (Abington and New York, Routledge, 2014)

Stalla-Bourdillon, Sophie, Papadaki, Evangelia and Chown, Tim, 'Metadata, Traffic Data, Communications Data, Service Use Information… What Is the Difference? Does the Difference Matter? An Interdisciplinary View from the UK', in: Gutwirth, Serge, Leenes, Ronald and De Hert, Paul (eds), *Data Protection on the Move:*

Current Developments in ICT and Privacy/Data Protection (Dordrecht Heidelberg New York London, Springer, 2016), 437-463

Tzanou, Maria, *The Fundamental Right to Data Protection, Normative Value in the Context of Counter-Terrorism Surveillance* (Hart Publ. 2017)

Wesseling, Mara, *The European Fight against Terrorism Financing, Professional Fields and New Governing Practices* (Boxpress, 2013)

Wolff, Heinrich Amadeus, 'BDSG 2018 § 45 Anwendungsbereich', in: Wolff and Stefan Brink (eds), *BeckOK Datenschutzrecht* (24th edn, C.H. Beck 2018)

Woods, Lorna, Watson, Philippa, Costa, Marios and Steiner, Josephine, *Steiner & Woods EU law* (13th edn, Oxford, Oxford University Press, 2017)

Periodicals and Papers

Abazi, V., "The future of Europol's parliamentary oversight: a great leap forward?' (2014) German Law Journal Vol.15 Issue 6, 1121-1144

Amicelle, Anthony, 'The Great (Data) Bank Robbery: Terrorist Finance Tracking Program and the 'Swift Affair'' (2011) Questions de recherche / Research Questions, Centre d'études et de recherches internationales (CERI-Sciences Po/CNRS) <https://ssrn.com/abstract=2282627> accessed 07 July 2017

- 'The EU's Paradoxical Efforts at Tracking the Financing of Terrorism: From criticism to imitation of dataveillance' (2013) CEPS Paper in Liberty and Security in Europe No. 56 / August 2013 <https://www.ceps.eu/publications/eu%E2%80%99s-paradoxical-efforts-tracking-financing-terrorism-criticism-imitation-dataveillance> accessed 07 July 2017

Argomaniz, Javier, 'The Passenger Name Records Agreement and the European Union Internalisation of U.S. Border Security Norms' (2009) Journal of European Integration Vol.31 Issue 1, 119-136

Ballaschk, Julia, 'In the Unseen Realm: Transnational Intelligence Sharing in the European Union – Challenges to Fundamental Rights and Democratic Legitimacy' (2015) Stanford Journal of International Law Vol.15 Issue 1, 19-51

Barabási, Albert-László, 'Scale-Free Networks: A Decade and Beyond' (2009) Science Vol.325 Issue 5939, 412-413

Basra, Rajan, Neumann, Peter R. and Brunner, Clausia, 'Criminal Pasts, Terrorist Futures: European Jihadists and the New Crime-Terror Nexus' (2016) The International Centre for the Study of Radicalisation and Political Violence (ICSR) <http://icsr.info/wp-content/uploads/2016/10/Criminal-Pasts-Terrorist-Futures.pdf> accessed 23 May 2018

Bates, Rodger A., 'Tracking Lone Wolf Terrorists' (2016) The Journal of Public and Professional Sociology Vol.8 Issue 1 Article 6

Bignami, Francesca, 'The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens' (2015), Study for the LIBE Committee, 2015; GWU Law School Public Law Research Paper No. 2015-54 <http://dx.doi.org/10.2139/ssrn.2705618> accessed 27 July 2017

- with Resta, Giorgio, ‘Transatlantic Privacy Regulation: Conflict and Cooperation’ (2015) Law and Contemporary Problems Vol.78 Issue 4, 231-266

Bloch-Wehba, Hannah C., ‘Global Governance in the Information Age: The Terrorist Finance Tracking Program’ (2013) New York University Journal of International Law & Politics Vol.45 Issue 2 595-640

Boehm, Franziska and Cole, Mark D., ‘Data Retention after the Judgement of the Court of Justice of the European Union’ (2014), <http://www.zar.kit.edu/DATA/veroeffentlichungen/237_237_Boehm_Cole-Data_Retention_Study-June_2014_1a1c2f6_9906a8c.pdf> accessed 12 March 2017

Bohannon, John, ‘Investigating Networks: The Dark Side’ (2009) Science Vol.325 Issue 5939 410-412

Bulloch, David B., ‘Tracking Terrorist Finances: The ‘SWIFT’ Program and the Amercian Anti-terrorist Finance Regime’ (2011) Amsterdam Law Forum Vol.3 Issue 4, 74-101

Cameron, Iain, ‘Balancing data protection and law enforcement needs: Tele2 Sverige and Watson’ (2017) Common Market Law Review Vol.54 Issue 5. 1467-1495

Cocq, Céline C., ‘EU Data Protection Rules Applying to Law Enforcement Activities: Towards an Harmonised Legal Framework?’ (2016) New Journal of European Criminal Law Vol.7 Issue 3, 263-276

Cole, Mark D. and Vandendriessche, Annelies, ‘From Digital Rights Ireland and Schrems in Luxembourg to Zakharov and Szabo/Vissy in Strasbourg’ (2016) European data Protection Law Review Vol.2 Issue 1, 121-129

- with Quintel, Teresa, ‘Data Protection under the Proposal for an EU Entry?Exit System (EES) Analysis of the impact on and limitations for the EES by Opinion 1/15 on the EU/Canada PNR Agreement of the Court of Justice of the European Union’ (October 2017) <https://orbilu.uni.lu/bitstream/10993/35446/1/Legal%20Opinion.PDF> accessed 07 June 2018

Connorton, Patrick M., ‘Tracking Terrorist Financing Thorugh SWIFT: When U.S. Subpoenas and Foreign Privacy Law Collide’ (2007) Fordham Law Review Vol.76 Issue 1, 283-322

Coudert, F., ‘The Europol Regulation and Purpose Limitation: From the „Silo-Based Approach’ to… What Exactly?’ (2017) European Data Protection Law Review Vol.3 Issue 3, 313-324

Cremona, Marise, ‘Justice and Home Affairs in a Globalised World: Ambitions and Reality in the tale of the EU-US SWIFT Agreement’ (2011) Institute for European Integration Research, Working Paper 04/2011, March 2011 <https://eif.univie.ac.at/downloads/workingpapers/wp2011-04.pdf> accessed 03 March 2017

Cross, Mai’a K. Davis, ‘A European Transgovernmental Intelligence Network and the Role of IntCen’ (2013) Perspectives on European Politics and Society Vol.14 Issue 3, 388-402

Drewer, Daniel and Miladinova, Vesela, ‘The BIG DATA Challenge: Impact and opportunity of large quantities of information under the Europol Regulation’ (2017) Computer Law & Securitz Review Vol.33 Issue 3 298-308

Federico Fabbrini, ‘Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States’ (2015) Harvard Human Rights Journal Vol.28 ,65-96

Fahey, Elaine, ‘Law and Governance as Checks and Balances in Transatlantic Security: Rights, Redress, and Remedies in EU-US Passenger Name Records and the Terrorist Finance Tracking Program’ (2013) Yearbook of European Law Vol.32 Issue 1, 368-388

Forde, Aidan, ‘The Conceptual Relationship Between Privacy and Data Protection’ (2016) Cambridge Law Review Vol.1, 135-149

Gaub, Florence and Lisiecka, Julia, ‘The crime-terrorism nexus’, EUISS Brief Issue 10/2017
<https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_10_Terrorism_and_crime.pdf> accessed 13 April 2018

Gellman, Barton, Blustein, Paul and Linzer, Dafna, ‘Bank Records Secretly Tapped’ The Washington Post (Washington, 23 June 2006)

Giegerich, Thomas, ‘Europäische Vorreiterrolle im Datenschutzrecht: Neue Entwicklungen in der Gesetzgebung, Rechtsprechung und internationalen Praxis der EU’ (2016) Zeitschrift für Europarechtliche Studien Heft 3/2016, 301-343

De Goede, Marieke, ‘The SWIFT Affair and the Global Politics of European Security’ (2012) Journal of Common Market Studies Vol.50 Issue 2, 214-230

- with Sullivan, Gavin, ‘The politics of security lists’ (2016) Environment and Planning D: Society and Space Vol.34 Issue 1, 67-88

- with Wesseling, Mara, ‘Secrecy and security in transatlantic terrorism finance tracking’ (2017) Journal of European Integration Vol.39 Issue 3, 253-269

Gonzalez Fuster, Gloria, de Hert, Paul and Gutwirth, Serge, ‘SWIFT and the vulnerability of transatlantic data transfers’ (2008) International Review of Law Computers and Technology Vol.22 Nos.1-2, 191-202

- with Gutwirth, Serge, Szekely, Ivan and Uszkiewicz, Eric, ‘PRIvacy and Security MirrorS: Towards a European framework for integrated decision making. Deliverable 5.1: Discussion paper on legal approaches to security, privacy and personal data protection’ (2013) <http://prismsproject.eu/wp-content/uploads/2012/06/PRISMS-D5-1-Legal-approaches.pdf> acessed 25 May 2017

- ‘Fighting for Your Right to What Exactly – The Convoluted Case Law of the EU Court of Justice on Privacy and/Or Personal Data Protection’ (2014) Birkbeck Law Review Vol.2 Issue 2, 263-278

Grief, Nicholas, ‘EU law and security’ (2007) European Law Review Vol.32 Issue 5, 752-765

Guastaferro, Barbara, ‘Beyond the Exceptionalism of Constitutional Conflicts: The Ordinary Functions of the Identity Clause’ (2016) Yearbook of European Law Vol.31 Issue 1, 263-318

Hijmans, Hielke, ‘PNR Agreement EU-Canada Scrutinised: CJEU Gives Very Precise Guidance to Negotiators’ (2017) European Data Protection Law Review Vol.3 Issue 3, 406-412

Kierkegaard, Sylvia, ‘US war on terror EU SWIFT(ly) signs blank cheque on EU data’ (2011) Computer Law & Security Review Vol.27 Issue 5, 449-570

Kokott, Juliane and Sobotta, Christoph, ‘The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR’ (2013) International Data Privacy Law Vol.3 Issue 4, 222-228

Lichtblau, Eric and Risen, James, ‘Bank Data Is Sifted by U.S. in Secret to Block Terror’ The NY Times (New York, 23 June 2017)

Lowe, David, ‘The European Union’s Passenger Name Record Data Directive 2016/681: Is it Fit for Purpose?’ (2017) International Criminal Law Review Vol.17 Issue 1, 78-106

Mbioh, Will R., ‘The TFTP Agreement, Schrems Rights, and the Saugmandsgaard Requirements’ (2016) Journal of Internet Law Vol.20 Issue 6, 29-38

Meyer, Josh and Miller, Greg, ‘U.S. Secretly Tracks Global Bank Data’ LA Times (Los Angeles, 23 June 2006)

Milaj, Jonida and Kaiser, Carolin, ‘Retention of data in the new Anti-money Laundering Directive—‘need to know’ versus ‘nice to know’’ (2017) International Data Privacy Law Vol.7, Issue 2, 115-125

Mitsilegas, Valsamis, ‘The Transformation of Privacy in an Era of Pre-emptive Surveillance’ (2015) Tilburg Law Review Vol.20 Issue 1, 35-57

- ‘Surveillance and digital privacy in the transatlantic "war on terror": the case for a global privacy regime’ (2016) Columbia Human Rights Law Review Vol.47, 1-77

Müller-Wille, Björn, ‘The Effect of International Terrorism on EU Intelligence Co-operation’ (2008) Journal of Common Market Studies Vol.46 Issue 1, 49-73

Murphy, Maria Helen, ‘Algorithmic surveillance: the collection conundrum’ (2017) International Review of Law, Computers & Technology Vol.31 Issue 2, 225-242

Nesterova, Irena, ‘Crisis of Privacy and Sacrifice of Personal Data in the Name of National Security: The CJEU Rulings Strengthening EU Data Protection Standards’ (January 31, 2017). European Society of International Law (ESIL) 2016 Annual Conference (Riga). <http://dx.doi.org/10.2139/ssrn.2911999> accessed 13 November 2017

Occhipinti, John D., ‘Still Moving Toward a European FBI? Re-Examining the Politics of EU Police Cooperation’ (2015) Intelligence and National Security Vol.30 Issue 2-3, 234-258

Ojanen, Tuomas, ‘Making the Essence of Fundamental Rights Real: The Court of Justice of the European Union Clarifies the Structure of Fundamental Rights under the Charter’ (2016) European Constitutional Law Review Vol.12 Issue 2, 318-329

Palmisano, Michael, ‘The Surveillance Cold War: Recent Decisions of the European Court of Human Rights and their Application to Mass Surveillance in the United States and Russia’ (2017) Gonzaga Journal of International Law Vol.20, 75-102

Pfisterer, Valentin, ‘The Second SWIFT Agreement Between the European Union and the United States of America – An Overview’ (2010) German Law Journal Vol.11 No.10, 1173-1190

Powell, Kenton and Chen, Greg, ‘Three degress of separation’ (The Guardian, 1 November 2013) <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1> accessed 02 May 2018

Richards, Neil M., ‘The Dangers of Surveillance’ (2013) Harvard Law Review Vol.126 Issue 7, 1934-1964

Ripoll Servent, Ariadna and MacKenzie, Alex, ‘Is the EP Still a Data Protection Champion? The Case of SWIFT’ (2011) Perspectives on European Politics and Society Vol.12 No.4, 390-406

Mary DeRosa, Data Mining and Data Analysis for Counterterrorism (CSIS March 2004) <https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/040301_data_mining_report.pdf> accessed 18 March 2017

Roßnagel, Alexander, ‘Neue Maßstäbe für den Datenschutz in Europa aus dem EuGH-Urteil zur Vorratsdatenspeicherung’ (2014) Multimedia und Recht, 372-377

Sandhu, Aqilah, ‘Anmerkung zum Urteil des EuGH vom 21.12.2016 in der Rs. C-203/15 (Tele2)’ (2017) Europarecht Vol.52 Heft 3, 453ff

Suda, Yuko, ‘Transatlantic Politics of Data Transfer: Extraterritoriality, Counter-Extraterritoriality and Counter-Terrorism’ (2013) Journal of Common Market Studies Vol.51 Issue 4, 772-788

Tracol, Xavier, ‘The judgment of the Grand Chamber dated 21 December 2016 in the two joint Tele2 Sverige and Watson cases: The need for a harmonised legal framework on the retention of data at EU level’ (2017) Computer Law & Security Review Vol.33 Issue 4, 541-553

Tzanou, Maria, ‘Is Data Protection the Same as Privacy? An Analysis of Telecommunications’ Metadata Retention Measures’ (2013) Journal of Internet Law Vol17 no.3, 21-34

- ‘European Regulation of Transatlantic Data Transfers and Online Surveillance’ (2017) Human Rights Law Review Vol.17, 545-565

Vedaschi, Arianna, ‘Privacy and data protection versus national security in transnational flights: the EU-Canada PNR agreement’ International Data Privacy Law 2018 Vol.8 No.2, 124-139

Vranken, Jan, 'Exiting Times for Legal Scholarship' (2012) Recht en Methode in onderzoek en onderwijs Vol.2, 42ff

Wesseling, Mara, de Goede, Marieke and Amoore, Louise, 'Data Wars Beyond Surveillance: Opening the black box of Swift' (2012) Journal of Cultural Economy Vol.5 Issue 1 (2012), 49-66

- 'Evaluation of EU measures to combat terrorist financing' (In-depth Analysis for the LIBE Committee, EU 2014) <http://www.europarl.europa.eu/RegData/etudes/note/join/2014/509978/IPOL-LIBE_NT(2014)509978_EN.pdf> acccessed 18 February 2017

- 'An EU Terrorist Finance Tracking System' (Occasional Paper, RUSI September 2016) <https://rusi.org/sites/default/files/op_wesseling_an_eu_terrorist_finance_tracking_system.1.pdf> accessed 18 February 2017

Weyemberg, Anne, Armada, Inès and Brière, Chloé 'Competition or Cooperation? State of Play and Future Perspectives on the Relations Between Europol, Eurojust and the European Judicial Network' (2015) New Journal of European Criminal Law Vol.6 Issue 2, 258-287

Winkler, Daniela, 'Vergangenheit und Zukunft der Flexibilitätsklausel im Spannungsfeld von unionalem Integrations- und mitgliedstaatlichem Souveränitätsanspruch - Eine Analyse von Artikel 352 AEUV unter dem Eindruck des BVerfG-Urteils zu "Lissabon"' (2011) Europarecht No.3/2011, 384-404

Cases

Court of Justice of the European Union

ECJ, Case C-8/73 *Hauptzollamt Bremerhaven v. Massey-Ferguson* ECR 897

ECJ Opinion 2/94, *Accession of EC to ECHR* [1996] ECLI:EU:C:1996:140

Joined Cases C 465/00, C 138/01 and C 139/01 *Österreichischer Rundfunk and Others* [2003] ECR I-4989

Joined Cases C-317/04 and C-318/04 *European Parliament v Council of the European Union and Commission of the European Communities* [2006] ECR I-04721

Case C-553/07 *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer* [2009] ECLI:EU:C:2009:293

Case C-301/06 *Ireland v European Parliament and Council of the European Union* [2009] ECLI:EU:C:2009:68

Case C-145/09 *Land Baden-Württemberg v Panagiotis Tsakouridis* [2010] ECLI:EU:C:2010:708

C‑518/07 *Commission v. Germany* [2010] ECLI:EU:C:2010:125

Case C-300/11 ZZ v Secretary of State for the Home Department [2013] ECLI:EU:C:2013:363

Case C‑288/12 *Commission v. Hungary* [2014] ECLI:EU:C:2014:237

Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Others v Minister for Communications, Marine and Natural Resources and Others* [2014] ECLI:EU:C:2014:238; Opinion of Advocate General Villalón (abbrev.: *DRI*)

Case C-362/14 *Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650; Opinion of Advocate General Bot (abbrev.: *Schrems*)

Joined Cases C-203/15 and C-698/15 *Tele2 Sverige and Secretary of State for the Home Department v Post- och telestyrelsen and Others* [2016] ECLI:EU:C:2016:970; Opinion of Advocate General Saugmandsgaard (abbrev.: *Tele2*)

Opinion 1/15 *EU-Canada PNR-Agreement* [2017] ECLI:EU:C:2016:656; Opinion of Advocate General Mengozzi (abbrev.: *PNR Canada*)

Case T-670/16 *Digital Rights Ireland v. Commission* (2017) ECLI:EU:T:2017:838

European Court of Human Rights

Weber and Saravia v. Germany ECHR 2006-XI 309

Liberty and Others v. The United Kingdom App. No. 58243/00 (ECtHR, 01 July 2008)

S. and Marper v. The United Kingdom ECHR 2008-V 167

M.K. v. France App. No.19522/09 (ECtHR, 18 April 2013)

Szabó and Vissy v. Hungary Appl. No. 37138/14 (ECtHR, 12 January 2016) (abbrev.: *Szabó*)

Zakharov v. Russia Appl. No. 47143/06 (ECtHR, 04 December 2015) (abbrev.: *Zakharov)*

10 Human Rights Organisations v. The United Kingdom App. No. 8170/13

German Bundesverfassungsgericht

BVerfGE 123, 267ff (*Lissabon-Urteil*)

Legislation

EU-Law

Commission, Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the U.S. Department of Commerce (2000/520/EC) [2000] OJ L215/7

Council Framework Decision of 13 June 2002 on combating terrorism [2002] OJ L164/3.

Agreement on mutual legal assistance between the European Union and the United States of America (EU-US) (adopted 25 June 2003, entered into force 01 January 2010) [2003] OJ L181/34

Agreement between the European Community and the United States of America on the Processing and Transfer of PNR Data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection (EU-US) (adopted 28 May 2004; out of force since 30/09/2006) [2004] OJ L183/84.

Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing [2005] OJ L309/15

Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) [2007] OJ L204/16

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 purposes of the Terrorist Finance Tracking Program (EU-US) (adopted 30 November 2009) [2010] OJ L8/11

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 (adopted 13 July 2010; entered into force 1 August 2010) [2010] OJ L195/5.

Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice [2011] OJ L 286/1

Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences (adopted 2 June 2016, in force since 1 February 2017) [2016] OJ L336/3.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89

Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime; all published in [2016] OJ L119/132

Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA [2016] OJ L135/53

Commission, Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield [2016] OJ L207/1

U.S.

Presidential E.O. 13224 of 23 September 2001 on Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten To Commit, or Support Terrorism 66 FR 49079

Administrative Procedure Act, 5 U.S.C. Subchapter 2.

Freedom of Information Act, 5 U.S.C. § 552 (4) (B)

1974 US Privacy Act, 5 U.S.C. § 552a (g)(1), as amended by the 2015 Judicial Redress Act, 5 U.S.C. 552a note.

Policy Documents

EU Documents

Article 29 Working Party

- Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) (WP128) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2006/wp128_en.pdf> accessed 04 April 2017

- Letter from Jacob Kohnstamm (Art.29 Working Party) and Francesco Pizzetti (Working Party on Police and Justice) to Juan Fernando Lopez Aguilar (LIBE Committee) (25 June 2010) <http://ec.europa.eu/justice/article-29/documentation/other-document/files/2010/2010_06_25_letter_to_libe_en.pdf> accessed 17 April 2018 (abbrev.: Letter to LIBE)

- Letter from Paul Breitbarth to Reinhard Priebe (14 April 2011) <http://www.statewatch.org/news/2011/apr/eu-tftp-review-report-letter-priebe-re-review-report.pdf> accessed 06 April 2017

- Letter from Jacob Kohnstamm to Cecilia Malmström (29 September 2011) <file:///C:/Users/HP/Downloads/20110929_letter_to_commission_tfts_en.pdf> accessed 23 June 2018

- Letter from Isabelle Falque-Pierrotin to Rihards Kozlovskis (23 March 2015) <http://ec.europa.eu/justice/article-29/documentation/other-

document/files/2015/20150323__letter_of_the_art_29_wp_on_the_renewal_of_the_tftp_agreement_between_eu_and_us_.pdf> accessed 24 June 2018

Commission

- Impact Assessment accompanying the Proposal for a European Parliament and Council Directive on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (Staff Working Paper) SEC (2011) 132 final

- A European terrorist finance tracking system: available options COM(2011) 429 final (abbrev.: 2011 TFTS preliminary study)

- '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 17-18 February 2011' (Commission Staff Working Paper) SEC(2011) 438 final (abbrev.: 2nd Joint Review Report)

- A European terrorist finance tracking system (EU TFTS) COM(2013) 842 final (abbrev.: 2013 TFTS Study)

- Joint Report from the Commission and the U.S. Treasury Department regarding the value of TFTP Provided Data pursuant to Article 6 (6) of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messanging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, Annex to COM(2013) 843 final (abbrev.: Value Report)

- Joint Review Report 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 (Commission Staff Working Document) SWD(2014) 264 final (abbrev.: 3rd Joint Review Report)

- European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union COM (2016) 230 final

- Communication on an Action Plan for strengthening the fight against terrorist financing COM(2016) 50 final (abbrev.: 2016 Action Plan)

- Roadmap: A possible European system complementing the existing EU-US TFTP agreement (2016) <http://ec.europa.eu/smart-regulation/roadmaps/docs/2016_home_191_system_complementing_tftp__en.pdf> accessed 07 June 2018

- European Political Strategy Centre, ‘Towards a "Security Union" - Bolstering the EU's Counter-Terrorism Response’ EPSC Strategic Notes 12/2016

- Joint Review Report 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 Commission Staff Working Document SWD(2017) 17 final (abbrev.: 4th Joint Review Report)

- Eleventh progress report towards an effective and genuine Security Union COM (2017) 608 final

Council

- Discussion paper on the future Standing Committee on Internal Security (COSI) - Constitutional Treaty, art.III-261; 21/02/2005’ doc.6626/05

- 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 (2010) OJ L195/3

European Council

- Bratislava Declaration (16 September 2016) Decl. 517/16

European Data Protection Supervisor

- Opinion on the role of the European Central Bank in the SWIFT case [2007] <https://edps.europa.eu/sites/edp/files/publication/07-02-01_opinion_ecb_role_swift_en.pdf> accessed 06 March 2017

- Comments 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 of 25 January 2010 <https://edps.europa.eu/sites/edp/files/publication/10-01-25_eu_us_data_exchange_en.pdf> accessed 02 May 2018

- Opinion on the proposal for a 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 purposes of the Terrorist Finance Tracking Program (TFTP II) [2010] OJ C355/10

- EDPS comments on the Communication from the Commission to the European Parliament and the Council on a European Terrorist Finance Tracking System (TFTS) and on the Commission Staff Working

Document - Impact Assessment accompanying the Communication from the Commission to the European Parliament and the Council on a European Terrorist Finance Tracking System (TFTS) (2014) < https://edps.europa.eu/sites/edp/files/publication/14-04-17_tfts_comments_en.pdf> accessed 23 June 2018

- Opinion 5/2015 Second Opinion on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (24 September 2015), <https://edps.europa.eu/sites/edp/files/publication/15-09-24_pnr_en.pdf> accessed 01 May 2018

- Opinion 1/2016 Preliminary Opinion on the agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offences (12 February 2016), <https://edps.europa.eu/sites/edp/files/publication/16-02-12_eu-us_umbrella_agreement_en.pdf> accessed 06 July 2018

- Annual Report 2017 (2018) <https://edps.europa.eu/sites/edp/files/publication/18-03-15_annual_report_2017_en.pdf> accessed 23 April 2018

Europol

- Europol Activities in Relation to the TFTP Agreement - Information Note to the European Parliament (1 August 2010 – 1 April 2011) <http://www.statewatch.org/news/2012/jun/eu-usa-tftp-europol-2012.pdf> accessed 14 June 2017

- 2017 Consolidated Annual Activity Report (Public Version 2018) <file:///M:/consolidated_annual_activity_report_2017.pdf> accessed 13 June 2018

- TESAT European Union Terrorism Situation and Trend Report 2017 <file:///M:/tesat2017_0.pdf> 10 April 2018

Europol Joint Supervisory Body

- Report on the Inspection of Europol's Implementation of the TFTP Agreement, conducted in November 2010' <http://collections.internetmemory.org/haeu/20170706142918/http://europoljsb.europa.eu/media/111009/terrorist%20finance%20tracking%20program%20(tftp)%20inspection%20report%20-%20public%20version.pdf> accessed 02 May 2018

- Europol JSB Inspects for the Second Year the Implementation of the TFTP Agreement' <http://collections.internetmemory.org/haeu/20170706142918/http://europoljsb.europa.eu/media/205081/tftp%20public%20statement%20-%20final%20-%20march%202012.pdf> accessed 2 May 2018

European Union Agency for Fundamental Rights

- *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Mapping Member States' legal frameworks* (2015)

European Ombudsman

- Decision of the European Ombudsman closing the inquiry into complaint 1148/2013/TN against the European Police Office (Europol) of 02 September 2014 <https://www.ombudsman.europa.eu/de/cases/decision.faces/de/54678/html.bookmark> accessed 06 April 2017

EU Eminent Person Jean Louis Bruguière

- Summary of the First Annual Report on the Processing of EU Originating Personal Data by the United States Treasury Department for Counter-Terrorism Purposes [2008] <http://www.statewatch.org/news/2011/apr/eu-usa-tftp-swift-1st-report-2008-judge-bruguiere.pdf> accessed 02 May 2017

- Second Report on the Processing of EU-Originating Personal Data by the United States Treasury Department for Counter Terrorsim Purposes [2010] <http://www.statewatch.org/news/2010/aug/eu-usa-swift-2nd-bruguiere-report.pdf> accessed 02 May 2017

European Parliament

- Resolution on the interception of bank transfer data from the SWIFT system by the US secret services (P6_TA(2006)0317) [2006] OJ CE303/843

- Resolution on SWIFT, the PNR agreement and the transatlantic dialogue on these issues (P6_TA(2007)0039) [2007] OJ CE287/349

- 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 (P7_TA(2009)0016) [2010] OJ CE224/8

- LIBE, 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 (P7_A(2010)0224), 7f.

- Legislative Resolution of 11 February 2010 on the proposal for a 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

purposes of the Terrorist Finance Tracking Program (P7_TA(2010)0029) [2010] OJ C341E/100

- Resolution of 5 May 2010 on the Recommendation from the Commission to the Council to authorise the opening of negotiations for an agreement between the European Union and the United States of America to make available to the United States Treasury Department financial messaging data to prevent and combat terrorism and terrorist financing (P7_TA(2010)0143) [2010] OJ CE81/66

- Legislative resolution P7_TA(2010)0279 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 <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0279+0+DOC+XML+V0//EN> accessed 19 April 2018

- Resolution of 23 October 2013 on the suspension of the TFTP agreement as a result of US National Security Agency surveillance (2013/2831(RSP)) [2016] OJ C208/153

- Plenary Verbatim Record (10 February 2010) P7_CRE(2010)02-10

- Formal Sitting Verbatim Record (06 May 2010) P7_CRE(2010)OT-06

- Plenary Verbatim Record (12 April 2016) P8_CRE-REV(2016)04-12 (9)

- Legal Service, 'Legal Opinion on EU-US Umbrella agreement concerning the protection of personal data and cooperation between law enforcement authorities in the Eu and the US', Doc.no. SJ-0784/15 (2016)

U.S. Documents

US Congress

- The Terror Finance Tracking Program: Hearing before the Subcomm. on Oversight and Investigations of the Comm. on Financing Services, 119 Cong. 2nd Sess. (2006), Serial No.109-125

US Department of the Treasury

- Financial Crimes Enforcement Network, Feasibility of a Cross-Border Electronic Funds Transfer Reporting System under the Bank Secrecy Act (2006) <https://info.publicintelligence.net/CBFTFS_Complete.pdf> accessed 06 June 2017

- Processing of EU originating Data by United States Department for Counter Terrorism Purposes - SWIFT - Terrorist Finance Tracking Program - Representations of the United States Department of the Treasury [2007] OJ C166/18 (abbrev.: UST Representations)

- UST Disclosure Services, ‘Freedom of Information Act Handbook’ (July 2010)

- TFTP Redress Procedure <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Terrorist-Finance-Tracking/Documents/Revised%20Redress%20Procedures%20for%20Web%20Posting%20(8-8-11).pdf> accessed 3 July 2018

Belgium

Belgian Data Protection Commission

- Opinion No. 37/2006 of 27 September 2006 on the Transfer of Personal Data by the CSLR SWIFT by Virtue of UST (OFAC) Subpoenas (inofficial translation into English) (2006)

- Decision of 9 December 2008 (free translation) <https://www.privacycommission.be/sites/privacycommission/files/documents/swift_decision_en_09_12_2008.pdf> accessed 19 April 2018

United Kingdom

House of Lords

- The Treaty of Lisbon: An Impact Assessment. Volume I: Report (2008)

Council of Europe

European Commission for Democracy Through Law (Venice Commission)

- Report on the Democratic Oversight of Signals Intelligence Agencies, adopted by the Venice Commission at its 102nd Plenary Session (Venice, 20-21 March 2015) on the basis of comments by Mr Iain Cameron (Member, Sweden) (CDL-AD(2015)011) (Study No. 719/2013) (Strasbourg, 15 December 2015)

<u>Other</u>

Bhagat, Smriti, Burke, Moira, Diuk, Carlos, Filiz, Ismail Onur and Edunov, Sergey, ‘Three and a half degrees of separation’ (Facebook research, 2016) <https://research.fb.com/three-and-a-half-degrees-of-separation/> accessed 8 May 2017

Commission, ‘European Commission seeks high privacy standards in EU-US data protection agreement’ <http://europa.eu/rapid/press-release_IP-10-609_en.htm?locale=en> accessed 06 April 2017

Clerix, Kristof, ‘Ilkka Salmi, the EU's spymaster’ (04 March 2014) <https://www.mo.be/en/interview/ilkka-salmi-eu-s-007> accessed 29 June 2017

Korff, Douwe, ‘Expert Opinion prepared for the Committee of Inquiry of the Bundestag into the ‘5Eyes’ global surveillance systems revealed by Edward Snowden’ (Committee Hearing of 5 June 2014) <https://www.bundestag.de/blob/282874/8f5bae2c8f01cdabd37c746f98509253/mat_a_sv-4-3_korff-pdf-data.pdf> accessed 06 July 2018

- ‘EU-US Umbrella Data Protection Agreement: Detailed analysis by Douwe Korff’ (14 October 2015), <https://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/> accessed 21 November 2017.

Pop, Valentina, ‘MEP: Swift ‘secrecy’may hamper new data deals with US’ (28 February 2011) <https://euobserver.com/institutional/31880> accessed 17 April 2018

Schlamp, Hans-Jürgen, ‘EU to Allow US Access to Bank Transaction Data’ (spiegel online, 27 November 2009) <http://www.spiegel.de/international/europe/spying-on-terrorist-cash-flows-eu-to-allow-us-access-to-bank-transaction-data-a-663846.html> accessed 02 May 2018

SWIFT, ‘Highlights 2017’ <https://www.swift.com/about-us/highlights-2017> accessed 16 April 2018

- ‘SWIFT completes transparency improvements and obtains registration for Safe Harbor’ <https://www.swift.com/about-us/swift-and-data> accessed 04 April 2017

- ‘SWIFT announces plans for system re-architecture’ <https://www.swift.com/insights/press-releases/swift-announces-plans-for-system-re-architecture> accessed 04 April 2017