DATA PROTECTION CONFLICTS BETWEEN THE UNITED STATES AND THE EUROPEAN UNION IN THE WAR ON TERROR: LESSONS LEARNED FROM THE EXISTING SYSTEM OF FINANCIAL INFORMATION EXCHANGE

Matthew R. VanWasshnova[*]

INTRODUCTION

In the middle of 2006, two significant issues, both involving privacy and specifically data protection, came to the forefront of U.S. efforts in the War on Terror. First, in May 2006, the European Court of Justice (ECJ) annulled an agreement between the United States and the European Union regarding the transfer of airline passenger information—or passenger name records (PNR)—from the European Union to the United States.[1] The annulment of the PNR data transfer agreement by the ECJ reignited the debate as to whether the transfers violated E.U. data protection laws. The second major issue arose on June 24, 2006 when the *New York Times* uncovered a secret U.S. government financial record surveillance program called the Terrorist Finance Tracking Program (TFTP).[2] Details of the secret TFTP immediately raised concerns of data protection violations both in the United States and in the European Union.

Because terrorists reveal themselves to the international community only (1) when they travel abroad; or (2) when they transact abroad, both the PNR transfer and the TFTP represent noteworthy counter-terrorism efforts by the United States. Clearly, however, the annulment of the PNR data transfer agreement and disclosure of the TFTP to the international community have strained relations between the European Union and the United States. The European Union and the United States will be hard-pressed to improve relations unless the two governments can find common ground regarding the impact of their data protection policies on these two distinct problems. In order to find that common ground, this note recommends (1) that the United States terminate the TFTP and improve the existing system

---

[*] BA, University of Michigan (2003); JD, Case Western Reserve University School of Law (2008). I would like to thank Professors Richard Gordon and Carol Fox for their helpful thoughts and comments during the development of this Note. I would also like to thank my wife, Stacy, for all her patience and support. This Note is current as of September 24, 2007.

[1] Joined cases Case C-317/07 and C-318/04, European Parliament v. Council of the European Union (C-317/04) and European Parliament v. Comm'n of the European Communities (C-318/04), 2006 E.C.R. I-4721 [hereinafter European Parliament].

[2] Eric Lichtblau & James Risen, *Bank Date Sifted in Secret by U.S. to Block Terror*, N.Y. TIMES, June 23, 2006, at A1.

of financial information exchange to obtain the information that it needs for combating the financing of terrorism; and (2) that the United States apply the existing system of financial information exchange to the PNR data transfer process.

This Note seeks to adapt and apply the universally accepted system of financial information exchange that was first developed as an anti-money-laundering tool, and later embraced as a counter-terrorism finance instrument, to the PNR data transfer and TFTP issues introduced above. Therefore, it will address the transfer of airline passenger data alongside the current global model of sharing financial information in anti-money laundering and countering the financing of terrorism (AML/CFT) efforts. Part I analyzes the general distinctions between data privacy protection policies in the United States and European Union and examines the reasons underlying the conflicts addressed in Part II. Part II first sets out the background of PNR data transfers between the United States and European Union and the evolution of the subsequent conflict regarding the transfers. Part II then explores the TFTP and its alleged violations of E.U. data protection laws. Part III considers the existing AML/CFT approach to financial information exchange and its implementation in the United States and Europe. Remaining mindful of the delicate balance between security and privacy protection, Part IV recommends that (1) the United States and European Union follow the existing system of financial information exchange in sharing airline passenger information, and (2) the United States terminate the TFTP or restructure it so that it follows the AML/CFT model of sharing financial records.

I. E.U. AND U.S. DATA PROTECTION LAWS

A. The E.U.'s Blanket Protection vs. the U.S.'s "Patchwork Quilt"

The European Union and the United States have taken two separate, and perhaps incompatible, paths in legislating data privacy.[3] The European Union aims to restrict the amount of data collected and to prevent the data from being used for purposes other than those for which they were collected.[4] The United States, on the other hand, allows broader data collection and storage.[5] Moreover, while the European Union has tightly woven a blanket data protection policy "covering the full spectrum of uses of personally identifiable information,"[6] the United States has stitched a "patchwork

---

[3] DOROTHY HEISENBERG, NEGOTIATING PRIVACY 14 (2005).

[4] *Id.*

[5] *Id.*

[6] Beth Givens, *Privacy Expectations in a High Tech World*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 347, 348–49 (2000).

quilt"[7] of privacy legislation, legislating restrictions only where individual problems arise.[8] This basic difference between the data protection policies of the United States and the European Union is the root problem underlying the PNR data transfer and TFTP disputes outlined in Part II of this Note.

B. The European Union and the Data Protection Directive

In 1995, the European Parliament and the European Council passed Directive[9] 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive).[10] The Data Protection Directive "can be seen as a general framework legislative provision, which has as its principle aims: (1) the protection of an individual's privacy in relation to the processing of personal data; and (2) the harmonization of the data protection of the Member States."[11]

Another important principle of the Data Protective Directive is that personal data can be transferred only to countries outside of the European Union that guarantee an "adequate level of protection."[12] Thus, the Data Protection Directive has an extra-territorial effect because it prevents private and public sector entities within the European Union from transferring data to any countries outside of the European Union that provide inadequate data protection. In determining whether a foreign country affords an adequate level of protection, the Commission assesses the totality of the

> circumstances surrounding a data transfer operation . . . [with] particular consideration . . . given to the nature of the data, the purpose and proposed processing operation or operations, the country of origin and the country

---

[7] Robert Gellman, *Conflict and Overlap in Privacy Regulation: National, International and Private*, *in* BORDERS IN CYBERSPACE: INFORMATION POLICY AND THE GLOBAL INFORMATION INFRASTRUCTURE 255, 257 (Brian Kahin & Charles Nesson eds., 2d ed. 1998) (1987).

[8] *See*, *e.g.*, Fair Credit Reporting Act, 15 U.S.C. § 1681 (1994); Family Education and Privacy Rights Act, 20 U.S.C. § 1232(g) (1994); Right to Financial Privacy Act, 12 U.S.C. §§ 3401–22 (1994); Video Privacy Protection Act, 18 U.S.C. § 2710 (2000).

[9] A Directive is a piece of E.U. legislation that is addressed to Member States. PETER CAREY, DATA PROTECTION: A PRACTICAL GUIDE TO UK AND EU LAW 5 (2d ed. 2004). After the legislation is passed at the EU level, the Member States must ensure that its directive is applied in their own legal systems. *Id.*

[10] Council Directive 95/46/EC, 1995 O.J. (L 281) 1 (EC).

[11] CAREY, *supra* note 9, at 6.

[12] Council Directive 95/46/EC, art. 25, 1995 O.J. (L 281) 1, 20 (EC) ("Where the Commission finds . . . that a third country does not ensure an 'adequate' level of within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data."); *see also* HEISENBERG, *supra* note 3, at 31.

> of final destination, the rules of law . . . and the professional rules and security measures which are complied with in that country.[13]

When the European Commission (Commission) finds that a foreign country does not maintain an adequate level of protection, Member States are required to prevent any data from being transferred to that country and the Commission is required to enter into negotiations with the country to remedy the problem.[14]

A final major principle of the Data Protection Directive is its focus on oversight. For instance, Article 28 of the Data Protection Directive requires each Member State to establish an independent enforcement body.[15] Each Member State's independent authority must be consulted when the government drafts legislation relating to processing of personal data.[16] These independent authorities also have the power to conduct investigations, initiate legal proceedings, and hear claims pertaining to data protection violations.[17] In addition, Article 29 established the Article 29 Working Party, which advises the Commission on data protection and privacy matters.[18] The Article 29 Working Party is composed of a representative from each Member State, a representative of the Community, and a representative of the Commission.[19]

C. The Sectoral and Self-Regulatory Approach to Data Protection in the United States

While the European Union has focused specifically on data protection in the Data Protection Directive, U.S. privacy law refers to a more general right to privacy.[20] This is a direct result of the evolution of the U.S. right to privacy at common law,[21] which was necessitated by the failure of

---

[13] Council Directive 95/46/EC, art. 25, 1995 O.J. (L 281) 1, 20 (EC).

[14] *Id.* art. 25.

[15] *Id.* art. 28(1).

[16] *Id.* art. 28(2).

[17] *Id.* art. 28(3)–(4).

[18] *Id.* art. 29. Because the Data Protection Directive allows each Member State to implement the Data Protection Directive in different ways so long as all of the elements of the Data Protection Directive are included in the Member State's national law, the actions of the Article 29 Working Party constitute the primary EU-level involvement. HEISENBERG, *supra* note 3, at 27.

[19] Council Directive 95/46/EC, art. 29(2), 1995 O.J. (L 281) 1, 23 (EC).

[20] *See* HEISENBERG, *supra* note 3, at 32(citation omitted); Julia M. Fromholz, *The European Union Data Privacy Directive*, 15 BERKELEY TECH. L.J. 461, 470 (2000).

[21] *See* Barbara Crutchfield George et. al., *U.S. Multinational Employers: Navigating Through the "Safe Harbor" Principles to Comply with the EU Data Privacy Directive*, 38 AM. BUS. L.J. 735, 746–50 (2001).

the U.S. Bill of Rights to specifically provide for a fundamental right to privacy.[22] Because the term "privacy" can have various meanings in U.S. law, ranging from a woman's right to an abortion to a person's choice to keep or remove his or her name from a telemarketing list, a person has to scour a number of authorities—the "patchwork quilt"—to determine how any element of his or her data is protected in the United States.[23] This sectoral approach has at times left parts of the public inadequately protected from privacy infringements and is specifically problematic because technological developments render some legislation obsolete.[24]

The U.S. Congress has also applied protections unevenly between the public and private sectors. As shown by the Freedom of Information Act (FOIA)[25] and the Privacy Act of 1974,[26] the U.S. Congress has been willing to regulate the use of data in the public sector.[27] The Privacy Act of 1974, which amended the FOIA, protects a person's records[28] from government agency disclosure and requires that federal agencies establish "appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity."[29] Also under the Privacy Act of 1974, agencies must "establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records . . . ."[30] However, the fact that Congress deliberately chose not to extend the Privacy Act of 1974 to the private sector illustrates the general reluctance of the U.S. government to interfere in the affairs of individuals and businesses.[31]

---

[22] *Id.* at 741. The U.S. Supreme Court has, however, found an implicit fundamental right to privacy in certain circumstances. *Id.*

[23] Fromholz, *supra* note 20, at 470.

[24] HEISENBERG, *supra* note 3, at 32–33.

[25] The Freedom of Information Act, 5 U.S.C. 552 (2003). The FOIA permits any person, regardless of nationality or country of residence, access to a U.S. federal agency's records, unless one of the exemptions applies and protects the records in question from public disclosure. See 5 U.S.C 552(a)–(b). Under the FOIA, an agency must withhold a record, where (1) the information is confidential and commercial in nature, (2) "disclosure of [the information] would constitute a clearly unwarranted invasion of personal privacy," or (3) the information is "compiled for law enforcement purposes . . . to the extent that . . . [disclosure may] reasonably be expected to constitute an unwanted invasion of personal privacy." 5 U.S.C. §§ 552(b)(4), (6)–(7).

[26] The Privacy Act of 1974, 5 U.S.C. § 552a (Supp. IV 2000).

[27] George, *supra* note 21, at 747, n.52.

[28] Under the Privacy Act of 1974, a person's records means "any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history." The Privacy Act of 1974, 5 U.S.C. § 552a(a)(4) (Supp. IV 2000).

[29] *Id.* § 552a(e)(10).

[30] *Id.* § 552a(e)(9).

[31] *See* George, *supra* note 21, at 746–48.

Besides this "patchwork quilt" of data privacy legislation, the United States also relies on various forms of self-regulation, "in which companies and industry bodies establish codes of practice and engage in self-policing."[32] Like the sectoral approach, however, self-regulation is often criticized for being predominantly reactive, providing inadequate data protection, and failing to have sufficient independent oversight and enforcement mechanisms.[33]

When the European Council passed the Data Protection Directive in 1995, the Commission considered U.S. protection of European data inadequate because the United States did not have comprehensive privacy protections.[34] To enable the continuing free flow of commerce between the United States and the European Union, the two governments approved the Safe Harbor Principles—effective November 21, 2000.[35] In Decision 2000/520/EC, the Commission declares that the Safe Harbor Principles provide an adequate level of protection for the transfers of data from the European Union to the United States.[36] While the Safe Harbor Principles enable the free flow of information between the European Union and U.S. companies (i.e. commercial transactions),[37] they do not apply to transfers to government agencies.[38] Thus, after the Safe Harbor Principles had served to mend a portion of the U.S. "patchwork quilt" to the E.U. blanket Data Protection Directive, the stage was set for the two data privacy conflicts, which both involved data transfers from the European Union to U.S. government agencies.

II. THE TWO MAJOR TRANSATLANTIC DATA PRIVACY CONFLICTS IN 2006

A. PNR Transfers Between the United States and European Union

> *Some observers hailed [the ECJ airline passenger agreement annulment] decision as a triumph of E.U. privacy law for protecting passenger information and beating back the United States' post-September 11 efforts to*

---

[32] Privacy International, PHR 2005—Overview of Privacy (Oct. 10, 2006), http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-543673.

[33] *See*, *e.g.*, George, *supra* note 21, at 748.

[34] HEISENBERG, *supra* note 3, at 32.

[35] Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,666-01 (July 24, 2000); Commission Decision 2000/520/EC, Safe Harbor Privacy Principles, Annex, 2000 O.J. (L 215) 7, 10.

[36] Commission Decision 2000/520/EC, Safe Harbor Privacy Principles, Annex, art. 1, 2000 O.J. (L 215) 7, 8 (EC).

[37] *See generally*, Steven R. Salbu, *The European Union Data Privacy Directive and International Relations*, 35 VAND. J. TRANSNAT'L L. 655, 678–84 (2002) (describing the development, negotiation, and the nature of the Safe Harbor provisions).

[38] *See* HEISENBERG, *supra* note 3, at 141–42.

> *extend its jurisdictional reach in the name of national security. Others, however, have portrayed the ECJ as deciding the case on a technicality, laying the groundwork for the Commission and the U.S. negotiators to tweak the agreement only slightly—or the Commission simply to alter the legal grounds for entering in the agreement—and for the data transfer to continue as planned.*[39]

This section lays out the background of the passenger name record transfers from the European Union to the United States and explains how the latter observer's view in the quoted material above essentially has come to fruition, allowing for a continuation of the status quo—a status quo that many E.U. policymakers and privacy watchdogs feel provides the United States with unbridled access to the statutorily protected private information of European citizens.

1. Post-September 11th Legislation and the Creation of Conflict

On November 19, 2001, just two months after the September 11, 2001 terrorist attacks, the United States enacted the Aviation and Transportation Security Act of 2001 (ATSA).[40] ATSA requires all airline carriers operating to, from, or across U.S. territory to provide the U.S Customs and Border Protection Bureau (U.S. Customs) with electronic access to the PNR data contained in their reservation and departure control systems.[41] ATSA also provides that the information transmitted to U.S. Customs "may be shared with other Federal agencies for the purpose of protecting national security."[42] Airlines that did not comply with ATSA could be subject to fines or a revocation of landing rights.

2. European Reaction to ATSA and Subsequent Negotiations

As ATSA forced European commercial airlines to either violate the Data Protection Directive or pay substantial penalties as a result,[43] it created the first concrete transatlantic conflict over data privacy.[44] Although the Data Protection Directive does not apply to the processing of personal data in operations concerning public security, defense, and Member State securi-

---

[39] Henriette Tielemans et al., *The Transfer Of Airline Passenger Data to the U.S.: An Analysis of the ECJ Decision*, BNA INT'L WORLD DATA PROTECTION REP, June 2006, at 15.

[40] Aviation and Transportation Security Act of 2001, Pub. L. No. 107-71, 115 Stat. 597 (codified as amended in scattered section of 49 U.S.C.).

[41] 49 U.S.C. 44909(c) (Supp. IV 2000).

[42] *Id.*

[43] *See* HEISENBERG, *supra* note 3, 140–41.

[44] *See id.* at 140.

ty,[45] the PNR were "collected for a commercial purpose (flying abroad), and only subsequently exploited for national security information. . . . Hypothetically, if the data had been collected only for security purposes, they likely would have fallen under the security exemption that the national privacy laws have created for security and policing issues."[46]

After more than a year of initial talks between the Commission and U.S. officials and a postponement of the entry into force of the ATSA requirements, senior officials of the Commission and U.S. Customs met in Brussels in February 2003 to negotiate a solution to the conflict.[47] Although the parties failed to reach an agreement that fully reconciled the provisions of ATSA with the Data Protection Directive, they did issue a joint statement (Joint Statement).[48] The Joint Statement detailed the initial data protection undertakings agreed to by U.S. Customs and confirmed the parties' intention to pursue talks with a view of allowing the Commission to make an "adequacy finding" declaring U.S. data protection safeguards adequate in accordance with Article 25(6) of the Data Protection Directive.[49]

Ten months later, on December 16, 2003, in a communication (Communication) to the European Council and Parliament, the Commission presented its approach for the transfer of PNR data to the United States.[50] The legal framework called for a "light" bilateral agreement between the United States and the European Union and an "adequacy finding" by the Commission.[51] The Communication outlined a series of "undertakings" with the United States, whereby the United States had agreed to: (1) limit its PNR requests to a closed list of thirty-four items, (2) delete all categories of sensitive data, (3) use the data only to prevent and combat terrorism and related crimes, (4) retain the PNR data for no more than three and a half years, (5) receive and handle representations from E.U. data protection authorities on behalf of E.U. citizens who have outstanding complaints with the Department of Homeland Security, and (6) participate with an E.U. team

---

[45] Council Directive 95/46/EC, art. 3(2), 1995 O.J. (L 281) 1, 12 (EC).

[46] HEISENBERG, *supra* note 3, at 142.

[47] Press Release, European Commission/U.S. Customs Talk on Passenger Name Record (PNR) Transmission (July 2006), http://ec.europa.eu/comm/external_relations/us/intro/pnr.htm.

[48] Joint Statement, European Commission / US Customs talk on Passenger Name Record (PNR) Transmission, (February 17–18, 2003), http://ec.europa.eu/comm/external_relations/us/intro/pnr-joint03_1702.htm.

[49] *Id.*

[50] *Communication from the Commission to the Council and the Parliament, Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach*, COM (2003) 826 final (Dec. 12, 2003) [hereinafter *Communication*].

[51] *Id.* at 7.

led by the Commission in an annual joint review.[52] The Communication detailed the characteristics of a "push" system of data transfers, which means that the airlines would transmit the data to U.S. authorities, as opposed to the current "pull" system, which allows the United States access to the airline reservation systems, and envisioned "switching to 'push' with filters by the middle of 2004."[53] Finally, the Communication advocated that a multilateral approach to the PNR data transfer problem be developed and recommended that the International Civil Aviation Organization (ICAO)[54] was "the most appropriate framework" for bringing forth a multilateral initiative.[55]

3. Bilateral PNR Data Transfer Agreement

On May 14, 2004, the Commission, under Article 25(2) of the Data Protection Directive and in line with the Joint Statement and the Communication, found that U.S. Customs ensured an adequate level of protection for PNR data transferred from the European Union.[56] Subsequently, on May 17, 2004, the E.U. Council approved the conclusion of the PNR data processing and transfer agreement,[57] and on May 28, 2004, the United States and the European Union signed a definite agreement on the processing and transfer of the PNR data (Original Agreement).[58] For the most part, the Original Agreement contained the provisions set forth above in the Communication, except that it contained no mention of a multilateral approach under the ICAO nor did it mention an expiration date for the current "pull" system of PNR data transfers.[59]

---

[52] *Id.* at 5–8.

[53] *Id.* at 5–8.

[54] The ICAO is a U.N. specialized agency, which "works to achieve its vision of safe, secure and sustainable development of civil aviation through cooperation amongst its member States." Int'l Civil Aviation Org. [ICAO], *Strategic Objectives of ICAO for 2005–2010*, §1.1 app., U.N. Doc CAR/WG/1 – IP/06 (May 31, 2007), *available at* http://www.icao.int/nacc/meetings/2007/carwg01/CARWG01ip06.pdf. The ICAO was established on December 7, 1944 under the Convention on International Civil Aviation (Chicago Convention). Convention on International Civil Aviation art. 43, Dec. 7, 1944, 61 Stat. 1180, 1192, 15 U.N.T.S. 295, 324. The ICAO has 189 contracting states. ICAO, Contracting States, http://www.icao.int/cgi/goto_m.pl?cgi/statesDB4.pl?en.

[55] *Communication*, *supra* note 50, at 9.

[56] Commission Decision on the Adequate Protection of Personal Data Contained in the Passenger Name Record of Air Passengers Transferred to the United States' Bureau of Customs and Border Protection 2004/535/EC, art. 1, 2004 O.J. (L 235) 11, 13 (EC).

[57] Council Decision 2004/496/EC, art. 1, 2004 O.J. (L 183) 83, 83 EC).

[58] *Id.*; Press Release, European Commission, International Agreement on Passenger Name Records (PNR) Enters into Force, (May 28, 2004), *available at* http://ec.europa.eu/comm/external_relations/us/news/ip04_694.htm.

[59] Council Decision 2004/496/EC, 2004 O.J. (L 183) 83 (EC).

4. ECJ Annulment of the PNR Agreement

On July 27, 2004, the European Parliament applied to the ECJ for annulment of the May 17, 2004 Council decision and of the Commission's decision on the adequacy of United States' data protection, contending "that adoption of the decision on adequacy was *ultra vires*, that Article 95 EC does not constitute an appropriate legal basis for the decision approving the conclusion of the agreement and, in both cases, that fundamental rights have been infringed."[60] On May 30, 2006, the ECJ joined the actions against the Council (C-317/04) and the Commission (C-318/04) and without addressing the *ultra vires* or fundamental rights infringement claims, annulled both the Council decision and the Commission's decision on adequacy and gave the parties until September 30, 2006 to work out a new agreement.[61]

In the case against the Commission, the ECJ reasoned that even though the PNR data may be viewed as being collected first by the airlines for commercial purposes (the sale of an airplane ticket for a supply of services), the Commission's decision on adequacy concerns data processing regarded as necessary for safeguarding public security and for law-enforcement purposes.[62] Since Article 3(2)[63] of the Data Protection Directive excludes data processing for operations concerning public security, defense, and Member State security from the scope of the Data Protection Directive, the ECJ held that the Commission's decision on adequacy does not fall within the scope of Data Protection Directive and it must therefore be annulled.[64]

In the case against the E.U. Council, the Parliament argued that Article 95 of the Treaty Establishing the European Union does not constitute an appropriate legal basis for the Council's decision.[65] Article 95(1) provides, in pertinent part, as follows: "[t]he Council shall . . . adopt the meas-

---

[60] Press Release, European Court of Justice, The Court Annuls the Council Decision Concerning the Conclusion of an Agreement Between the European Community and the United States of America on the Processing and Transfer of Personal Data and the Commission Decision on the Adequate Protection of Those Data, (May 30, 2006) (citation omitted), *available at* http://curia.europa.eu/en/actu/communiques/cp06/aff/cp060046en.pdf.

[61] Joined cases Case C-317/07 and C-318/04, European Parliament v. Council of the European Union (C-317/04) and European Parliament v. Comm'n of the European Communities (C-318/04), 2006 E.C.R. I-4721.

[62] *Id.* at paras. 56–57.

[63] "This Directive shall not apply to the processing of personal data: in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence [and] State security . . . ." Council Directive 95/46/EC, art. 3(2), 1995 O.J. (L 281) 1, 12 (EC).

[64] European Parliament*,* 2006 E.C.R. I-4721, paras. 58–59.

[65] European Parliament, 2006 E.C.R. I-4721, para. 63.

ures for approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market."[66] The Parliament further argued that Article 95 "cannot justify [c]ommunity competence to conclude the [Original] Agreement" because the Original Agreement relates to data processing operations which "are excluded from the scope of the [Data Protection] Directive."[67] Although Article 25 of the Data Directive allows personal data to be transferred to a third country provided that the country ensures an adequate level of protection, the ECJ held Article 95 EC, even read "in conjunction with Article 25 of the Data Protection Directive, cannot justify Community competence to conclude the Agreement" because as determined in Decision C-318, the PNR data transfer to the United States is outside the scope of the Data Protection Directive.[68] Thus, the E.U. Council did not have an appropriate legal basis for its decision.[69]

5. The Interim and Revised PNR Transfer Agreements

As directed by the ECJ in the annulment decisions, the European Union and United States negotiators reached an interim agreement on October 16, 2006 (Interim Agreement), which subsequently expired on July 31, 2007.[70] Before the Interim Agreement expired, the European Union and United States negotiators finalized a revised agreement (Revised Agreement), signed on July 23, 2007 in Brussels, and July 26, 2007 in Washington, D.C.[71] The Revised Agreement consists of three elements: (1) "an agreement signed by both parties"; (2) "[a] letter by [the U.S. Department of Homeland Security] giving assurances on the way it intends to protect PNR data"; and (3) "[a] reply letter from the [European Union] . . . confirming that on the basis of the assurances, it considers the level of protection of

---

[66] Treaty Establishing the European Community, art. 95, Nov. 10, 1997, 1997 O.J. (C340) 3, 213 [hereinafter EC Treaty].

[67] European Parliament, 2006 E.C.R. I-4721 para. 67–68.

[68] *Id.* at paras. 63–67.

[69] *See id.* at para. 69.

[70] 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, U.S.-E.U., Oct. 27, 2006 , 2006 O.J. (L 298) 29, 29–31 [hereinafter Interim Agreement]; *see also* Press Release, European Commission, EU and US Reach Agreement on the Continued Use of Passenger Name Record (PNR) Data (October 6, 2006), http://www.eurunion.org/News/press/2006/20060086.htm. The Council adopted the Interim Agreement on October 16, 2006. Council Decision 2006/729/CFSP/JHA 2006 O.J. (L 298) 27(EU).

[71] 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 PNR Agreement), U.S.-E.U., July 23, 2007, 2007 O.J. (L 204) 18, 18–20 [hereinafter Revised Agreement].

PNR data in the United States as adequate."[72] It expires seven years after the "date of signature," unless the parties mutually agree to replace it or if one of the parties terminates the agreement, at any time, through diplomatic channels.[73]

In order to abide by the annulment decisions, the Council—first in the Interim Agreement and then in the Revised Agreement—changed the legal basis of the E.U.-U.S. PNR agreement from the Treaty Establishing the European Community[74] or "first pillar" to the Treaty on European Union[75] or "third pillar."[76] As a result, the Revised Agreement now falls under the competence of the European Union, as opposed to the European Community.[77]

To the dismay of the European Parliament and the Article 29 Working Party, the Revised Agreement did not go as far as expected in safeguarding airline passenger privacy.[78] On the one hand, the Revised Agreement does incorporate some important safeguards that were lacking in the previous two agreements. For instance, the Revised Agreement extends the privacy protections found in the Privacy Act of 1974 and the Freedom of Information Act to non-U.S. citizens and provides a system of redress for persons seeking information about or correction of PNR.[79] In addition, the Revised Agreement provides assurances from the Department of Homeland Security that it "will provide to airlines a form of notice concerning PNR collection and redress practices to be available for public display [and] . . . will work with interested parties in the aviation industry to promote greater visibility of this notice."[80] Finally, the Revised Agreement adopts the "push" system of transmitting PNR.[81]

---

[72] Article 29 Data Protection Working Party, *Opinion 5/2007 on the Follow-Up 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 Concluded in July 2007*, at 5, *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp138_en.pdf (last visited Nov. 15, 2007) [hereinafter Opinion 5/2007].

[73] Revised Agreement, *supra* note 71, at 19.

[74] *See* Interim Agreement, *supra* note 70; Revised Agreement, *supra* note 71; E.C. Treaty, *supra* note 66.

[75] *See* Consolidated Version of the Treaty on European Union, 2002 O.J. (C325) 5.

[76] *See* Interim Agreement, *supra* note 70, at 30; EUR. PARL. DOC. (B6-0393) 4 (2006) at para. 11.

[77] *See* Revised Agreement, *supra* note 71, at 18.

[78] *See*, *e.g.*, EUR. PARL. DOC. (B-6-0393) (2006) (addressing issues in the draft version of the Revised Agreement that were included in the final version of the Revised Agreement); Opinion 5/2007 *supra* note 72, at 2–4.

[79] Revised Agreement, *supra* note 71, at 23.

[80] *Id.*

[81] *Id.* at 23–24.

On the other hand, the Revised Agreement weakens many of the safeguards provided for under the previous two agreements. First, the Revised Agreements extends the retention period from three and one-half years to fifteen years, with the possibility of it being extended further.[82] Second, the Department of Homeland Security now may use sensitive PNR data elements—"personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning health or sex life of the individual"—in exceptional cases, "where the life of a data subject or of others could be imperiled or seriously impaired."[83] Third, while the Revised Agreement seems to reduce the number of PNR elements transferred to U.S. authorities from thirty-four to nineteen,[84] this change is a mere subterfuge as the Revised Agreement groups all but one of the thirty-four elements into one of nineteen new data sets.[85] Fourth, and finally, the Revised Agreement requires the airlines to transfer new PNR data that were not required under the previous agreements, including additional baggage and frequent flyer information.[86]

Because the Revised Agreement does not adequately provide privacy protections, Part IV of this Note recommends a solution for the PNR transfer issue which respects the principles of the Data Protection Directive without sacrificing the effective elements of PNR transfer as a counter-terrorism tool.

B. The Terrorist Financing Tracking Program

1. The *New York Times'* Disclosure of the Secret Government Program

The other major development of 2006 in the E.U-U.S. conflict over data protection occurred on June 23, 2006 when the *New York Times* published details of the U.S. government's Terrorist Finance Tracking Program.[87] TFTP, which is run by the CIA and overseen by the Treasury Department, relies on Executive powers under the International Emergency

---

[82] Under the Revised Agreement, data is stored in an active analytical database for seven years and then moved to dormant, non-operational status for eight years, where it can be "accessed only with approval of a senior [Department of Homeland Security] official . . . and only in response to an identifiable case, threat, or risk. *Id.* at 23. After the fifteen year period has expired, the Department of Homeland Security *expects* that the data will be deleted, and the Revised Agreement states that "questions of whether and when to destroy PNR data . . . will be addressed . . . as part of future discussions." *Id.*

[83] *Id.*

[84] *See id.*; *Opinion 5/2007*, *supra* note 72, at 9.

[85] *Id.*

[86] Revised Agreement, *supra* note 71, at 21–22.

[87] Lichtblau & Risen, *supra* note 2.

Economic Powers Act of 1978[88] (IEEPA) to acquire information about financial transactions from the world's largest financial communication network—the Society for Worldwide Interbank Financial Telecommunication (SWIFT).[89] Since just after the September 11 terrorist attacks, the U.S. government has been secretly requesting financial data from SWIFT in an effort to track terrorist financing activities.[90] Once the U.S. Department of Treasury receives the information from SWIFT, it compiles the data in a massive database, which is searchable by the CIA, FBI, and other government agencies.[91]

a. SWIFT: The "Plumbing" Between Financial Institutions[92]

SWIFT is a Belgian company owned and operated by a consortium of financial institutions.[93] It supplies secure messaging services in more than 200 countries and to more than 8,100 financial institutions (banks, brokers, investment managers, and market infrastructures).[94] Generally, the secure messages that are transmitted by SWIFT contain only limited amounts of personal data such as the name of the beneficiary or the ordering customer and a reference number, which "allows the payer and payee to reconcile the payment with their respective accounting documents."[95]

---

88 International Emergency Economic Powers Act, 50 U.S.C. §§ 1701–07 (2000).

89 Lichtblau & Risen, *supra* note 2.

90 *Id.*

91 *Id.*

92 At the European Parliament Hearing held on October 4, 2006, Francis Vanbever, Chief Financial Officer of Swift described SWIFT "as the 'plumbing' between financial institutions." Press Release, SWIFT, SWIFT Re-Iterates Calls for EU-US Dialogue on Security and Data Privacy (Oct. 4, 2006), http://www.swift.com/index.cfm?item_id=60670.

93 *See* SWIFT, About SWIFT, http://www.swift.com/index.cfm?item_id=43232 (last visited Nov. 16, 2007).

94 Leonard H. Schrank, Yawar Shah, & Stephen Zimmerman, SWIFT Statement on Compliance Policy, SWIFT, http://www.swift.com/index.cfm?item_id=59897 (last visited Nov. 16, 2007).

95 Article 29 Data Protection Working Party, *Opinion 10/2006 on the Processing of Personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, 01935/06/EN, *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_en.pdf [hereinafter *Opinion 10/2006*]. These user disclosure requirements relate to Special Recommendation VII of the Financial Action Task Force's Nine Special Recommendations on Terrorist Financing. *See* discussion *infra* Part III.B.1. Special Recommendation VII on wire transfers suggests, in pertinent part, that: "[c]ountries should take measures to require financial institutions . . . to include accurate and meaningful originator information (name, address and account number) on funds transfers and related messages that are sent, and the information should remain with the transfer or related message through the payment chain." *Id.*

SWIFT maintains two operations centers—one in the United States and the other in Belgium.[96] All messages processed by SWIFT are stored for 124 days in both of the two operation centers.[97] The dual storage or "mirroring" acts as a back-up recovery tool for customers in case of disputes between financial institutions or data loss.[98]

Since SWIFT is neither a bank nor a payment or settlement system, it is not regulated by central banks or bank supervisors.[99] Nevertheless, the central banks of the Group of Ten countries have set up a system of cooperative oversight of SWIFT.[100] Although the European Central Bank knew of TFTP, it did not notify European data protection authorities.[101] Jean-Claude Trichet, President of the European Central Bank, said that the European Central Bank "has no authority to supervise [SWIFT] with regard to compliance with data protection laws."[102] Peter Praet, President of the National Bank of Belgium, which leads the SWIFT oversight group, echoed Trichet's sentiments and added that the transfers posed no threat to financial stability.[103] The Bank of England claims that it informed the U.K. Treasury Department, and although the U.K. Treasury Department may have shared the information internally, it did not disclose SWIFT's activities to the Article 29 Working Party or the Commission.[104]

b. The Process of Obtaining Data from SWIFT

To obtain the data that it wanted from SWIFT, the Office of Foreign Assets Control of the U.S. Department of Treasury sent administrative subpoenas[105] to SWIFT.[106] In responding to the U.S. Department of Treasury

---

96 *Opinion 10/2006*, *supra* note 95, at 8.

97 *Id.*

98 *Id.*

99 SWIFT, Oversight of SWIFT, http://www.swift.com/index.cfm?item_id=57001 (last visited Nov. 17, 2007).

100 *Id.*

101 *See* Dan Bilefsky, *Europeans Berate Bank Group and Overseer for U.S. Access to Data*, N.Y. TIMES, Oct. 5, 2006. The European Data Protection Supervisory ("EDPS") heavily criticized the European Central Bank for not notifying the proper authorities. *Id.*

102 *Id.*

103 *Id.*

104 Alexi Mostrous & Ian Cobain, *CIA's Secret Bank Trawl May Be Illegal: US Effort to Track Jihadist Money Transfers Faces Inquiry Over Privacy*, GUARDIAN, Aug. 21, 2006, *available at* http://www.guardian.co.uk/terrorism/story/0,,1854813,00.html.

105 An administrative subpoena is an official order from a government agency compelling a third party to produce certain information. *See*, *e.g*,. United States. v. Allis-Chalmers Corp., 498 F.Supp. 1027, 1028–1030 (E.D.Wis. 1980). Generally, for an administrative subpoena to be valid, the inquiry must be within the authority of the agency, the demand must not be too indefinite, and the information sought must be reasonably relevant to the inquiry. *Id.* at 29

subpoenas, SWIFT activated its "compliance policy," adopted by its Board of Directors in the early 1990s.[107] SWIFT's policy, which is included in its customer contracts and published on its website, states that while SWIFT takes all necessary measures to ensure the highest degree of integrity and confidentiality for the data messaging service that it provides, it has to comply with legal subpoenas and warrants issued by authorities.[108] SWIFT, in accordance with this policy, then sent the requested information to the U.S. Department of Treasury.[109] According to Under Secretary for the Office of Terrorism and Financial Intelligence, Stuart Levey, before a search can be run, analysts must first explain how the target of the search is connected to a counter-terrorism investigation.[110] Levey claims that the program is legal and that the authority to ascertain the records from SWIFT and review them comes from the IEEPA.[111] Levey stated that with respect to oversight, SWIFT's auditors are able to monitor the searches and that a record of each search is kept. Booz Allen Hamilton (Booz Allen), an outside independent auditor, then reviews the record.[112]

c. The Aftermath of the Disclosure

As soon as the *New York Times* initially released the details of TFTP,[113] foreign officials from across the globe, but especially in the European Union, raised concerns as to whether the program violated their countries' privacy laws.[114] In fact, on July 7, 2006 the European Parliament

---

(citing United States v. Morton Salt Co., 338 U.S. 632, (1950)). An administrative agency obtains subpoena power by statute. *Id.* at 28.

106 Josh Meyer & Greg Miller, *U.S. Secretly Tracks Global Bank Data*, L.A. TIMES, June 23, 2006, at 1A.

107 Press Release, SWIFT, SWIFT Statement on Compliance Policy (June 23, 2006), http://www.swift.com/index.cfm?item_id=59897.

108 *Id.*

109 Meyer & Miller, *supra* note 106.

110 *Id.*

111 *Id.*

112 *Id.*

113 Lichtblau & Risen, *supra* note 2. It is interesting to note that on October 22, 2006, the public editor of the New York Times, Byron Calame, admitted that his earlier defense of the newspaper's decision to publish details on the TFTP was a mistake. Byron Calame, *Banking Data: A Mea Culpa*, N.Y. TIMES, October 22, 2006. Calame cited two factors in reversing his position: (1) he had not found any evidence that the program was illegal under United States laws, and (2) no abuses of private data had been uncovered. *Id.* Calame's "original support for the article rested heavily on the fact that so many people already knew about the program that serious terrorists also must have been aware of it," but as Calame points out if the program was not secret, why did the New York Times portray it as such. *Id.*

114 *See*, *e.g.*, Dan Bilefsky & Eric Lichtblau, *Swiss Official Says Bank Broke Law by Supplying Data to U.S.*, N.Y. TIMES, Oct. 14, 2006, at A7; Dan Bilefsky, *Europeans Berate Bank*

adopted a resolution which expressed "its serious concern at the fact that a climate of deteriorating respect for privacy and data protection is being created" and urged the United States "and its intelligence and security services to act in a spirit of good cooperation and notify their allies of any security operations they intend to carry out on E.U. territory."[115] The resolution focused its concern on the European citizens and their parliamentary representation lacking adequate notice of the program, but also raised the possibility of the transfers of "information on the economic activities of the individuals and countries concerned" being linked to "large-scale forms of economic and industrial espionage."[116]

Surprisingly, despite the concerns that the program violates E.U. data protection laws, the Article 29 Working Party,[117] an independent E.U. advisory body on data protection and privacy, waited until November 22, 2006 to issue an opinion—Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (Opinion 10/2006)—denouncing SWIFT's activities with respect to the TFTP participation.[118] In Opinion 10/2006, the Article 29 Working Party concludes that SWIFT violated the Directive and calls for it to cease all infringements.[119] Opinion 10/2006's first and most important finding is that SWIFT represents a data controller under Article 2 of the Data Protection Directive.[120] SWIFT, on the other hand, contends that it served only as a data processor under the Act.[121] Under the Data Protection Directive, a "controller" means "the natural or legal persona, public authority, agency or any other body which alone or jointly with others determines the purposes

---

Group and Overseer for U.S. Access to Data, N.Y. TIMES, Oct. 5, 2006, at A15. Because SWIFT is based in Belgium, it is subject to Belgian data protection law and thus the Data Protection Directive. *Opinion 10/2006*, *supra* note 95, at 2.

115 EUR. PARL. DOC. (B6-0393) 4 (2006).

116 EUR. PARL. DOC. (B6-0386) 2 (2006).

117 *See supra* notes 18–19 and accompanying text.

118 *Opinion 10/2006*, *supra* note 95. In fact, the Article 29 Working Party did not hold its first plenary discussion regarding the SWIFT transfers to the United States until September 26, 2006. Press Release, Article 29 Working Party, Press Release on the SWIFT Case (Sept. 26, 2006), http://ec.europa.eu/justice_home/fsj/privacy/news/docs/PR_Swift_Affair_26_09_06_en.pdf.

119 *Id.* Switzerland, which is not a member of the European Union, has also stated that "Swiss banks broke their nation's laws by providing banking information to American counterterrorism officials." Dan Bilefsky & Eric Lichtblau, *Swiss Official Says Banks Broke Law by Supplying Data to U.S.*, N.Y. TIMES, Oct. 14, 2006, at A7.

120 *Opinion 10/2006*, *supra* note 95, at 9.

121 SWIFT, SWIFT Supports Calls for Debate to Move Beyond Data Privacy to Security and Public Safety (Nov. 9, 2006), http://www.swift.com/index.cfm?item_id=60784 [hereinafter *SWIFT Response*] (containing SWIFT's response to the Belgian Privacy Commision's Advisory Opinion of September 27, 2006).

and means of the processing of personal data," while a "processor" means "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller."[122] The distinction is important because as the definitions indicate, a data processor processes information *on behalf* of the controller; therefore, the processor's duties under the Data Protection Directive are limited as compared to those of the data controller.[123] The Article 29 Working Party, however, held that SWIFT acts as a controller in *both* its normal secure messaging services and its processing of the subpoenaed data, and thus is responsible for complying with the Data Protection Directive, as a controller, even before the information was sent to the U.S. authorities.[124] As such, the Article 29 Working Party called for SWIFT to cease its Data Protective Directive infringements and return to lawful data processing immediately.[125]

d. SWIFT Joins the Safe Harbor

After issuing Opinion 10/2006, the Article 29 Working Party—at its Fifty-Ninth,[126] Sixtieth,[127] and Sixty-First[128] Meetings held on February 14–15, April 17–18, and June 19–20, 2007, respectively—reported on SWIFT's progress in complying with the Data Protection Directive. It appears that after the Article 29 Working Party had called for SWIFT to cease its efforts in the TFTP, it shifted its focus to aiding SWIFT in complying with the Data Protective Directive and ensuring that the financial institutions alert their clients that U.S. authorities may have access to the client's personal data.

After nearly a year of limited response on the TFTP, on June 28, 2007, Stuart Levey sent a letter to the European Commission transmitting "a [unilateral] set of representations which describe the controls and safeguards

---

122 Council Directive 95/46/EC, art. 2(d)–(e), 1995 O.J. (L 281) 1, 11–12 (EC).

123 A data processor still must comply with the provisions of the Data Protection Directive. *See*, *e.g.*, *id.* art. 16 ("Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.").

124 *See SWIFT Response*, *supra* note 121, at 2.

125 *Opinion 10/2006*, *supra* note 95, at 28.

126 *See* Press Release, Article 29 Working Party, The Article 29 Data Protection Working Party Met Representatives of SWIFT (Feb. 16, 2007), http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp29_pr_16_02_07_en.pdf.

127 Press Release, Article 29 Working Party, The Article 29 Data Protection Working Party Considered Again the SWIFT Case, (Apr. 20, 2007), http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_20_04_07_en.pdf.

128 Press Release, Article 29 Working Party, The Article 29 Data Protection Working Party Continued its Deliberations on the SWIFT Case (June 21, 2007), http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_21_06_07_en.pdf.

governing the handling, use and dissemination of data under the [TFTP]."[129] The representations (Representations) were sent in preparation for SWIFT's possible entry into the Safe Harbor. As mentioned in Part II, the Safe Harbor Principles do not apply to data transfers to government authorities.[130] Unlike the PNR transfers by the E.U. airlines to the U.S. Department of Homeland Security, however, the SWIFT processing center in Europe transfers the data to its U.S. branch for commercial purposes—mirroring the data to ensure its integrity—and any access by U.S. authorities takes place subsequently, in the United States. Nonetheless, since the data is subsequently accessed by U.S. authorities, U.S. efforts under the TFTP invoke the Safe Harbor Principles,[131] and the Representations provide an assurance that the United States will process the SWIFT data in compliance with E.U. data protection principles.[132]

The Representations first provide a background of the TFTP—the fundamental principles underlying the program, the concerns raised within the European Union, and even its adherence to international counterterrorist financing principles.[133] Then, in defense of the TFTP, the Representations provide the United States legal authority for obtaining and using the SWIFT data.[134] The Representations also describe the limited scope of the TFTP—including restrictions on extraction from SWIFT and the sharing of data among U.S. agencies, the "multiple complementary layers of independent oversight," and the system of redress available to those harmed by U.S. governmental authorities.[135] Finally, and most importantly, the Representations declare that "an eminent European person will be appointed to confirm that the [TFTP] is implemented consistent with the[] Representations for the purpose of verifying the protection of EU-originating personal data."[136] In

---

[129] Letter from Stuart A. Levey, U.S. Dep't of the Treasury Under Secretary for the Office of Terrorism and Financial Intelligence, to Peer Steinbrück and Vice-President Frattini, German Minister of Finance and Vice-President of the European Comm'n (June 28, 2007), 2007 O.J. (C 166/08) 17.

[130] *See supra* text accompanying notes 37–38.

[131] The Safe Harbor Principles allow limitations "to the extent necessary to meet national security, public interest or law enforcement [purposes]." Commission Decision 2000/520/EC, Safe Harbor Privacy Principles, Annex, 2000 O.J. (L 215) 7, 10 (EC).

[132] *See* Press Release, Council of the European Union, Processing and Protection of Personal Data Subpoenaed by the Treasury Department From the U.S. Based Operation Centre of the Society for Worldwide Interbank Financial Telecommunication (SWIFT) (June 28, 2007), http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/misc/95017.pdf.

[133] *Processing of EU Originating Personal Data by the United States Treasury Department for Counter Terrorism Purposes—'SWIFT,'* 2007 O.J. (C 166/09) 18 [hereinafter *Representations*].

[134] *Id.* at 20.

[135] *Id.* at 21–23.

[136] *Id.* at 25.

particular, the eminent person, who will be appointed by the Commission for a two year renewable term, will ensure that non-extracted data has been deleted.[137] In carrying out his or her duties, the eminent person will be completely independent and will report his or her findings annually to the Commission.[138]

In a reply letter, representatives of the Commission and the Council, took note of Levey's letter, welcomed the unilateral representations, and declared that once SWIFT provided the financial data to the United States for commercial purposes in accordance with the Safe Harbor Principles, it (and the financial institutions making use of its services) would be "in compliance with [its] respective legal responsibilities under European data protection law."[139]

Accordingly, on July 16, 2007, the U.S. branch of SWIFT joined the Safe Harbor, thereby agreeing to handle the personal data that it receives from the European Union in accordance with the Safe Harbor Principles.[140]

III. EXISTING INTERNATIONAL SYSTEM OF FINANCIAL INFORMATION EXCHANGE

Part III provides a background of the existing system of financial information exchange. An understanding of this system is critical in conceptualizing the positions that are advocated in Part IV.

A. The International Anti-Money-Laundering Legal Framework

Formalized international exchange of financial information began as an anti-money-laundering effort but has since evolved into an effective counter-terrorism tool. The international exchange of financial transactions came as a natural result of progressive international efforts in the late 1980's and early 1990's to develop an "international law enforcement regime"[141] to combat the ills of money-laundering. That is, given the transnational characteristics of money-laundering transactions, law enforcement

---

137 *Id.*

138 *Id.*

139 Franco Frattini & Peer Steinbruck, *Reply from the European Union to the United States Treasury Department—SWIFT/Terrorist Finance Tracking Programme*, 2007 O.J. (C 166/10) 26.

140 SWIFT, SWIFT Safe Harbor Policy (July 16, 2007), http://www.swift.com/index.cfm?item_id=62653.

141 "An international law enforcement regime can be defined as: 'a global arrangement among governments to co-operate against particular transnational crimes.'" GUY STESSENS, MONEY LAUNDERING: A NEW INTERNATIONAL LAW ENFORCEMENT MODEL 17 (2000) (quoting E. NADELMANN, COPS ACROSS BORDERS: THE INTERNATIONALIZATION OF U.S. CRIMINAL LAW ENFORCEMENT 22 (1993)).

agencies from around the globe needed an effective means of sharing financial information in order to effectively counter money-laundering activities.

The first major international anti-money-laundering effort[142] came in 1984 when the United Nations (UN) began working on a convention to combat the growing international drug-trafficking problem.[143] In 1988, the UN enacted the Convention Against Illicit Drug Traffic in Narcotic Drugs and Psychotropic Substances (Convention).[144] Although the Convention does not expressly use the phrase "money-laundering,"[145] the drafters of the Convention recognized that in order to effectively combat the widespread distribution and sale of illicit drugs, law enforcement authorities should go after those who "direct, finance, manage and profit from the criminal networks . . . ."[146] In fact, one commentator has noted that the Convention's central purpose was to "provide the law enforcement community with the necessary tools to undermine the financial power of the cartels . . . ."[147]

Anti-money-laundering efforts have also been deeply influenced by a number of "soft" law instruments, which lack justiciability[148] but not necessarily content.[149] The "crown jewel of soft law"[150] anti-money-laundering instruments is the forty recommendations for fighting money-laundering

---

142 The first international instrument to *specifically* address the issue of money laundering was the Basel Statement of Principles passed on December 12, 1988. Although not a truly international effort, the Basel Statement of Principles "played a pioneer role . . . [in providing] a framework of rules in an area of law where formal legislation was still lacking." STESSENS, *supra* note 141, at 16–17.

143 *See* John Evans, *International Efforts to Contain Money Laundering*, INTERNATIONAL CENTRE FOR CRIMINAL LAW REFORM AND CRIMINAL JUSTICE POLICY 3 (Apr. 8, 1997), *available at* http://www.icclr.law.ubc.ca/Publications/Reports/MoneyLaundering.pdf.

144 Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, Dec. 20, 1988, 32 U.S.T 543, 26 U.N.T.S. 164.

145 The Convention expresses the wrongdoing as follows: "[t]he conversion or transfer of property, knowing that such property is derived from any offence or offences established in accordance with subparagraph *a)* of this paragraph, or from an act of participation in such offence or offences, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an offence or offences to evade the legal consequences of his actions." *Id.* at art. 3(b)(i).

146 Evans, *supra* note 143, at 3.

147 WILLIAM GILMORE, DIRTY MONEY: THE EVOLUTION OF MONEY LAUNDERING COUNTER-MEASURES 64 (1995).

148 Justiciabilty means "[t]he quality or state of being appropriate or suitable for adjudication by a court." BLACK'S LAW DICTIONARY (8th ed. 2004); 13 CHARLES ALAN WRIGHT ET AL., FEDERAL PRACTICE AND PROCEDURE § 3529, 278–79 (2d ed. 1984) ("Concepts of justiciability have been developed to identify appropriate occasions for judicial action. . . . The central concepts often are elaborated into more specific categories of justiciability—advisory opinions, feigned and collusive cases, standing, ripeness, mootness, political questions, and administrative questions.")

149 *See* STESSENS, *supra* note 141, at 15.

150 *Id.*

and promoting good financial governance (Forty Recommendations) issued by the Financial Action Task Force (FATF) in 1990.[151] The G-7[152] heads of state created the FATF at the 1989 G-7 summit in Paris in recognition of the danger that money-laundering posed to the banking and financial systems of the developed world.[153] The FATF is an inter-governmental body, which currently has thirty-four members—thirty-two countries and governments and two international organizations.[154] The mandate of the FATF at its inception was

> to assess the results of co-operation already undertaken in order to prevent the utilization of the banking system and financial institutions for purpose [sic] of money laundering, and to consider additional preventative efforts in this field, including the adaptation of the legal and regulatory systems so as to enhance multilateral judicial assistance.[155]

The Forty (non-binding) Recommendations "provide a complete set of counter-measures against money-laundering covering the criminal justice system and law enforcement, the financial system and its regulation, and international co-operation."[156] Many governments and international bodies have, in whole or in part, recognized, endorsed, or adopted the Forty Recommendations as a means of combating money-laundering.[157] In fact, the European Council incorporated fifteen of the Forty Recommendations into the Directive on Prevention and Use of the Financial System for the Purpose of Money-Laundering.[158]

B. International Financial Information Sharing

Beginning in the early 1990's, the first few financial intelligence units were established "in response to the need for a central agency within each nation to receive, analyze, and disseminate financial information to

---

[151] Financial Action Task Force (FATF), FATF Documents on Forty Recommendations of, http://www.fatf-gafi.org (follow "40 Recs" hyperlink) (last visited oct. 10, 2007) [hereinafter Forty Recommendations].

[152] Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States compose the G-7 countries. *See* http://usinfo.state.gov/xarchives/display.html?p=washfile-english&y=2007&m=October&x=20071017175020saikceinawz0.9418756.

[153] Financial Action Task Force (FATF), About the FATF, http://www.fatf-gafi.org/ (follow "About the FATF" hyperlink) (last visited Oct. 10, 2007).

[154] *Id.*

[155] Evans, *supra* note 143, at 5–6 (citation omitted).

[156] Forty Recommendations, *supra* note 151.

[157] *Id.*

[158] *See* Council Directive 2005/60/EC, 2005 O.J. (L 309) 15, 20–32 (EC); Alan E. Sorcher, *Lost in Implementation: Financial Institutions Face Challenges Complying With Money-Laundering Laws*, 18 TRANSNAT'L L. 395, 408–12 (2005).

combat money-laundering."[159] A financial intelligence unit (FIU) is "a central, national agency responsible for receiving, (and as permitted, requesting), analyzing and disseminating to the competent authorities, disclosures of financial information: (i) concerning suspected proceeds of crime and potential financing of terrorism, or (ii) required by national legislation or regulation, in order to combat money-laundering or terrorism financing."[160]

In June of 1995, a group consisting of government agencies and international organizations met at the Egmont-Arenberg Palace in Brussels to discuss money-laundering and ways to confront this global problem.[161] As a result of this meeting and in recognition of the benefits inherent in the development of an FIU network, the Egmont Group, an informal organization of financial intelligence units, was formed.[162] Now, the Egmont Group consists of one hundred FIUs from around the globe.[163]

Because money-laundering is often a transnational activity, one of the principle priorities of the Egmont Group is the stimulation of information exchange among its members.[164] Similarly, although not specifically referencing FIUs, FATF Recommendation 40 states, in relevant part, that:

> [c]ountries should ensure that their competent authorities provide the widest possible range of international cooperation to their foreign counterparts . . . . Where the ability to obtain information sought by a foreign competent authority is not within the mandate of its counterpart, countries are also encouraged to permit a prompt and constructive exchange of information with non-counterparts.[165]

FIU-to-FIU information sharing allows "FIUs, domestic law enforcement agencies, and other domestic 'consumers' of financial intelligence . . . to seek and obtain information promptly from foreign governments in order to deter, detect, and prosecute money-laundering, terrorist financing, and re-

---

159 THE WORLD BANK GROUP & INT'L MONETARY FUND, FINANCIAL INTELLIGENCE UNITS: AN OVERVIEW 1 (Paul Gleason & Glenn Gottselig eds., 2004), *available at* http://www.imf.org/external/pubs/ft/FIU/fiu.pdf [hereinafter FIU OVERVIEW].

160 THE EGMONT GROUP, INTERPRETATIVE NOTE CONCERNING THE EGMONT DEFINITION OF A FINANCIAL INTELLIGENCE UNIT 2 (2004), http://www.egmontgroup.org/egmont_final_interpretive.pdf.

161 *Id.* at 1; THE EGMONT GROUP INFORMATION PAPER ON FINANCIAL INTELLIGENCE UNITS AND THE EGMONT GROUP (2004), http://www.egmontgroup.org/info_paper_final_oct_2004.pdf.

162 *Id.*

163 *See* THE EDGMONT GROUP FINANCIAL INTELLIGENCE UNITS OF THE WORLD (2007), http://www.egmontgroup.org/list_of_fius.pdf.

164 *See* THE EGMONT GROUP, STATEMENT OF PURPOSE OF THE EGMONT GROUP OF FINANCIAL INTELLIGENCE UNITS 1–2 (2004), http://www.egmontgroup.org/statement_of_purpose.pdf [hereinafter EGMONT GROUP STATEMENT OF PURPOSE].

165 Forty Recommendations, *supra* note 151, Recommendation 40.

lated crimes."[166] The information transfers are a result of a strong system of reciprocity.[167]

A country's own law determines the ability of its FIU to share information with other FIUs and agencies in foreign governments.[168] Some countries authorize their FIUs to exchange information with other FIUs without a formal agreement, while others require the existence of a Memorandum of Understanding (MOU),[169] setting forth the terms and conditions that govern the transfer.[170] Although an MOU is not judicially enforceable, it carries with it not only "a moral obligation to live up to the terms of the arrangement" but also a fear that any breach will damage the reciprocal lines of information exchange.[171]

The general model of information exchange between FIUs is rather simple. The requesting FIU[172] typically sends a request in writing—either on paper or electronically[173]—to another FIU.[174] Generally, the requests contain the type of information sought and the intended use of the information.[175] The Egmont Group recommends that the "[r]equests . . . contain sufficient background information to enable the requested FIU to conduct proper analysis/investigation" and "be accompanied by a brief statement of the relevant facts known to the requesting FIU."[176] The receiving FIU should then process the request and send the information to the requesting FIU as soon as possible.[177] If the transmitting FIU consents,[178] the receiving FIU may disseminate the information to law enforcement officials.[179]

---

166 FIU OVERVIEW, *supra* note 159, at 65.

167 *See* THE EGMONT GROUP, BEST PRACTICES FOR THE EXCHANGE OF INFORMATION BETWEEN FINANCIAL INTELLIGENCE UNITS 2 (2004), http://www.egmontgroup.org/bestpractices.pdf [hereinafter FIU BEST PRACTICES].

168 FIU OVERVIEW, *supra* note 159, at 66.

169 *See id.* Rather than entering into a MOU, some FIUs prefer to enter into an exchange of letters, which can be substantively the same as an MOU. *Id.*

170 The Egmont Group has developed a model MOU for FIU-to-FIU information sharing. *See* EGMONT GROUP STATEMENT OF PURPOSE, *supra* note 164; FIU OVERVIEW, *supra* note 159, at 66.

171 FIU Overview, *supra* note 159, at 66–67.

172 If an FIU comes across information that might be useful to another FIU, the Egmont Group recommends that the FIU should consider supplying it spontaneously. FIU BEST PRACTICES, *supra* note 167, at 3.

173 Some FIUs use shared networks like the Egmont Secure Web or the European Union's FIU-NET to transmit information. FIU OVERVIEW, *supra* note 159, at 67.

174 *Id.*

175 *Id.*

176 FIU BEST PRACTICES, *supra* note 167, at 3.

177 *Id.* at 4.

178 The Egmont Group advises that "[t]he providing FIU should not refuse its consent to such dissemination unless this would fall beyond the scope of the AML/CFT provisions . . .

1. A Paradigm Shift to Countering the Financing of Terrorism

After the terrorist attacks on September 11, 2001, anti-money-laundering authorities have focused their efforts on detecting and deterring money-laundering systems used to finance international terrorist activities.[180] The Financial Action Task Force altered the existing Forty Recommendations by deleting specific references to drugs and expanding existing Recommendations.[181] The FATF also established the Nine Special Recommendations on Terrorist Financing (Nine Special Recommendations).[182] Like the Forty Recommendations, the Nine Special Recommendations include a recommendation regarding international cooperation: "[e]ach country should afford another country . . . the greatest possible measure of assistance in connection with criminal, civil enforcement, and administrative investigations, inquiries and proceedings relating to the financing of terrorism, terrorist acts and terrorist organizations."[183] The Nine Special Recommendations are to be read in conjunction with the Forty Recommendations on money-laundering to provide a comprehensive AML/CFT framework.[184] Additionally, at a special meeting held in October 2001, the Egmont Group expanded its global network of information exchange to encompass terrorist financing.[185]

These efforts were no doubt influenced by the UN Security Council's unanimous adoption of Resolution 1373 on September 28, 2001.[186] Resolution 1373 called on all UN member states to prevent terrorist financing,[187] and created the UN Counter-Terrorism Committee, which monitors the implementation of counter-terrorism finance measures and requires member states to exchange information about terrorist funding.[188] By invok-

---

or would otherwise not be in accordance with the fundamental principles of its national law." *Id.* at 2.

179 *See id.*

180 FATF Standards, 9 Special Recommendations (SR) on Terrorist Financing, http://www.fatf-gafi.org/document/9/0,2340,en_32250379_32236920_34032073_1_1_1_1,00.htm [hereinafter Nine Special Recommendations].

181 *See* Forty Recommendations, *supra* note 151.

182 Nine Special Recommendations, *supra* note 180.

183 *Id.*

184 *See id.*

185 *International Legal Developments: Sub-Group 1: Critical Review of Terrorist Related Legislation and the Monitoring of New Legislation*, 6 J. MONEY LAUNDERING CONTROL 201, 213 (2003).

186 S.C. Res. 1373, U.N. Doc. S/RES/1373 (Sept. 28, 2001).

187 *Id.* para. 1(a).

188 *See id*. para. 6.

ing Chapter VII of the UN Charter, Resolution 1373 makes the anti-terrorism effort legally binding.[189]

2. Data Privacy Controls

According to the Egmont Group, the FIUs are "invited to do everything possible to ensure that national legal standards and privacy laws are not conceived so as to inhibit the exchange of information between or among FIUs."[190] The Forty Recommendations, however, take a slightly different stance on data privacy: "[c]ountries should ensure that financial institution secrecy laws do not inhibit implementation of FATF Recommendations."[191] The FATF's message is clear: that the Forty Recommendations and Nine Special Recommendations present the most effective AML/CFT strategy and that countries should follow them closely.

3. Financial Information Exchange in the United States and European Union

a. United States

The Financial Crimes Enforcement Network (FinCEN) is the U.S. FIU.[192] It was created by order of the Secretary of Treasury on April 25, 1990 and is charged with administering the Bank Secrecy Act.[193] Section 361 of the USA PATRIOT Act (PATRIOT Act), passed on October 25, 2001, established the organization as a bureau within the Department of Treasury and clarified the duties and powers of FinCEN's Director.[194] Section 314 of the PATRIOT Act requires the Secretary of the Treasury to adopt regulations that encourage information sharing between regulatory and law enforcement authorities and financial institutions regarding individuals, entities, and organizations engaged in or reasonably suspected of engaging in terrorist acts or money-laundering activities.[195]

As in the process of information sharing between FIUs, U.S. law enforcement agencies also follow a relatively straightforward process in

---

189 *Id.* at 1; U.N. Charter arts. 39–51.

190 FIU BEST PRACTICES, *supra* note 167, at 1.

191 Forty Recommendations, *supra* note 151, at Recommendation Four.

192 Financial Crimes Enforcement Network, International/Egmont Group/FIUs, http://www.fincen.gov/int_fius.html (last visited Sept. 30, 2007).

193 Financial Crimes Enforcement Network, About FinCEN/FAQs, http://www.fincen.gov/af_faqs.html#addressed (last visited Sept. 30, 2007).

194 United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT ACT), Pub. L. No. 107-56,§ 361, 310, 115 Stat 272, 329–31.

195 *Id.* § 314(a).

obtaining data from FinCEN. First, a federal law enforcement agency requests information from FinCEN.[196] The agency must provide assurance that the request has been scrutinized at the agency level and that it satisfies FinCEN's standards for processing a Section 314(a) inquiry, and certify that the investigation is based on credible evidence of terrorist financing or money-laundering.[197] Next, FinCEN sends a request for information to a designated contact within each financial institution.[198] Then, the financial institution queries its records for data matches.[199] If an account or transaction match, the law enforcement agency must then meet the applicable legal standards to obtain the information.[200] If there is no match, then the financial institution does not reply to the request.[201]

b. European Union

E.U. law requires each E.U. Member state to have its own FIU,[202] and most of these FIUs[203] utilize a web-based electronic system called FIU.Net to share AML/CFT information with one another.[204] Directive

---

196 Financial Crimes Enforcement Network, *FinCEN's 314(a) Fact Sheet*, http://www.fincen.gov/314afactsheet.pdf.

197 *Id.*

198 *Id.*

199 *Id.*

200 *Id.*

201 *Id.*

202 Without specifically requiring each member state to establish an FIU, Directive 91/308/EEC on the prevention of the use of the financial system for the purposes of money laundering set forth numerous provisions requiring Member States to regulate their credit and financial institutions closely in order to prevent money laundering. Council Directive 91/308/EEC, 1991 O.J. (L 166), 77 (EU). Recognizing that all E.U. Member States had already established FIUs to abide by Directive 91/308/EEC, the Council, on October 17, 2000 adopted a Decision, which articulated a framework of cooperation and information exchange between the Member State FIUs. Council Decision 2000/642/JHA, 2000 O.J. (L 271) 4 (EC). Directive 2001/97/EC, which amended Directive 91/308/EEC, adopted measures that were espoused by the FATF in the late 1990s, but similar to the 1991 Directive, it had no specific reference to FIUs. Council Directive 2001/97/EC, 2001 O.J. L 344, 76 (EU). Finally, on October 26, 2005, the European Parliament and Council ratified Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. Council Directive 2005/60/EC, 2005 (L 309) 15, 27 (EC) (providing that "[e]ach Member State shall establish a FIU in order to effectively combat money laundering and terrorist financing.").

203 Austria, Ireland, and Malta are only observers; Cyprus, Denmark, Finland, Greece, Portugal, and Sweden will be connected in the near future. *See* FIU.Net, FIU.Net Connections, http://www.fiu.net/index.php?option=com_content&task=view&id=48&Itemid=64 (last visited Sept. 30, 2007).

204 *See* FIU OVERVIEW, *supra* note 159, at 68 ("FIU.NET runs over a private network and is highly secure, protected by firewalls as well as sophisticated encryption and authentication technologies.").

2005/60/EC (Third Directive)—the third of three Directives governing how Member States regulate their financial and credit institutions[205]—expanded the scope of two previous Directives to specifically reference terrorist financing and to account for the June 2003 revisions in the Forty Recommendations.[206] It is important to note that Third Directive *prohibits* financial institutions from disclosing to their customers and other third persons that the customer's information has been sent to the FIU or that their records are under review.[207] This demonstrates that the European Union is willing to put criminal investigation ahead of its strict adherence to data protection when the processes that will ensure adequate data protection are followed.

IV. RECOMMENDATIONS

A. The United States Should Terminate the TFTP and Instead Continue to Use FinCEN to Achieve Its AML/CFT Goals

The international community has almost universally accepted and implemented the practice of international information sharing by FIUs.[208] It has been able to do this within the constructs of the Data Protection Directive, while at the same time achieving AML/CFT successes.[209] In accessing the SWIFT network without first gaining an "adequacy finding" by the European Commission and then a bilateral agreement with the European Commission, the United States has circumvented all the data protection filters that the FIU model is founded upon—mutual trust, home country

---

205 *See supra* note 202 and accompanying text.

206 *See* Alan E. Sorcher, *Lost in Implementation: Financial Institutions Face Challenges Complying With Anti-Money Laundering Laws*, 18 TRANSNAT'L LAW 395 (2005).

207 Council Directive 2005/60/EC, art. 28, 2005 (L 309) 15, 28 (EC).

208 *See* discussion *supra* Part III.

209 According to FinCEN's former Director Robert W. Werner, FinCEN shared valuable information with Spain's FIU—Executive Service of the Commission for the Prevention of Money Laundering and Monetary Infractions ("SEPLAC")—after the Madrid subway bombings and with the United Kingdom's FIU—Serious Organised Crime Agency ("SOCA") following the United Kingdom's August 2006 discovery of a terrorist plot to blow up commercial airliners flying from the United Kingdom to the United States. *See* Robert W. Werner, Dir., Fin. Crimes Enforcement Network, Remarks at the American Bankers Association/American Bar Association Money Laundering Enforcement Conference, 10–12, (Oct. 9, 2006); THE EGMONT GROUP, FINANCIAL INTELLIGENCE UNITS OF THE WORLD 4 (2007), http:www.egmontgroup.org/list_of_fius.pdf. The information shared with SOCA "arose from U.S. financial institutions that proactively queried their records based on suspect lists released publicly by foreign authorities, found relevant information, and provided information to FinCEN . . . [using] FinCEN's Financial Institutions Hotline." Robert W. Werner, Dir., Fin. Crimes Enforcement Network, Remarks at the American Bankers Association/American Bar Association Money Laundering Enforcement Conference, 12, (Oct. 9, 2006), http://www.fincen.gov/werner10906.pdf.

oversight, reciprocity, and confidentiality.[210] This naturally is unacceptable to the European Union and other countries that have sophisticated data protection policies.[211] Indeed, that is why on November 22, 2006, the Article 29 Working Party called for the immediate termination of the TFTP, claiming that SWIFT had violated the Data Protection Directive. While the Representations represent a step in the right direction, they came nearly a year after the initial disclosure of the TFTP by the *New York Times*.[212] In addition, the Representations are simply a series of unilateral, and for the most part, overly broad commitments from the United States. It is unclear whether the acknowledgement of such unilateral representations by representatives of the Commission and Council is authorized under the Data Protection Directive and the Safe Harbor Principles.

Even if the transfers are now legal under E.U. data protection law through SWIFT's entry into the Safe Harbor, they still raise several other concerns. First, SWIFT and the United States claim that the searches were limited and targeted;[213] however, some privacy watchdog organizations and European Union officials doubt the limited nature of the program.[214] If the searches were not targeted, given the sheer magnitude of data that SWIFT manages,[215] it is highly doubtful that the United States is able to get anything from the data other than matching transactions and accounts with

---

210 *See supra* notes 164–167 and accompanying text.

211 *See* discussion *supra* Part II.B.1.c.

212 Lichtblau & Risen, *supra* note 2, at A1.

213 *See*, *e.g.*, SWIFT, *Update and Q&A to SWIFT's 23 June 2006 Statement on Compliance*, August 25, 2006, http://www.swift.com/index.cfm?item_id=60275 ("The United States Department of Treasury (UST) subpoenas to SWIFT are only for a limited set of data and for the exclusive purpose of terrorism investigations and for no other purpose. . . . The UST . . . [is] only allowed to see data that is responsive to targeted searches in the context of a specific terrorism investigation. Data searches must be based only on persons, entities or related information with an identified connection to ongoing terrorism investigation. . . ."); Press Release, Stuart Levey, Under Secretary for the Office of Terrorism and Financial Intelligence, Statement on the Terrorist Finance Tracking Program, (June 23, 2006), http://www.treasury.gov/press/releases/js4334.htm.

214 Privacy International estimates that roughly one-percent (or 4.6 million) of the 460 million financial transactions originating in the United Kingdom and subsequently sent through the SWIFT network in 2004 were secretly transferred to the United States under the TFTP. Press Release, Privacy International, PI Estimates over 4 Million UK Financial Records Sent Each Year to the U.S. (July 6, 2006), http://pi.gn.apc.org/article.shtml?cmd[347]=x-347-539301. According to the International Herald Tribune, Belgium Prime Minister, Guy Verhofstadt, said that SWIFT had received administrative subpoenas for millions of records. Dan Bilefsky, *Belgian Leader Orders Bank Inquiry*, INT'L HERALD TRIB., June 26, 2006, at 3.

215 As mentioned earlier, SWIFT provides messaging services for roughly 8,100 financial institutions in 207 countries and territories. *See Schrank*, *supra* note 94. This means that the network carries up to 12.7 million messages per day. *See* Meyer & Miller, *supra* note 106.

people on terror-watch lists. FinCEN could theoretically achieve the same ends by providing these terror-watch lists to foreign FIUs.

Although the U.S. authorities may be able to extract valuable information from the SWIFT data, the authorities are skipping a valuable step—communication with foreign AML/CFT authorities. This step is important for two main reasons. First, the communication helps further global AML/CFT efforts because by making a request to another FIU, the requesting FIU is sharing information on individuals suspected of being involved in terrorist or money-laundering activities. Second, and more importantly, the communication helps ensure that foreign data protection controls are not breached because the transferring FIU provides an oversight mechanism that is very limited under the TFTP—home country oversight.

The Representations state that the TFTP has "multiple complementary layers of independent oversight," including the U.S. Treasury Department, SWIFT representatives, an independent auditing firm, and even the U.S. Congress.[216] The addition of an eminent European provides another layer. All of these "layers," however, present significant problems, which are absent in the FIU system of financial information exchange.

First, while the appointment of an eminent European represents a step in the right direction, the Representations state that "[i]n particular, the eminent person will monitor that processes for deletion of non-extracted data have been carried out."[217] Therefore, the eminent person's role strangely appears limited to overseeing the deletion of non-extracted data, not the use, dissemination, and retention of extracted data.

Second, several of the "multiple complementary layers of independent oversight"—including the U.S. Treasury Department and SWIFT—are not independent. In fact, their activities are, or at least should be, the subject of the oversight.

Third, TFTP's independent auditor, Booz Allen—a global consulting firm with over 19,000 employees worldwide[218]—may not be entirely independent.[219] In a memorandum to the Article 29 Working Party, however, Privacy International and the American Civil Liberties Union claim that Booz Allen's oversight of the TFTP is not independent because Booz Allen: (1) has substantial U.S. government contracts, (2) is involved in other existing controversial U.S. government surveillance programs, (3) has numerous employees—including many high level executives—with connections to

---

216 *Representations*, *supra* note 133, at 21.

217 *Id.* at 25.

218 Booz Allen Hamilton, About Booz Allen, http://www.boozallen.com/about (last visited Oct. 11, 2007).

219 Memorandum by the Am. Civil Liberties Union and Privacy Int'l for the Article 29 Working Party of the European Comm'n 1–2 (Sept. 14, 2006), http:www.aclu.org/pdfs/safefree/boozallen20060914.pdf.

federal intelligence and military agencies, and (4) lobbies for increased information sharing.[220] Regardless of whether these allegations are true, the TFTP clearly does not provide the same level of oversight as the FIU method of information sharing because the home country only has a limited role in the process.

If the internationally-accepted FIU model does not meet the needs of the United States in its AML/CFT efforts, then the United States should seek changes within the current system, not create an entirely new and secret system. The United States has already made promising inroads in achieving this objective. On January 17, 2007, the Department of Treasury[221] delivered a report to Congress on the feasibility of a cross-border electronic funds transfer system, which concluded that "the reporting of cross-border wire transfer data by financial institutions is technically feasible for the government and may be valuable to the government's efforts to combat money-laundering and terrorist financing."[222] The report calls for an incremental process for the system's development, including spending the remainder of 2007 "conduct[ing] a cost-benefit analysis with the participation of both the financial services industry and law enforcement, to determine and quantify both the benefits to the public of such a system and the cost to all parties affected by any such potential regulatory requirement."[223] FinCEN projects that the implementation of such a system would require three and one-half years of labor and $32 million in investment over that time period.[224]

---

[220] *See* Memorandum by the Am. Civil Liberties Union and Privacy Int'l for the Article 29 Working Party of the European Comm'n 1–5 (Sept. 14, 2006), http:www.aclu.org/pdfs/safefree/boozallen20060914.pdf.

[221] Section 6302 of the Intelligence Reform and Terrorism Prevention Act of 2004 requires the Secretary of the Treasury to "prescribe regulations requiring such financial institutions as the Secretary determines to be appropriate to report . . . certain cross-border electronic transmittals of funds. If the Secretary determines that reporting of such transmittals is reasonably necessary to conduct the efforts of the Secretary against money laundering and terrorist financing." Intelligence Reform and Terrorism Prevention Act of 2004, 31 U.S.C. § 5318(n) (Supp. IV 2000). Before prescribing the regulations, the Secretary of Treasury has to submit a report to Congress that identifies the information that will be reported, how it will be reported, what technology is necessary for FinCEN to manage the data, and the steps that will be taken to protect the data. *See id.*

[222] Press Release, U.S. Dep't of the Treasury Fin. Crimes Enforcement Network, FinCEN Report to Congress States that the Reporting of Cross-Border Wire Transfer Data is Technically Feasible for the Government but Requires Further Collaboration (Jan. 17, 2007), http://www.fincen.gov/news_release_cross_border.pdf.

[223] *Id.*

[224] U.S. DEP'T OF THE TREASURY, FIN. CRIMES ENFORCEMENT NETWORK, FEASIBILITY OF A CROSS-BORDER ELECTRONIC FUNDS TRANSFER REPORTING SYSTEM UNDER THE BANK SECRECY ACT 21–22 (2006), http://www.fincen.gov/cross_border/CBFTFS_Complete.pdf [hereinafter FEASIBILITY OF FUNDS TRANSFER REPORTING SYSTEM].

While a U.S. cross-border electronic funds reporting system will undoubtedly improve the U.S. AML/CFT capabilities, it will track the cross-border financial transactions only of U.S. banking and financial institutions. Thus, it cannot act as a replacement for the TFTP because TFTP monitors all of the international transactions stored by SWIFT. The United States, however, can encourage and support other FIUs in developing similar cross-border electronic reporting systems.[225] In promoting a global network of FIUs that monitor and store cross-border financial transactions, the United States can achieve its AML/CFT goals without circumventing the current system of financial information exchange and without further straining diplomatic relations, especially with the Member States of the European Union.

B. The United States Should Follow the Existing System of Financial Information Exchange for PNR Data Transfers

Likewise, the United States' efforts to protect its borders from terrorists could be substantially benefited by the adoption of a network of global travel information modeled after the FIU network of financial information exchange. Besides improving the terrorist-tracking capabilities, such a system would appease the E.U. data protection authorities because the E.U. Member States would have full oversight and control over the data. A system modeled after the FIU network of financial information exchange also constitutes the multilateral approach that the European Union has been advocating since before the passage of the Original Agreement.[226]

Although the Revised Agreement does address some of the concerns of the E.U. data protection authorities, it does not go far enough to ensure that PNR information transfer abides by the Data Protection Directive. For example, while the Revised Agreement appears to solve the push-pull problem,[227] a system modeled after the current FIU network would provide even more data protection. That is, because of pre-existing fears that the United States will discontinue airline service for the E.U. airline companies operating in and through the United States, the E.U. airline companies

---

[225] FinCEN, through its Office of Global Liason, already advises developing FIUs on all relevant AML/CFT efforts. FEASIBILITY OF FUNDS TRANSFER REPORTING SYSTEM, *supra* note 224, at 42. In addition, Australia's FIU, the Australian Transaction Report & Analysis Centre (AUSTRAC), and Canada's FIU, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), already require their domestic financial institutions to report cross-border wire transfers to their respective FIU. Werner *supra* note 209, at 11. In fact, both AUSTRAC and FINTRAC have aided FinCEN in developing its own cross-border reporting system by providing FinCEN with demonstrations of their respective systems and recommendations on how to design and implement such a system. *Id.*

[226] *See Communication*, *supra* note 50, at 9.

[227] *See supra* Part II.A.5.

may feel pressure to abide by all requests, even those that do not fully abide by the provisions set forth in the Revised Agreement. Additionally, U.S. Customs has already had full access to the E.U. airline companies' databases through the Original Agreement. This history of open access helps to create a somewhat normative standard of full disclosure.

1. The Proposed Model

A global traveler information network modeled after the FIU network of financial information exchange and guided by the principles of the FATF's Forty Recommendations and Nine Special Recommendations could be relatively simple in both design and practice. Each country would enact legislation establishing a travel intelligence unit (TIU) as an autonomous agency or ministry. The TIU would collect limited sets of information[228] on airline passengers[229] traveling within and outside of its borders. The information would then be stored in a secure database for a limited duration—possibly less than the current three and one-half year timeframe. In order to obtain information on suspected international criminals,[230] domestic law enforcement officials would have to follow a similar process of obtaining information from the TIU that they have to follow in order to obtain information from their country's FIU.[231] TIU-to-TIU information exchanges would be guided by memorandums of understanding, similar to those in place for the existing FIU-to-FIU exchange. Just as an FIU's ability to share information (which would otherwise most likely be protected under its country's data privacy laws) with other FIUs is determined by law or statute,[232] so to would the TIU's ability to share information internationally be determined by statute.

The TIU method of PNR data exchange is quite similar to the current transfers of PNR data from the European Union to the United States, but with two major changes. First, the requesting country's TIU has to deal with another TIU, not with an airline carrier. This government-to-government exchange, as opposed to the commercial entity-to-government exchange, significantly increases the oversight of the transaction. The same government that is responsible for upholding the privacy protections of its

---

228 The efficacy of the TIU method of PNR data exchange depends on its ability to serve as a investigatory tool for law enforcement authorities from across the globe.

229 Passenger data could also be collected using other forms of international mass-transit where advance ticketing systems are utilized, including commercial train, boat, and bus travel.

230 In this context, suspected international criminals means persons allegedly involved in serious international crimes, including but not limited to terrorist-related activities, money-laundering, drug trafficking, war crimes, etc.

231 *See supra* notes 195–201 and accompanying text.

232 FIU OVERVIEW, *supra* note 159, at 66.

citizens would also be accountable in sharing PNRs with other governments. Second, this arrangement puts the onus on the country requesting the data, as opposed to the current system where the burden lies on the commercial airline carriers.

To further increase cooperation and oversight, the intelligence activities of the TIUs could be supported and periodically monitored by a central international organization like the Financial Action Task Force. As recognized by the European Commission, the transfer of PNR data is truly an international problem.[233] The Commission posited that the best solution would be multilateral with the International Civil Aviation Organization[234] representing the best forum to bring forth such a multilateral initiative.[235]

The International Air Transport Administration (IATA), [236] on the other hand, categorically opposes "[a]ny movement toward intergovernmental regulation of PNR construction, whether through introduction of Standards by ICAO . . . or through the imposition of any State's national legislation."[237] The IATA argues that "any movement to impose changes on the industry with respect to the way that PNR's are constructed stored or exchanged would require a massive restructure of the entire industry's underlying [information technology] base."[238] Instead, the IATA has advocated Advanced Passenger Information systems, in which passenger data is transmitted to the border control authorities of the receiving country allowing the border control authorities to perform watch-list checks.[239] After the checks are run, the authority would then send a message back to the airline carrier confirming or denying boarding privileges.[240] While Advanced Passenger Information may serve as an effective one-time security screening process, it does not afford law enforcement authorities with the tracking and investigatory tools that PNR systems provide. Furthermore, the IATA's analysis assumes that the standard would be the current system of PNR

---

233 *Communication*, *supra* note 50, at 9.

234 *See id.* and accompanying text.

235 *See Communication*, *supra* note 50, at 10.

236 The International Air Transportation Administration (IATA) is a global trade organization with approximately 240 airline-members, which comprise roughly ninety-four percent of the international scheduled air traffic. IATA, About Us, http://www.iata.org/about/ (last visited Oct. 28, 2007). Its mission is to represent, lead, and serve the airline industry. *Id.*

237 ICAO, *Airline Reservation System and Passenger Name Record (PNR) Access by States*, ICAO Doc. FAL/12-WP/74 para. 5.4 (2004) [hereinafter IATA Presentation to ICAO], *available at* http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp074_en.pdf.

238 *Id.* at para. 3.4.

239 INT'L AIR TRANSP. ADMIN., ANNUAL REPORT 26 (2006), http://www.iata.org/iata/Sites/agm/file/2006/file/annual_report_06.pdf.

240 *Id.*

transfers, not the multilateral framework that this Note recommends. In fact, the IATA later concedes that a system where the airline carriers extract raw PNR data from their systems and transmit it to a secure intermediate body to be cleaned—a system similar to the one proposed in this Note—"has gained a certain level of support amongst governments and airlines."[241]

Although a multilateral approach represents the best solution to this date transfer problem, the International Civil Aviation Organization may not represent the best medium for managing a multilateral initiative. The ICAO is a UN Specialized Agency, and as with any UN agency, it is subject to the bureaucratic constraints of the UN. Both the FATF and the Egmont Group, on the other hand, are independent of UN bureaucracy and function as independent groups with specific, specialized goals and objectives.[242] In addition, the independent-agency framework allows each country to further its own specific criminal policy considerations while at the same time receiving centralized guidance from one or more specialized organizations.

2. Implementation of the Model

Before drafting Transportation Intelligence Unit legislation, the United States and other developed nations should conduct a series of consultations with the private sector and the International Civil Aviation Organization.[243] These consultations will aid in drafting legislation that will be the least burdensome on the private sector and most efficient in carrying out the goals of PNR exchange.[244] In addition, the consultations will help to build confidence in the TIU concept and in each country's own TIU on the part of the institutions that will be charged with submitting the PNR data to the TIU.[245]

Next, each country will need to determine how the TIU will be financed.[246] This undoubtedly will be one of the greatest, if not, the greatest challenge to implementing a global travel intelligence network. The International Air Transport Administration claims that since the collection of PNR data by a government agency is an intelligence gathering operation, the associated costs "should be borne solely by the government(s) requesting . . . data."[247] Although the IATA's premise is generally correct, it fails to take into account the reciprocal benefits that the airline carriers will receive from

---

241 IATA Presentation to ICAO, *supra* note 237, para. 4.5.

242 *See* discussion *supra* part III.

243 *See* FIU OVERVIEW, *supra* note 159, at 7.

244 *Cf. id.* (discussing countries' consultations with the private sector prior to setting up FIUs).

245 *See id.*

246 *See id.* at 8.

247 IATA Presentation to ICAO, *supra* note 237, para. 4.4.

a system that will give airline passengers more confidence in air travel security. With that being said, the contributions of the airline carriers should be small and in proportion to their presence within that country's air travel market. Thus, the brunt of the financing will need to be borne by each respective government. To help reduce operational costs, the TIU could be located within another ministry or government agency.[248] In addition, the TIU could borrow technology, procedures, and expertise from its country's FIU to keep costs at a minimum.

Finally, the implementation of such a network of travel intelligence information also would be subject to country-specific restraints and requirements. For instance, in the United States, as mandated by the E-Government Act of 2002,[249] the Department of Homeland Security would have to conduct a "privacy impact assessment" prior to developing such a system.[250] A privacy impact assessment is defined as:

> [a]n analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[251]

3. Anticipated Objections and Problems with the Proposed Model

There are several possible objections to the cross-border travel intelligence system described above. The first possible challenge is that the European Union is not concerned with terrorists flying from the United States into Europe, and thus, the principle of reciprocity, which is vital to the effective operation of FIUs, would be lacking entirely. There are three responses to this objection: (1) as evidenced by the Revised Agreement, the European Union is considering implementing a PNR transfer system similar to that of the United States;[252] (2) once the system becomes more globalized, countries like the European Union will be able to receive PNR data from countries with a higher concentration of suspected terrorists; and (3) the data collected by the TIUs could be used to track other persons who are

---

248 *See* FIU OVERVIEW, *supra* note 159, at 8.

249 E-Government Act of 2002, Pub. L. No. 107-347 § 208, 116 Stat, 2899, 2921–22 (codified as amended in scattered sections of 44 U.S.C.).

250 *Id.*

251 Memorandum from Joshua B. Bolten, Dir., Office of Mgmt. and Budget to the Heads of Executive Departments and Agencies (Sept. 26, 2003), http://www.whitehouse.gov/omb/memoranda/m03-22.html.

252 *See* Revised Agreement, *supra* note 71, at 24.

suspected of committing serious international crimes.[253] In fact, in the December 12, 2003 Communication to the European Council and Parliament, the Commission stated that "any possible information exchange with the US authorities should be based on a system of reciprocity in the transfer of data between the EU and the US, whilst at the same time considering the possibility for the collection and controlled transfer of PNR-data through a central European entity."[254]

Second, a comprehensive cross-border travel intelligence system would actually represent a greater invasion of privacy than the current arrangement between the United States and the European Union because all passengers flying internationally would have their information collected by their country's TIU. As noted by the International Air Transport Administration, despite the fact that "only the United States, Canada, Australia, and New Zealand have legislation in place that makes government access to airline reservation data mandatory[,] [a] number of other [countries] are exploring this process as an additional component of their border security strategy, and it is likely that more such requirements will be imposed in the [future]."[255] As more countries consider introducing PNR legislation, the need for a multilateral solution only grows stronger. Additionally, an international travel intelligence system may have important applications outside of fighting international crime. For instance, it could be invaluable in tracking and quarantining passengers exposed to infectious disease outbreaks.

Third, much of the effectiveness of the FIUs' ability to combat terrorist financing and money-laundering operation comes from the activities of the individual financial institutions, including their reporting of suspicious activities. Because airlines deal with passengers on more of a single-transaction basis, they would have less background information and would have to make decisions on a particular passenger given his or her appearance, demeanor, or behavior. Obviously, this is not an optimal result given the room for racial and ethnic profiling and harassment. Therefore, instead of selectively reporting suspicious transactions, the airline would simply have to report all transactions involving international travel to its respective TIU. This removes any possibility of profiling by the airline carriers. In addition, airline carriers, airport security, and the Federal Aviation Authorities would all have to report other major security-related instances to its TIU—for instance, when a passenger is detained for security reasons before, during, or after his or her flight.

---

253 In order to prevent governments from abusing the PNR data, the TIU's disclosure to law enforcement officials should be limited to serious international crimes, including but not limited to: drug trafficking, money laundering, and espionage.

254 *Communication*, *supra* note 50, at 9.

255 IATA Presentation to ICAO, *supra* note 237, para. 1.3.

A final potential objection to a comprehensive cross-border travel intelligence system is that it would be an enormous undertaking, too complex for many undeveloped and developing nations. While such an undertaking would be a substantial enterprise for undeveloped and developing nations, the G-7, led strongly by the United States, could pilot such a program at first and then provide financial incentives for developing nations to implement their own TIUs. To address the problems that the small developing island economies, such as those in parts of the Caribbean and the South Pacific, are having in establishing their own FIUs,[256] the International Monetary Fund and the Egmont Group envisage establishing "an organization to support national FIUs in the subregion, rather than a regional FIU" because according to the Egmont Group and the Financial Action Task Force, FIUs are *national* entities.[257] Similar sub-regional organizations could be established to support the developing nations in initiating their own TIUs.

V. CONCLUSION

In order to effectively combat terrorist-related activities and other serious international crimes, law enforcement authorities must identify terrorists and other international criminals during the only two instances in which they reveal themselves to the international community—when they travel abroad and when they transact abroad. Recognizing this notion nearly two decades ago, the United States and other global powers began sharing information pertaining to financial transactions for the purpose of combating money-laundering and its support of the international drug trade.[258] Then, after the September 11, 2001 terrorist attacks, both governments started using this financial information sharing network to combat terrorism. During the same period, the United States began secretly subpoenaing financial records from SWIFT under TFTP. It also passed legislation that required air carriers "operating a passenger flight in foreign air transportation to the United States [to] provide the Commissioner of Customs [with PNR data],"[259] and that would eventually require the United States and the European Union to agree on how the E.U. airlines would provide that PNR data.

---

256 In general, the developing economies experience four main problems in establishing an FIU: (1) finding staff sufficiently knowledgeable in financial investigations, forensic accounting, and other AML/CFT tasks; (2) achieving the same economies of scale as the larger FIUs, which deal primarily with formal banking and fund-transfer networks; (3) establishing a relationship of reciprocity and trust with other established FIUs; and (4) finding adequate financial commitments. *See* FIU OVERVIEW, *supra* note 159, at 30–31.

257 *Id.* at 31.

258 STESSENS, *supra* note 141, at 15–17.

259 49 U.S.C 44909(c) (Supp. IV 2000).

While the PNR data transfers and the TFTP maintain the appropriate focus of identifying suspected terrorists when they reveal themselves to the international community, they do not provide adequate privacy protection for citizens of foreign countries. Therefore, a careful balance must be struck between tracking down suspected international criminals—including terrorists—and the protection of privacy rights. In order to strike this delicate balance, (1) the United States should terminate the TFTP immediately and improve the existing system of financial information exchange to satisfy its AML/CFT needs, and (2) the United States and the European Union should work to develop an international system of travel information exchange based on the existing model of financial information exchange.