amsterdamlawforum
VU University Amsterdam

TRACKING TERRORIST FINANCES: THE 'SWIFT' PROGRAM AND THE AMERICAN ANTI-TERRORIST FINANCE REGIME

*David B. Bulloch, LL.M. **

Abstract

This article examines the political and legislative history of a formerly classified anti-terrorist finance program initiated in the days after 9/11 that subpoenaed millions of financial records from the Belgian-based Society for Worldwide Interbank Financial Telecommunications (SWIFT) without the knowledge of European authorities. The European outrage in response to its public disclosure in 2006 — and the subsequent struggle to generate support for the continuation of the program — has been interpreted by many as further evidence of a strategic divide concerning American and European efforts to thwart terrorism. This research will investigate the dramatic changes to the American anti-terrorist finance regime after 9/11, and will demonstrate that the European reluctance to cooperate with this program represents a fundamental disagreement concerning the prioritization of privacy rights rather than an unwillingness to take the steps necessary to combat the financing of terror.

Introduction: "Following the Money" to Save Lives

In the years since 9/11, Western decision-makers have developed a number of security policies based on the assumption that the "knowledge about future risk is *always already present* in the data, if only information on transaction patterns can be effectively integrated and mined."[1] In fact, a joint inquiry in 2003 concluded that, "on September 11, enough relevant data was resident in existing databases" so that "had the dots been connected, the events could have been exposed and stopped."[2] For the United States, the ability of Al-Qaeda to use the global banking system to finance terror was extremely unsettling. Upon their arrival in the US, the 9/11 hijackers opened bank accounts in their real names, and proceeded to transfer funds ranging from

* *The author has studied American politics, international relations, and terrorism, and was previously an archival intern at the Richard M. Nixon Presidential Library in Yorba Linda, California. He holds a B.A. in Political Science from California State University Fullerton (2009), and a Research LL.M. specializing in the 'Law and Politics of International Security' from VU University Amsterdam (2011).*

[1] Amoore & de Goede, 'Transactions After 9/11: The Banal Face of the Preemptive Strike', *Transactions of the Institute of British Geographers* 2008 -33(2), p. 174. Emphasis in the original.

[2] See US Joint Inquiry, *Report of the Joint Inquiry into the Terrorist Attacks of September 11, 2001*. House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, Washington, DC 2003, p. 14. Cited in Amoore & de Goede (2008), *ibid.*

$5,000 to $70,000 between them.[3] Although the 1970 Bank Secrecy Act had previously placed an affirmative duty on financial institutions to report suspicious transactions, the existing banking regulations failed to detect the transfers between the hijackers — and the $130,000 in 9/11 seed money sent from banks in Germany and the United Arab Emirates — because the transactions were not necessarily inconsistent with the student profiles the terrorists had established. The relatively small amounts of money required to carry out these attacks however, and the ease with which the hijackers utilized the 'Western' financial system to facilitate terror, significantly refocused the American regulatory regime squarely on stemming the flow of funds to terrorists.

The war on terrorist finance has become central to the larger 'War on Terror' because it is assumed that tracing financial transactions is a way to deduce the intentions of terrorists, as well as track and apprehend them before they commit violent acts. In the words of Juan Carlos Zarate, the former deputy National Security Advisor and the first assistant secretary of the Treasury for Terrorist Financing and Financial Crimes: "Financial records and audits provide blueprints to the architecture of terrorist organizations. By following the money trail through financial information sharing worldwide, we can save lives by unearthing terrorist cells and networks."[4] Law enforcement officials highly value financial information due to the belief that "money trails don't lie,"[5] that they are like a "fuel for their intelligence engine, […] contain a wealth of identity information, […] and amount to a new kind of weapon in the amorphous war on terror."[6]

This article will investigate the dramatic changes to the American anti-terrorist finance regime after 9/11, and will explore the legislative and political history of the 'Terrorist Finance Tracking Program' (TFTP) as an example of this renewed interest in preventing the abuse of the global financial system.

I. The History of the 'Terrorist Finance Tracking Program'

On June 23, 2006, Eric Lichtblau and James Risen of the New York Times were the first to reveal the existence of a highly classified Bush administration program developed in the weeks after 9/11 to identify and track terrorists and

---

[3] See Roth, Greenburg, & Willie, 'National Commission on Terrorist Attacks Upon the United Stated of America', *Monograph on Terrorist Financing: Staff Report to the Commission* 2003, pp. 32-34, at: http://www.9-11commission.gov/staff-_statements/911_TerrFin_Monograph.pdf (July 2011).

[4] J. Zarate, 'Bankrupting Terrorists', *The Global War on Terrorist Finance*, US Department of State, eJournal USA 9(3) September 2004, at: *www.usembassy-mexico.gov/bbf/ej/ijee0904.pdf* (July 2011).

[5] S. Levey, 'Remarks before the American Enterprise Institute for Public Policy Research', Washington, D.C., 8 September 2010, at: http://www.treasury.gov/press-center/press-releases/Pages/hp86.aspx (July 2011).

[6] R. O'Harrow, *No Place to Hide*, New York: Free Press 2005, p. 260.

their financial supporters. A joint initiative between the Central Intelligence Agency (CIA) and the US Department of the Treasury, the 'Terrorist Finance Tracking Program' (TFTP) was designed to allow counterterrorism officials to examine a vast international database of financial transactions relying on the messaging infrastructure of the Society for Worldwide Interbank Financial Telecommunications (SWIFT).[7] Established in 1973 by a consortium of European financial institutions, the Belgian-based SWIFT does not actually handle or exchange money, but rather processes transfer instructions and supplies standardized messaging services and interface software to more than 8,000 financial institutions in 206 different countries.[8] The Belgian Data Privacy Commission has analogized SWIFT's services to a series of envelopes and letters. The 'envelopes' contain information about the financial institutions facilitating the transaction, as well as the date and time of the transfer. The 'letters,' on the other hand, are encrypted messages disclosing the amount and method of the transfer, and information identifying the parties involved. SWIFT routes approximately six trillion dollars daily through an average of 15 million transactions between banks, brokerages and other financial institutions — two thirds of which originate in Europe.[9] Because of the widespread use of SWIFT's messaging services among international financial institutions, the TFTP is envisioned as a vital pre-emptive tool that provides a "unique and powerful window into the operations of terrorist networks."[10]

Six days after the public revelation of the TFTP, the US House of Representatives passed a resolution voicing their support for the program as lawful, condemning the unauthorized disclosure of a classified intelligence operation, and calling on the news media to refrain from publishing further classified information.[11] The Belgian Data Protection Authority and the European Union's Article 29 Data Protection Working Party, however, disagreed with the legality of the program, and argued that the TFTP was a violation of the 1995 EU Data Privacy Directive.[12] Despite these conclusions, the Bush

---

[7] See Lichtblau & Risen, 'Bank Data is Sifted by US in Secret to Block Terror', *New York Times*, A-1, 23 June 2006, at:
http://www.nytimes.com/2006/06/23/washington/23intel.html (June 2011).

[8] SWIFT, *About Swift*, Company Information 2011, at: http://www.swift.com (June 2011).

[9] J.Santolli, 'The Terrorist Finance Tracking Program: Illuminating the Shortcomings of the European Union's Antiquated Data Privacy Directive', *The George Washington University International Law Review* 2008-40, pp. 559-560.

[10] S. Levey, US Treasury Department. Lichtblau & Risen 2006, *supra* note 7.

[11] US House Resolution 895, 109th Congress, in: Elsea & Murphy, 'Treasury's Terrorist Finance Program's Access to Information Held by the Society for Worldwide Interbank Financial Telecommunications (SWIFT)', *Congressional Research Service Report for Congress*, 7 July 2006.

[12] Parliament and Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L281/40) [hereinafter Data Privacy Directive]; Belgian Data Protection Authority, Summary of the Opinion of the Transfer of Personal Data by SWIFT Following the US Treasury, at: www.steptoe.com/assets/attachments/2644.pdf;

administration made it clear that the United States would not voluntarily abandon a program they considered an important tool allowing them to "choke off funds for the terrorists,"[13] and thus began a highly politicized privacy debate that would significantly strain transatlantic counterterrorism cooperation for years to come.

It has been suggested that the European Union's Data Privacy Directive, with its ability to create a potential 'information embargo,' is perhaps the world's 'first universal data privacy regime.' Because the privacy of an individual's data is viewed by many European legislators as a fundamental human right, and due to the fact that a number of countries are attempting to develop their own data privacy regulations to satisfy the 'adequacy standards' of the Data Privacy Directive, the resolution of the controversy involving SWIFT's participation in the TFTP is significant for several reasons.[14] Not only does it serve as a global precedent for states attempting to balance privacy protection and effective counterterrorism policy, but the legislative history of the TFTP also clearly demonstrates how the perception of and response to the risk of terrorist financing is largely influenced by social and political considerations. In order to fully understand the development and significance of the TFTP, the next section will examine the extent to which the post 9/11 War on Terrorism Financing represents a marked break with earlier regimes of American anti-terrorist finance regulation.

II. The American Anti-Terrorist Finance Regime Before 9/11

Unlike many European countries with previous experience combating domestic and international terrorism, the US administrative structure was not actively concerned with anti-terrorist finance before the attacks on 11 September 2001. Because successful prosecution would have required tracing donor funds to a particular attack, the Department of Justice tended not to bring serious criminal charges against individuals who contributed to terrorists organizations, relying instead on minor charges they hoped would disrupt terrorist operations. In addition to after-the-fact claims that the political climate prior to 9/11 would not have allowed them to investigate religious charities for suspected ties to terrorism, the FBI was also concerned that opening a criminal investigation in more serious cases would prevent them from using broader powers under the Foreign Intelligence Surveillance Act to place suspects under surveillance.[15] The relatively small amounts of money required to conduct terrorist operations convinced law enforcement officials that there were more efficient ways to fight terrorism than attempting to trace the flow of illicit funds, and

---

Article 29 Data Protection Working Party, Opinion 10/2006: On the Processing of Personal Data by SWIFT, 01935/06/EN WP128, 22 November 2006, at: http://eceuropa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_en.pdf (July 2011).

[13] D. Perino, deputy White House press secretary, Lichtblau & Risen 2006, *supra* note 7.

[14] Santolli 2008, *supra* note 9, pp. 554-555.

[15] Roth, Greenburg, & Willie 2003, *supra* note 3.

government agencies seemed largely uninterested or incapable of conducting successful anti-terrorist finance campaigns. Neither the Federal Bureau of Investigation (FBI) nor the Department of Justice had a single unit solely dedicated to the financing of terrorist organizations, and when investigations were initiated they were significantly complicated by bureaucratic turf battles between the agencies.[16]

With specific regard to Al Qaeda, like the Department of Justice and the FBI, the Central Intelligence Agency (CIA) believed that efforts to monitor the terrorist money trail were inefficient, but based their beliefs on the erroneous assumption that Usama bin Laden largely financed the organization's operations with his personal fortune.[17] The National Security Agency (NSA) did have a small contingent of staff focusing on terrorist financing, but at that time they lacked effective foreign language capabilities. The US Treasury Department had the Office of Foreign Assets Control (OFAC) running the Foreign Terrorist Asset Tracking Center (FTATC), but they too were plagued by bureaucratic infighting with the CIA. The Treasury's Financial Crimes Enforcement Network (FinCEN) was established in 1990 to combat money laundering by facilitating cooperation between federal law enforcement and financial institutions, but they tended to focus on Russian money laundering and other crimes of a more urgent nature than terrorism. The only organization that paid any serious attention to terrorist financing before 9/11 was the National Security Council (NSC), where Richard Clarke established an inter-agency effort after the 1998 East Africa embassy bombings that included the Treasury Department, the CIA, the FBI, and the State Department. Initially concerned with determining the assets of Usama bin Laden, it was this NSC-led interagency group that would eventually discredit the CIA's erroneous assumption that bin Laden himself was the primary source of funding for Al-Qaeda.[18]

According to Laura Donohue, the US administrative structure was "not alone in exhibiting malaise," as the legal framework addressing terrorist financing "arose rather late in the game," and only began to directly focus on stemming the flow of funds to international terrorist organizations after the attacks on 9/11.[19] Three streams of legislative authority flowed into the American anti-terrorist finance regime before 9/11 prompted a dramatic shift in legal and administrative focus. The first of these was the Trading With the Enemy Act (TWEA) of 1917, which allowed the president to "investigate, regulate […] prevent or prohibit […] transactions" during a time of war or national emergency.[20] This statute was originally intended to prevent individuals within the US from conducting trade with declared enemies during a time of war, and

[16] *Ibid.*, p. 33.
[17] *Ibid.*, p. 20.
[18] L. Donohue, 'Anti-Terrorist Finance in the United Kingdom and the United States', *Michigan Journal of International Law* 2006-27, pp. 349-350.
[19] *Ibid.*, p. 350.
[20] *Ibid.*; See 50 U.S.C.S. appendix § 3.

was subsequently amended by Congress in 1933 to apply during times of national emergency. Executive overreach during the Richard Nixon administration led congress to revoke and replace this statute in 1977 with the International Emergency Economic Powers Act (IEEPA), although the TWEA remains in force to this day during times of war.[21] The IEEPA gave the President the ability to declare a national emergency in response to a specific threat located wholly or mostly outside of the US, at which time he is authorized to designate individuals or entities a threat to national security, freeze their assets, and make it illegal for any US citizens to conduct transactions with those designated. Within ten days of this designation, the president is required to submit a report to the Treasury's Office of Foreign Assets Control (OFAC), who informs financial institutions that then become subject to criminal or civil penalties if they fail to comply with the order.[22] Libya and Cuba were the subjects of early uses of the IEEPA, and in the 1990s non-state actors like Palestinian organizations and Columbian drug cartels were included as threats to national security under this statute. President Bill Clinton issued Executive Order 12,947 under the IEEPA in 1995, blocking the US assets of those threatening to disrupt the Middle East peace process, and creating the 'Specially Designated Terrorist List.'[23] Usama bin Laden was not added to the list until Executive Order 13,099 included him and a number of key aides after the 1998 East Africa embassy bombings,[24] and in retribution for their protection of Bin Laden, financial transactions with the Taliban were subsequently blocked in 1999.[25]

The second stream of legislative authority resulted from the bombing of the Federal Building in Oklahoma City in 1995. Although the attack was planned and executed by US citizens, a number of the provisions Congress incorporated into the 1996 Antiterrorism and Effective Death Penalty Act (AEDPA) dealt with foreign threats. Section 321 criminalized financial transactions between US citizens and those designated under the 1979 Export Administration Act as state sponsors of terrorism, except where special permission had been given by the Treasury in consultation with the State Department. Section 302(a) provided a legislative supplement to Clinton's Executive Order 12,947, and made it a crime to provide "material support or resources to a foreign terrorist organization."[26] The term 'material support,' however, was defined rather broadly, and included financial securities and services, lodging, training, advice, assistance, food, transportation, weapons, or any other physical asset other than medicine and religious materials.[27]

---

[21] *Ibid.,* p. 351; Trading With the Enemy Act, 50 U.S.C para. 1702(a)(1) (1977).
[22] *Ibid*.
[23] Executive Order No. 12,947, 60 Fed. Reg. 5,079 (23 January 1995), *reprinted as amended in* 50 U.S.C.A. para. 1701 (2003).
[24] Executive Order No. 13,099, 63 Fed. Reg. 45,167 (20 August 1998).
[25] Donohue 2006, *supra* note 18, p. 352.
[26] Anti-terrorism and Effective Death Penalty Act § 321; 302(a), *codified in* 18 U.S.C. §2339B.
[27] Donohue 2006, *supra* note 18, p. 353.

The third legislative stream relating to anti-terrorist finance flows from efforts to prevent laundering the proceeds from drug trafficking, and tended to focus on creating a paper trail to assist in the investigation and prosecution of violations of the tax and criminal code. In addition to the 1998 Money Laundering and Financial Crimes Strategy Act calling for cooperation between the Treasury and law enforcement in creating a national strategy to combat money laundering,[28] three additional pieces of legislation formed the due diligence standard to which financial institutions were held before the 9/11 attacks. The Bank Secrecy Act and Regulations of 1970 required individuals to report transactions to the Treasury that moved more than $10,000 into or out of the US, and obliged financial institutions to file Suspicious Activity Reports (SARs) with the Treasury's FinCEN within 30 days of detecting suspicious financial activity. The rationale behind such a regulation was that private industry was in a better position to detect the illicit transfer of funds, and that having a non-government entity filing the reports would also protect customer privacy. The statute required financial institutions to 'know' their customers, the source of their funds, and whether their transactions matched their customer profile.[29] The Anti-Drug Abuse Act of 1988 made it a crime to knowingly assist in money laundering, to handle transactions of more than $10,000 derived from criminal proceeds, or to structure transactions to attempt to avoid statutory reporting requirements.[30] The third piece of legislation was Title XV of the 1992 Housing and Community Development Act, which gave regulatory officials the authority to seize the assets of financial institutions that violated money laundering statutes. This measure effectively required an even broader range of financial institutions to file SARs with the Treasury's FinCEN, although the determination of what constituted 'suspicious activity' was largely left up to the institutions.[31]

While pre-9/11 terrorist measures required that the defendant be tied specifically to the commission of a particular act, money laundering statutes only required that the funds could be traced to a specific unlawful activity. As Donohue has argued, although these measures "had teeth, and were steadily becoming more extreme, when held against the dramatic changes post September 11, they appear almost mild."[32] Before 11 September, the financial industry was actively lobbying against further intrusion into and regulation of the financial world, and the Clinton and Bush administrations for their part seemed reluctant to force the issue. In 1994, for example, the Treasury Department was instructed by Congress to begin regulating "money services

[28] Money Laundering and Financial Crimes Strategy Act of 1998, Pub. L. 105-310, 112 Stat. 2941.
[29] Bank Secrecy Act of 1970, Pub. L. No. 91-508, 84 Stat. 1114 (1970) (*codified as amended in parts of* 12 U.S.C., 15 U.SC., 18 U.S.C, and 31 U.S.C.).
[30] Anti-Drug Abuse Act of 1988, Pub. L. No. 100-690, 102 Stat. 4181 (1988).
[31] Title XV (Annunzio-Wylie Anti-Money Laundering Act) of the Housing and Community Development Act of 1992, Pub. L. No. 102-550, 106 Stat. 3672.
[32] Donohue 2006, *supra* note 18, p. 359.

businesses" like check cashers, wire transfers, money orders, and traveller's checks. The Treasury drafted regulations in 1997, but they were not issued for another two years, and were not scheduled for implementation until 31 December 2001. Before the 9/11 attacks, it has been suggested that the Bush administration planned to follow in the Clinton administration's footsteps, and further delay implementation until late 2002 to allow more time for the government to 'educate' financial institutions about their obligations.[33] When the Treasury Department proposed stronger 'know your customer' requirements in 1998, they were bombarded with over 200,000 negative responses spanning the entire political spectrum, and they eventually withdrew their proposal when the Congress began openly contemplating rolling back the controls that were already in place. The Money Laundering Control Act of 2000, which would have given the Treasury control over foreign banks with accounts in the US, was also soundly rejected by the Congress,[34] reaffirming the assertion that neither the legislative nor the administrative structure was actively concerned with the threat of terrorist financing before terrorists struck the financial and political heart of the United States on 11 September 2001.

III. The Post-9/11 Anti-Terrorist Finance Regime

Before 9/11, the Bush administration and many in the government had been reluctant to support new money laundering laws or put political pressure on financial institutions, but after the attacks financial regulation increasingly became central to the larger War on Terror. As the chairman of the Senate Banking Committee, Phil Gramm boasted in early 2001 that he had personally killed the Clinton administration's anti-money laundering legislation.[35] Two months before 9/11, Secretary of the Treasury Paul O'Neill announced his intention to "ease the US regulatory regime and depend on international cooperation rather than threats of sanctions for combating illicit money flows." When the NSC had previously attempted to establish a terrorist asset tracking center, O'Neill led the charge against it.[36] One month after 9/11, however, Secretary O'Neill favoured the development of special anti-terrorist finance regulation and stringent compliance monitoring.[37]

In the administrative realm, immediately after 9/11 the Department of Justice created the Terrorist Financing Unit to coordinate the effort to prosecute the financing of terrorism. The FBI established a Financial Review Group, later renamed the Terrorist Financing Operations Section (TFOS), to investigate the financing of the September 11 attacks. Located within the FBI's counterterrorist division, the unit represented the first single-office coordinating effort on

[33] *Ibid.*
[34] *Ibid*.
[35] M. de Goede, 'Financial Regulation and the War on Terror', in: Assassi, Wigan, & Nesvetailova (eds) *Global Finance in the New Century: Beyond Deregulation*, New York: Palgrave Macmillian 2007, p 195.
[36] Donohue 2006, *supra* note 18, p. 370.
[37] De Goede 2007, *supra* note 35, p. 195.

terrorist finance, and included staff from US Customs, the Internal Revenue Service (IRS), banking regulators, Treasury's FinCEN, and the OFAC.[38] The FBI also doubled the number of agents in their Joint Terrorism Task Force (JTTF), and began to include The Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), and the IRS Criminal Investigative Division in their meetings, which increasingly focused on terrorist finance.[39] The CIA also formed a new section on terrorist financing, which coordinated with the Department of Defence (DoD), FBI, and the NSA to collect intelligence, track terrorist funding, and disrupt operations. The Treasury then formed the Financial Action Task Force (FATF) to identify and prioritise which individuals and organizations should be subject to blocking orders, and established the Executive Office for Terrorist Financing and Financial Crimes (EOTF/FC) in an effort to prevent the abuse of the international financial system by terrorists and their financial supporters.[40]

All of these changes illustrate the extent to which the War on Terrorist Finance represents a remarkable turnaround from earlier regimes of anti-terrorist and anti-money laundering regulation. It was now becoming increasingly apparent to the Bush administration and the Congress that a regulatory regime focused on money laundering was of limited usefulness in the fight against terrorist financing because terrorism "dirties clean money," while money laundering attempts to "clean dirty money."[41] As David Aufhauser, the former chairman of the National Security Council on Terrorist Financing has suggested, efforts against money laundering saw the world "observed through the wrong end of a telescope." The concern is no longer with "illicit proceeds of crime looking for a place to hide," but with "clean money intended to kill."[42] The US then sought to evolve their regulatory regime from one designed to confiscate criminal money after the act, to one that is able to predict, pre-empt, and apprehend potential terrorists before they are able to realize their goals.[43]

IV. The Legal Justification of the Terrorist Finance Tracking Program (TFTP)

When President Bush addressed a joint session of Congress on 20 September 2001, he made clear his intention to refocus American efforts to stem the flow of terrorist financing:

> We will direct every resource at our command […] to the disruption and to the defeat of the global terror network. […] We will starve the terrorists of funding […] and we will pursue nations that provide

[38] Roth, Greenburg, & Willie (2003), *supra* note 3, p. 41.
[39] Donohue 2006, *supra* note 18, p. 367.
[40] *Ibid.*, p. 368.
[41] Santolli 2008, *supra* note 9, p. 557.
[42] D. Aufhauser, 'Terrorist Financing: Foxes Run to Ground', *Journal of Money Laundering Control* 2003-6(4), p. 301.
[43] Amoore & de Goede, 'Governance, Risk, and Dataveillance in the War on Terror', *Crime, Law, and Social Change* 2005-43, pp. 152-153.

> aid or safe haven to terrorism. Every nation, in every region, now has a decision to make. Either you are with us, or you are with the terrorists.[44]

The Terrorist Finance Tracking Program was one of these initiatives designed to "starve the terrorists of funding," and it draws its legal justification from two post-9/11 developments: Executive Order 13,224 and the USA PATRIOT Act.

IV.1 Executive Order 13, 224

Less than two weeks after 9/11, President Bush issued Executive Order 13,224 — declaring a national emergency and enabling him to exercise authority under the International Emergency Economic Powers Act (IEEPA).[45] This executive order, which Bush proudly referred to as "Draconian," reflected the administration's desire to avoid not just criminal law but the judicial system altogether in stemming the flow of funds to terrorists, and went some measure beyond Executive Order 12,947 issued by President Clinton in 1995, and section 302(a) of the subsequent AEDPA of 1996. The order essentially replaced a criminal law standard for prosecuting terrorist financers with an intelligence standard, as mere links to terrorists would now be sufficient to prove support, and administrative procedures would come to replace the judicial process.[46] The order began by creating a 'Specially Designated Global Terrorists' (SDGT) list, blocking "all property and interests in property" of those designated. The order then incorporated a list of those the Secretary of State determined were "assisting in, sponsoring, or providing financial, material, or technological support for those listed — and *any persons Treasury determined to be otherwise associated with those listed.*"[47] No longer prohibiting only financial institutions from conducting transactions with those listed, this provision now meant that any business or individual that failed to cease interacting with the listed entities could find themselves listed and have their assets frozen. This also meant that rather than demonstrated material support, individuals and businesses could now be found guilty and have their property seized merely for their association with listed entities. Furthermore, whereas the 1996 AEDPA provided a humanitarian exception for the provision of medicine and religious materials, Executive Order 13,224 now made it a crime for anyone to "make donations to relieve human suffering to persons listed under the order or determined to be subject to it."[48]

---

[44] G.W. Bush, 'Address to a Joint Session of Congress and the American People', Washington, D.C., 20 September 2001, at: http://georgewbush-whitehouse.archives.gov/news/releases/2001 (June 2011).

[45] Executive Order No. 13,224, 3 C.F.R. 786, 790 (2001), *reprinted as amended in* 50 U.S.C.A. § 1701 (2002). President Bush also cited U.N. Security Council Resolutions: S.C. Res. 1214, U.N. Doc. S/RES/1214 (Dec. 8, 1998); S.C. Res. 1267, U.N. Doc. S/RES/1267 (15 October 1999); S.C. Res. 1333, U.N. Doc. S/RES/1333 (19 December 2000); and S.C. Res. 1363, U.N. Doc. S/RES/1363 (30 July 2001).

[46] See Donohue 2006, *supra* note 18, p. 307.

[47] *Ibid.*, p. 377. Emphasis in the original.

[48] *Ibid.*, pp. 377-378.

It has been suggested that since the Treasury's Office of Foreign Assets Control (OFAC) already had the authority under Clinton's Executive Order 12,947 to target money flows to Bin Laden and Al-Qaeda, Executive Order 13,224 was in many ways a public relations effort to convince the public that something was being done.[49] The strength and tone of President Bush's remarks after the signing of the order reaffirm this suggestion:

> Today we have launched a strike on the financial foundation of the global terror network. […] Just to show you how insidious these terrorists are, they oftentimes use nice-sounding, non-governmental organizations as fronts for their activities. […] If you do business with terrorists, if you support or sponsor them, you will not do business with the United States of America.[50]

Treasury Secretary Paul O'Neill made similarly strong remarks:

> If you have any involvement in financing of the Al-Qaeda organization, you have two choices: cooperate in this fight, or we will freeze your US assets; we will punish you for providing the resources that make these evil acts possible. We will succeed in starving the terrorists of funding and shutting down the institutions that support or facilitate terrorism.[51]

IV.2 The USA PATRIOT Act

The second post-9/11 development providing the legal justification for the TFTP, and perhaps the most infamous American initiative in the fight against terrorism is the 'Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism' Act (USA PATRIOT Act). David Aufhauser has called Title III of the PATRIOT Act "the smart bomb of terrorist financing," and it is this section which sets forth the regulations that would thereafter govern the American anti-terrorist finance regime.[52] The PATRIOT Act revolutionized the ability to fight terrorist financing in four key areas: it broadened the President's power under the IEEPA; it significantly expanded the regulatory authority of the state; it strengthened the executive's capacity to freeze and seize assets; and it expanded the United States' extraterritorial jurisdiction.[53]

Title III gave the state an important bargaining tool to use against accused financers by authorizing the executive branch to block assets during the

---

[49] Roth, Greenburg, & Willie 2003, *supra* note 3, p. 45.
[50] Donohue 2006, *supra* note 18, p. 378.
[51] *Ibid*.
[52] Santolli 2008, *supra* note 9, p. 558. See also USA PATRIOT Act, Title III: The International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001), *codified in* 50 U.S.C. §1861.
[53] Donohue 2006, *supra* note 18, p. 371.

pendency of an investigation — which for all intents and purposes meant that assets could be frozen indefinitely. The statute did not allow for funds to be released under exceptions for humanitarian purposes, or even to be set aside for legal defence. The statute also authorized the President, "when the United States is engaged in armed hostilities or has been attacked," to "confiscate any property, subject to the jurisdiction of the United States, of any foreign person, foreign organization, of foreign country that he determines has planned, authorized, aided, or engaged in such hostilities or attacks against the United States."[54] The most extensive changes were in the form of the increased regulatory powers imposed by the state. Financial institutions were required to enhance their customer identification measures to a level just short of the extensive 'know your customer' procedures that had been defeated only two and a half years before. Where the Bank Secrecy Act had previously required banks to report $10,000 or more in cash transfers, The PATRIOT Act now expanded the number of entities required to file SARs, and obliged "any person who is engaged in a trade or business" to file an SAR if they received more than $10,000 in cash. Here Donohue argues that it is important to note that $10,000 in 1970 when the Bank Secrecy Act was passed is equivalent to approximately $2,625 today — meaning that a substantial portion of consumer transaction patterns can now be traced by the government.[55]

In the regulatory arena, Title III expanded the list of 'predicate offences' for which individuals and entities could have their assets seized. A new series of 'special unlawful activities' including foreign criminal offences, foreign public corruption, customs and firearm offences were now included with the aim of preventing corrupt foreign officials from taking advantage of the US banking system. Title III did provide a procedure for contesting the seizure of assets, but the burden of proof would now lie with the accused while simultaneously allowing evidence to be used against them that under normal circumstances would have been impermissible in a court of law.[56] Section 317 of Title III also expanded the United States' extraterritorial jurisdiction, bringing foreign money launderers, banks, and other financial entities within the jurisdiction of the judiciary. If a suspect foreign bank maintained a correspondent account within the US, the state was now authorized to seize the assets during the pendency of an investigation. In situations where a conflict of US and foreign law occurred, the Attorney General as opposed to the judiciary was granted the authority to decide the proper course of action.

V. The Disclosure and Development of the TFTP

Executive Order 13,224 and the PATRIOT Act, which substantially increased the government's power to compel financial institutions to cooperate with law enforcement, provided the legal justification that made the Terrorist Finance Tracking Program possible. The idea for the TFTP emerged from a conversation

[54] *Ibid*.
[55] *Ibid.*, p. 372.
[56] *Ibid.*, p. 376.

between a Wall Street executive and a senior Bush administration official. The administration at that time knew little about the SWIFT consortium, except that the current CEO Leonard Schrank was a New York native, and it was therefore assumed that he would be willing to assist the Treasury in its war on terrorist financing.[57] They soon learned that SWIFT offered "unparalleled access to international transactions," and was in the words of one former government official, "the mother lode, the Rosetta Stone" for financial data.[58] The intelligence community was so anxious to use the SWIFT database that they discussed having the CIA access the system covertly, but the Treasury resisted and favoured petitioning SWIFT directly. This, as it turns out, was not the first time that the US had attempted to access the SWIFT database. Before 9/11, the Treasury department had issued numerous subpoenas to SWIFT, which they had refused because they considered such access "untimely or unduly burdensome.'' During the Clinton administration, however, the CIA covertly accessed the SWIFT database in an attempt to locate Usama bin Laden, but when the Treasury learned of this unauthorized access, they convinced the CIA to cease their activities because of concerns over the potential backlash within the financial community.[59]

After deciding to approach SWIFT directly, lawyers from the Departments of Justice and the Treasury were concerned with possible legal obstacles from the 1978 Right to Financial Privacy Act, which placed a number of restrictions upon government access to American's banking records. Of particular concern was whether the law prohibited access to records without a warrant or subpoena that was based on the same level of suspicion for each individual target. Law enforcement officials had previously been required to obtain grand-jury subpoenas or court-approved warrants for access to financial data, but after 9/11, the PATRIOT Act had authorized the use of broad administrative subpoenas — more commonly known as 'National Security Letters' — to access such records. Treasury Department lawyers ultimately concluded that the privacy laws applied only to banks and not to a banking cooperative like SWIFT, and that individual customers were protected but not the institutions that route funds through SWIFT on behalf of their customers.[60] In relying on broad administrative subpoenas to access the SWIFT database, the Treasury was not required to seek prior judicial authorization, and was only obliged to meet a 'reasonableness' standard as opposed to the 'probable cause' standard typically required for criminal subpoenas. *The United States v. Powell* sets forth a four-part test used to determine whether an administrative subpoena satisfies the 'reasonableness' standard, the most important element of which

[57] SWIFT has maintained that their participation was never voluntary, and that they only provided data in response to a valid subpoena. See Lichtblau & Risen 2006, *supra* note 7.
[58] *Ibid*.
[59] See Santolli 2008, *supra* note 9, p. 561.
[60] Lichtblau & Risen 2006, *supra* note 7.

being the purpose of the investigation.[61] The legal justification for the TFTP and the purpose of the investigation, according to the Treasury, is Executive Order 13,224's determination that "a need exists for further consultation and cooperation, and sharing of information by, the United States and foreign financial institutions […] to enable the United States to combat and finance terrorism."[62]

The Treasury's Office of Foreign Assets Control (OFAC) issued the first administrative subpoena to SWIFT in October 2001, and subsequently issued at least sixty-three more over the next seven years. These subpoenas sought access to information that SWIFT stored in its operating centre in the United States, and because the information had already been legally transferred to within the Treasury's jurisdiction, the administration was attempting to ensure that US law would govern the TFTP rather than the arguably more stringent European Union Data Privacy Directive.[63] The initial subpoenas sought any information SWIFT contained that investigators thought relevant to the financing of terror, paying particular attention to transfers to or from Saudi Arabia and the United Arab Emirates. According to one source close to the operation:

> At first they got everything — the entire SWIFT database. […] The Volume of data, particularly at the outset, was often overwhelming. We were turning on every spigot we could find and seeing what water would come out." The initial subpoenas, however, failed to identify specific individuals or transactions investigators thought were suspicious, and there seem to have been few formal limits on the searches. According to officials, "Sometimes there were hits, but a lot of times there weren't.[64]

Once officials realized the potential for abuse, they narrowed the search guidelines and added a number of safeguards. The US consulting firm Booz Allen Hamilton was hired to independently audit and oversee the operation of the program, electronic records were kept of every search conducted, and analysts were required to document the intelligence that justified each search. Despite these increased safeguards, SWIFT executives were becoming increasingly worried about their secret involvement, and began discussing pulling out of the program due to concerns about the legal, financial, and political risks involved. These concerns led to a meeting in 2003 with administration officials, SWIFT executives, then-Federal Reserve Chairman Alan Greenspan, and then-FBI director Robert Mueller, where the government eventually agreed to impose tighter controls. Among the new controls, SWIFT

---

[61] United States Court of Appeals 8 June 2011-13 July 2011, United States v. Powell, 379 U.S. 48, 57-58 (1964).
[62] Santolli 2008, *supra* note 9, p. 562.
[63] *Ibid*.
[64] Lichtblau & Risen 2006, *supra* note 7.

representatives would now be placed alongside intelligence officials, and could monitor and block any searches they considered inappropriate.[65]

VI. The American Reaction to the Revelation of the TFTP

When multiple news organizations revealed the existence of the classified TFTP in June 2006, the European outrage was significantly greater than the limited criticism the program received within the United States. As was mentioned previously, six days after the revelation of the TFTP, the US House of Representatives passed H.Res. 895, voicing their support for the program as lawful, and condemning the unauthorized disclosure of a classified initiative. Shortly after, however, H.Res. 904 was introduced, which commended the American press for its service in keeping the public informed. Neither resolution questioned the legality of the program. When the House Financial Services Committee's Oversight and Investigations Subcommittee held a hearing on 11 July 2006, the only points of debate were whether Members of Congress or newspapers had the right to publicly disclose classified information, and whether the Congress had been adequately informed and invited to collaborate. According to Representative Spencer Bachus: "The legal foundation of this program is well established. […] The New York Times, two weeks after 9/11, in an editorial, urged the administration to start such a program as this. And […] no one has disputed that this is a very successful program."[66]

In his remarks before the subcommittee, Stuart Levey, the Treasury's Under Secretary for Terrorism and Financial Intelligence, defended the success of the program, its legality, and the extensive safeguards in place to protect privacy.

> The program is consistent with privacy laws as well as Treasury's longstanding commitment to protect sensitive financial data. The SWIFT subpoena that we issue is powerful but narrow. We cannot simply browse through the records that SWIFT turns over. We are only able to see that information that is responsive to targeted searches in the context of a specific terrorism investigation. The data cannot be searched unless the analyst first articulates and enters into a computer the justification that links that target of the search to a terrorism investigation.

Under Secretary Levey specifically emphasized that the Treasury could not conduct searches for evidence of non-terrorist related crimes like tax evasion, economic espionage, or money laundering. He then outlined the extensive

---

[65] *Ibid*.

[66] Remarks of Representative Spencer Bachus, 'The Terror Finance Tracking Program', *Hearing Before the Subcommittee on Oversight and Investigations of the Committee on Financial Services*, U.S. House of Representatives, One Hundred Ninth Congress, Second Session, 11 July 2006, p. 12.

overlapping layers of government and independent controls in place to ensure that the data is handled properly.

> SWIFT representatives are able to monitor our searches in real time and stop any of them if they have serious concerns about the links to terrorists. In addition, a record is kept of every search that is done and those records are reviewed by SWIFT's representatives and by an independent outside auditor.[67]

Among its many successes, the TFTP is said to have played an important role in the investigation and capture of Riduan Isamuddin, better known as Hambali — the Jemaah Islamiyya's operational chief and the mastermind of the 2002 Bali bombings. The data also helped to identify a Brooklyn man, Uzair Paracha, convicted in 2005 of helping an Al-Qaeda operative in Pakistan launder $200,000 through a bank in Karachi.[68] Among its other successes, Mark Hoban of the UK House of Commons European Committee has said that since its inception, the TFTP has shared more than 1,550 valuable leads with EU member states, and has been instrumental in the investigation and prevention of some of the most serious terrorist attacks and attempted attacks of the past decade.[69] The TFTP is said to have helped investigators with the 2004 Madrid train bombings, the 2005 London transport bombings, and the 2008 Mumbai attacks. In a report initiated by the European Commission on behalf of the EU, French investigative judge Jean-Louis Bruguière claimed that the TFTP was a "vital counterterrorism tool" that was largely responsible for thwarting the 2006 UK plot to bring down transatlantic airliners, the 2007 'Sauerland cell' plot to bomb US military installations in Germany, and the 2007 plot to blow up JFK airport in New York.[70]

Despite these successes, and assertions that the TFTP is "grounded in law and bounded by safeguards,"[71] the extensive controls of the program were still considered "insufficient" to protect individual privacy by many European Union legislators. James Risen has suggested that the intense negative reaction to the TFTP in Europe was likely the product of resentment towards many of the Bush administration's policies in the larger war on terror. By the time of the program's disclosure, according to Risen, many in Europe were already angry over reports that the CIA had operated secret prisons in Eastern Europe, and had been kidnapping terrorism suspects through the "extraordinary rendition" program and transporting them to countries that used torture.[72] According to

---

[67] Remarks of Under Secretary Stuart Levey 2006, *supra* note 66, p. 14.
[68] Lichtblau & Risen 2006, *supra* note 7.
[69] Remarks of the Financial Secretary to the Treasury, Mark Hoban, to the UK House of Commons European Committee: Terrorist Finance Tracking Programme, 8 February 2011.
[70] J. Rosenthal, 'Germany's War on the War on Terror. Terrorist financers: good. Tax evaders: bad' *The Weekly Standard* 2010-15(27).
[71] Levey 2006, *supra* note 66, at 15.
[72] J. Risen, 'US Reaches Tentative Deal with Europeans on Bank Data', *New York Times*, 29 June 2007.

Santolli, however, this explanation only partially accounts for the negative reaction towards the TFTP, because it fails to acknowledge that under the European Union's Data Privacy Directive, "failing to protect an individual's data privacy rights […] is seen as a failure to respect the fundamental rights of citizens."[73]

VII. The TFTP and the European Union's Data Privacy Directive

Under article 8 of the European Convention on Human Rights, the "right to respect for [an individual's] private and family life, his home, and his correspondence" is considered a fundamental human right.[74] In 1995, the European Union enacted a comprehensive legislative scheme in the Data Privacy Directive that specifically embraces this view of privacy. The motivation for viewing data privacy as a fundamental right is said to have originated from memories of Nazi Germany and other totalitarian regimes where identifying information was frequently used to persecute disfavoured groups. Legislation was thought to be necessary because it was believed that the free market failed to provide an adequate level of privacy protection, but some have argued that the real reason behind the Data Privacy Directive was a European desire to minimize the competitive advantage US businesses had in processing personal data.[75] The Directive is also said to promote two sometimes conflicting objectives: "protecting an individual's right to privacy in their private data," and "promoting the free flow of information amongst *member states* of the European Union."[76] The view of data privacy as a fundamental right has led the EU to attempt to impose its view on other countries, but the Directive does not apply to transfers within the European Union for the purposes of public safety or state security. Under article 25(2), the European Commission has the authority to prohibit the transfer of data to non-EU countries who fail to provide "an adequate level of protection" for personal data.[77] According to an opinion issued by the Article 29 Data Protection Working Party after the disclosure of the TFTP, the United States' approach to protecting data privacy failed to provide this "adequate level of protection."

Article 29 of the Data Privacy Directive established a Working Party to monitor the effectiveness of the Directive in accomplishing its goals of protecting the rights of individuals with regard to their personal data. Although the findings of the Working Party are only advisory in nature, they are nevertheless accorded substantial deference in determining the position of the European Union.[78] The Working Party arrived at three distinct conclusions after evaluating the TFTP.

---

[73] Santolli 2008, *supra* note. 9, p. 565.

[74] European Convention on Human Rights, Article 8, at: http://www.hri.org/docs/ECHR50.html (July 2011).

[75] Santolli 2008, *supra* note. 9, p. 565.

[76] *Idem*, p. 566. Emphasis added.

[77] Data Privacy Directive, Article 25(2), *supra* note 12. Santolli 2008, *supra* note 9, p. 567.

[78] Data Privacy Directive, Article 29; Article 30(1)(c), *supra* note 12.

They concluded that the TFTP was invalid under the Data Privacy Directive; that SWIFT's decision to maintain a storage centre in the United States violated the Directive; and that any financial institution utilizing SWIFT's services after the disclosure of the TFTP was also in violation of the Directive.[79] The European Data Protection supervisor then informed the European Central Bank that it had until April of the following year to bring SWIFT into compliance.[80]

According to Article 26 of the Directive, data can only be transferred to a non-EU country without providing for the adequate protection for private information if the transfer satisfies one of six 'Safe Harbour' provisions.[81] The only one of the six provisions that could have possibly legitimated the TFTP was if the transfer was "necessary or legally required on important public interest grounds," but this provision has been previously interpreted to indicate that a "simple public interest" is insufficient. Based on a 2006 German Constitutional Court decision — which demonstrated some apprehension as to whether the "possibility of future terrorist attacks [was] sufficient to justify antiterrorism datamining" — the Article 29 Working Party determined that SWIFT's transfer of data to the US failed to serve a "crucial public interest."[82] Even though the TFTP had proved instrumental in thwarting and helping to investigate a number of terrorist attacks, the Working Party thought it was "a luxury given the existing international mechanisms to combat terrorist financing."[83] The Working Party then turned their attention to SWIFT's interest in maintaining dual information storage centres to guarantee operational efficiency, and eventually determined that such an interest could just as well be served by storing the information in a country with data privacy standards approved by the European Union.[84]

SWIFT has argued that because they had an operations centre within US jurisdiction, their participation in the TFTP was necessary to fulfil their legal obligation to comply with the Treasury Department's compulsory subpoenas. Had they failed to cooperate with the program, their assets would have been subject to forfeiture under Executive Order 13,224 and Title III of the PATRIOT Act. In their evaluation of the whistle-blowing schemes mandated by the Sarbanes-Oxley Act of 2002, however, the Article 29 Working Party concluded that "an obligation imposed by a foreign legal statute of regulation […] may not qualify as a legal obligation by virtue of which data processing in the EU would be made legitimate."[85] As the European Parliament suggested, in other words,

---

[79] Opinion of the Article 29 Data Protection Working Party, *supra* note 12, p. 12-13.
[80] Santolli 2008, *supra* note 9, p. 568.
[81] Data Privacy Directive, Article 26(1), *supra* note 12.
[82] Opinion of the Article 29 Data Protection Working Party, *supra* note 12, pp. 24-25. Cited in Santolli 2008, *supra* note 9, p. 569.
[83] *Ibid*.
[84] *Ibid*.
[85] Sarbanes-Oxley Act of 2002, 15 U.S.C. §§78(j)-(l), 301(m)(4) 2002; Article 29 Working Party, Opinion 1/2006 on the Application of EU Data Protection Rules to Internal Whistleblowing Schemes in the Fields of Accounting, Internal Accounting Controls,

SWIFT should have foreseen that operating a storage centre in the US would lead to this sort of conflict, and therefore their obligation to respond to Treasury's compulsory subpoenas or have their assets frozen was "insufficient to satisfy the requirements of the Data Privacy Directive."[86]

SWIFT maintains that contrary to the "unfounded assertions in the press and in some data privacy opinions," the transfer of data to the Treasury under subpoena was "legal, limited, targeted, protected, audited, and overseen."[87] The advisory opinions of the Belgian Data Privacy Commission and the Article 29 Working party assert that SWIFT's participation in the TFTP violated the provisions of the Data Privacy Directive and failed to serve a crucial public interest. SWIFT and US authorities objected to both opinions, claiming they reflected serious interpretation issues concerning data privacy laws, and then went on to reiterate the substantial internal and external auditing measures in place to guarantee the legal use of the transferred information. SWIFT highlights that on 22 October 2006, Bryon Calame, the public editor of the New York Times, published an admission that his previous defence of the Times' original story on SWIFT compliance was a mistake. It is important to note that a number of data privacy organizations had quoted Lichtblau and Risen's original 23 June 2006 article as a basis for their concerns. Calame's October 'Mea Culpa' reversed his earlier position, and now asserted that because the TFTP was legal and there was "not one shred of evidence that anyone's private data had been abused, the program should have remained secret."[88]

SWIFT also notes that after examining the Belgian Data Privacy Commission's advisory report and SWIFT's comprehensive legal rebuttal, on 13 December 2006, the Belgian public prosecutor officially announced that he would not be taking legal action. That same month, European Commission Vice President Franco Frattini announced that the EU and the US would commence negotiations to establish a legal framework for providing financial intelligence to counterterrorism officials with an adequate level of data protection.[89] Just two months later, after European privacy watchdogs had repeatedly called the TFTP illegal but realized they were impotent to stop it, the European Parliament passed a resolution recommending that "the only logical way to stop US anti-

---

Auditing Matters, Fight Against Bribery, Banking, and Financial Crime (1 February 2006), p. 8. Santolli 2008, *supra* note 9, p. 571.

[86] Opinion of the Article 29 Data Protection Working Party, *supra* note. 12, pp. 18-19. Cited in Santolli 2008, *supra* note 9, pp. 571-572.

[87] SWIFT, 'US Terrorist Financing Investigations and the Role of SWIFT: A Summary of Developments to Date on SWIFT Compliance', SWIFT press release, 11 February 2007, at:
http://www.swift.com/about_swift/legal/compliance/statements_on_compliance/us_terrorist_financing_investigations_and_the_role_of_swift/index.page (July 2011).

[88] SWIFT, 'New York Times Public Editor Reverses Himself on 23 June Article', SWIFT Press Release, 24 October 2006, at:
http://www.swift.com/about_swift/legal/compliance/statements_on_compliance/new_york_times_public_editor_reverses_himself_on_23_june_article.page? (July 2011).

[89] SWIFT 2007, *supra* note 87.

terrorist investigators from illegally snooping on European financial transactions is to get the firm handling them (SWIFT) to remove its data from US shores."[90]

After months of public discord, in June 2007 the US Treasury transmitted to the Council Presidency of the EU and the European Commission a set of descriptions detailing the additional safeguards that would thereafter govern subpoenaed data under the TFTP, and which subsequently led to a tentative agreement between the parties. Under the new agreement, the US pledged to respect EU privacy rules, reaffirmed their commitment to only use the program for counterterrorism purposes, and agreed not to retain collected data for more than five years. The European Union announced their intention to compel financial institutions that use the SWIFT network to inform their customers that the US has the ability to access their personal data under subpoena, and to appoint an "eminent European person" to assess whether the Treasury is implementing the TFTP in accordance with its representations. Vice President Frattini then confirmed that these new guarantees were adequate to take account of EU privacy standards, verifying the "legality and value" of the SWIFT program in the eyes of the US Treasury.[91]

After an extensive review of the TFTP initiated in early 2007, on 10 December 2008, the Belgian Data Protection Commission concluded that the SWIFT program complied with all applicable Belgian legislation. The Commission agreed that SWIFT was obliged to comply with the lawful subpoenas they received, and added that while fulfilling their obligations, SWIFT "acted with prudence, diligence, and due care to protect personal data." The Commission therefore reconsidered the severity of their earlier opinions, and concluded that there was no reason to challenge SWIFT's good faith. The Commission cited a number of measures SWIFT had undertaken to ensure the adequate protection of personal data, including joining a transatlantic framework ensuring that European data transferred to the US would be protected under similar standards as in Europe, and a proposed change to SWIFT's messaging architecture to allow for all intra-European messages to be processed and stored only in European facilities.[92]

---

[90] M. Ballard, 'Pull European Data from the US: Europe's Solution to the SWIFT Problem', *The Register*, 15 February 2007, at: http://www.theregister.co.uk/2007/02/15/us_retreat/ (July 2011); European Parliament, 'European Parliament Resolution on SWIFT, the PNR Agreement and the Transatlantic Dialogue on These Issues', 2007/2503/RSP, 7 February 2007, at: http://www.europarl.europa.eu/sides/getDoc.do?language=EN&reference=B6-2007-0042&type=MOTION (July 2011).

[91] Risen 2007, *supra* note 72; SWIFT, 'Subpoenaed SWIFT Message Data is Adequately Protected', SWIFT Press Release, 18 February 2009, at: http://www.swift.com/about_swift/press_room/press_releases/press_releases_archive/subpoenaed_swiftmessagedata_adequatelyprotected.page (July 2011).

[92] SWIFT, 'SWIFT Protects Data Protection Legislation', SWIFT Press Release, 10 December 2008, at:

In February 2009, after a year-long review conducted by French investigative judge Jean-Louis Bruguière, the European Commission confirmed that the US Treasury had "from the outset" been vigilant in respecting appropriate "safeguards in the handling of personal data obtained from SWIFT under subpoena." The report of judge Bruguière, also issued to the European Parliament's Civil Liberties Committee, further found that the TFTP was targeted, narrowly focused, used exclusively for counterterrorism purposes, and had "generated significant value in the fight against terrorism, notably in Europe."[93]

The need for a new access agreement emerged following the announcement that SWIFT planned to shut down its American servers and store all relevant data in Europe, and in July 2009 the European Commission declared their intention to negotiate with the United States. A new storage centre was to be opened in Switzerland starting 1 January 2010, which would maintain redundancy without having to store European data in the United States. Since SWIFT would no longer store any data on US soil, they were outside the jurisdiction of the Treasury's subpoena, and without a new access agreement the TFTP would effectively grind to a halt. To prevent a disruption in the flow of data, the European Commission attempted to approve a temporary agreement negotiated with the Obama administration in November 2009. It has been suggested that the Commission attempted to force the approval of this interim agreement one day before the European Union's new Lisbon Treaty was to come into force — which would have circumvented the new requirement of Parliamentary consent.[94] Others have argued that it was hardly the Commission's aim to deny the Parliament their right to co-consideration in the matter, as the deal only concerned an interim agreement, and was only intended to keep the TFTP functioning while a permanent agreement was negotiated and submitted for Parliamentary approval.[95] Either way, after an outcry the commission backed down and postponed the approval of the temporary arrangement.

On 11 February 2010, following a British court's release of previously secret and politically damaging information on the treatment of a former Guantanamo Bay detainee by US interrogators, the European Parliament forced the rejection of the agreement that would have formalized the SWIFT data flow.[96] In making use of their new powers under the Lisbon Treaty, the Parliament's vote

---

http://www.swift.com/about_swift/press_room/swift_news_archive/home_page_stories_archive_2008/swift_respects_data_protection_legislation.page> (July 2010).

[93] SWIFT 2009, *supra* note 91.

[94] N. Kralev, 'European Vote on Counterterror Blocks Bank-Data Sharing with US', *The Washington Times*, 12 February 2010, at: http://www.washingtontimes.com/news/2010/feb/12/european-vote-blocks-bank-data-sharing-with-us/ (June 2011).

[95] Rosenthal 2010, *supra* note 70.

[96] Kralev 2010, *supra* note 94.

effectively shut down the TFTP, and was hailed in the media and halls of Parliament as a triumph of 'European democracy.' The fact that the vote was anonymously held, however, with no record of the votes of individual Members of the European Parliament (MEPs) being made public, has led some to question the level of European democracy in this regard.[97]

VIII. Understanding the European Reaction

The European Parliament eventually approved a revised version of the SWIFT agreement on 8 July 2010. It is important to note here that it is not my intention to reduce 'European governance' in general to the counterterrorism practices of individual European states. Exploring the variation in their policies, however, exposes transatlantic as well as intra-European tensions concerning the perception of terrorism risk and the prioritization of values to be protected by these policies.

Although the Parliament's vote on 11 February was anonymous, the overtly political run-up left little doubt about the central role played by the German MEPs in killing the agreement. "This agreement breathes the spirit of the security ideology of the United States of America," said Martin Schulz, the German leader of the Parliament's Progressive Alliance of Socialists and Democrats, "but it does not breathe the spirit of the protection of the fundamental rights that we as European deputies must guarantee for the citizens of this continent."[98] The European Commission merely mentioning their intention in July 2009 to negotiate with the US over the TFTP "sparked frenzied reactions across the German political spectrum." Horst Seehofer, the Chairman of the Christian Social Union, spoke of a "scandal," and described the plan to negotiate as "absolutely preposterous."[99] Although the German government did eventually consent to negotiations on the agreement in July 2009, when said agreement was completed four months later, they abstained. This abstention is significant because as the Council decision required unanimity, a German 'no' would have effectively killed the agreement. It has therefore been suggested that "rather than bearing the onus of having torpedoed a crucial transatlantic security agreement, the German government by its abstention simply handed off the issue [to the] European Parliament."[100]

Commentators like Rosenthal have argued that the German opposition to the TFTP is usually "couched in terms of privacy concerns and data protection," although they hardly ever specify the damage that unsuspecting Europeans might suffer from the European Union's cooperation with the TFTP. It is worth reiterating that counterterrorism officials are only able to conduct targeted searches on the transactions of individuals already suspected of financing terrorism and currently under investigation. As then-Treasury Secretary John

[97] Rosenthal 2010, *supra* note 70.
[98] *Ibid*.
[99] *Ibid*.
[100] *Ibid*.

Snow insisted: "The TFTP is *not* a fishing expedition, but rather a sharp harpoon aimed at the heart of terrorist activity."[101] When the Treasury receives financial data from SWIFT, it is placed into a 'black box' that prevents investigators from seeing any information that is not responsive to direct search criteria. A special software program allows investigators to search the SWIFT data for the transactions of suspected terrorists, and SWIFT is able to immediately suspend or prevent any inquiries they consider of dubious validity.[102] Despite these extensive controls which were expressly communicated to the European Commission and Parliament — and confirmed by the European Commission's own investigation — the general tone of the German opposition was captured in 2009 by the Berliner Zeitung, which sarcastically titled a report on the SWIFT negotiations: "So Much for Bank Secrecy."[103]

The irony of this position, according to commentators like Rosenthal, is that for many years the German government has been conducting a "veritable crusade" against the confidentiality of bank data within the European Union in the name of combating tax evasion. In 2009, German Chancellor Angela Merkel endorsed the purchase of stolen Swiss bank data by tax authorities, and the decision was announced only one week before the European Parliament voted down the SWIFT agreement largely due to the disapproval of the German Christian Democratic Union and Christian Social Union parties. The data thief was paid the equivalent of $3.4 million, after which the German finance minister Wolfgang Schäuble declared to the Swiss press his intention to "eliminate bank secrecy in Europe."[104] Only two years before, the German Foreign Intelligence Service purchased stolen data from the Liechtenstein-based LGT bank, which led to a televised raid on the home of well-known businessman and now infamous tax evader Klaus Zumwinkel. For this stolen information, the thief was paid the equivalent of $5.5 million, and subsequently furnished with a new identity. These apparent contradictions have led some in the American press to believe, like Rosenthal, that:

> …in the eyes of both of Germany's leading political parties, it is good and righteous for Germany to violate a bank client's expectation of privacy in the name of combating tax evasion and topping up the coffers of the German treasury, but it is bad and evil for the United States to do the same in the name of combating terrorism and saving lives.[105]

The European Parliament eventually approved a revised version of the SWIFT agreement on 8 July 2010, and President Obama subsequently announced that the TFTP — which had been suspended since January — would fully resume on the first of August. It appears that President Obama spoke too soon, however,

---

[101] Santolli 2008, *supra* note 9, p. 579. Emphasis added.
[102] *Ibid.*, p. 564.
[103] Rosenthal 2010, *supra* note 70.
[104] *Ibid*.
[105] *Ibid*.

as the new agreement called for the appointment of an 'eminent European person' to oversee the program, and such an appointment was not made until 27 August. This new agreement represents a dramatic shift in the operation of the original TFTP, where data was stored in the US and searches were overseen by SWIFT representatives and independent auditors. The identity of this anonymous European 'person' is of tremendous significance to the functioning of the program, as this observer can review and query searches, demand additional justification, block any and all searches they deem unfit, and because there is no mechanism in place to appeal their decisions. Although the European Parliament claims the observer will act "independently," it will be a European Commission official, and the appointment will therefore undoubtedly be subject to the same lobbying and "horse-trading" that is "part and parcel of the Commission's appointment process."[106]

Despite some assertions to this effect in the American press, it would not be accurate to imply that Europeans in general are 'soft' on terrorism, or have failed to take steps they consider appropriate to stem the flow of terrorist financing. The European Security Strategy of 2003 largely echoes its American counterpart, and articulates a security environment besieged by "radical new threats that render the traditional concept of self-defence obsolete."[107] Central to the European strategy is the 2002 'Framework Decision on Combating Terrorism,' which provides a uniform framework for counterterrorism within the European Union. The Framework Decision adopts a broad definition of what constitutes terrorism, sets forth a number of measures designed to prevent or pre-empt attacks during the early planning stages, and criminalizes a new series of 'terrorism related' activities. The European Council in 2005 issued the 'Strategy for Combating Radicalization and Recruitment to Terrorism,' which compels teachers, community workers, prison staff, etc. to intervene in the lives of those thought vulnerable to radicalization.[108] In 1995 the European Union created the Egmont Group to combat terrorist financing through the establishment of national 'financial intelligence units.' On 21 September 2001, the European Council approved over thirty measures specifically to respond to terrorist financing and money laundering. These measures included the mandatory creation of a 'financial intelligence unit' in each member state; increasing the priority of responding to terrorist financing among law enforcement; a common definition of terrorism; and the establishment of a European-wide arrest warrant.[109] In December of that year, the European Parliament and Council amended Directive 91/308/EEC on the prevention of the use of the financial system for money laundering to include a 'gatekeeper'

---

[106] J. Rosenthal, 'Terrorist Finance Tracking Program Re-Starts under Anonymous European Oversight', *The Weekly Standard,* 20 September 2010.

[107] M. de Goede, 'The Politics of Preemption and the War on Terror in Europe', *European Journal of International Relations* 2008-14, p. 168.

[108] *Idem*, pp. 169-170.

[109] Conclusions and Plan of Action of the Extraordinary European Council Meeting, 2001, O.J. (SN 140/01) (21 September 2001). Cited in Donohue 2006, *supra* note. 18, p. 387.

provision requiring lawyers, accountants, and notaries to report suspicious financial activities to national authorities.[110]

After 9/11, the EU also immediately began to block the assets of specific individuals and organizations associated with terrorism, including 170 Taliban officials, Afghan Airlines, and a number of Afghani financial institutions. In May 2002, the EU issued a list of eighteen specially designated terrorists and terrorist groups subject to asset forfeiture, but unlike the American freezing lists, the EU required checks prior to listing, an appeals process, and included sanctions against states that improperly or wrongly listed individuals. The European lists also made an exception in the freezing of funds for everyday living expenses and legal costs, a direct contrast to the American procedure that strictly forbids funds to be used even to relieve humanitarian suffering.

In March 2006, as a reaction to the London bombings the previous year, the European Parliament approved the 'Data Retention Directive' requiring all member states to retain telecommunications data including that from mobile telephones, email, internet and search engine traffic for a period of between six to twenty-four months for access by law enforcement officials.[111] In March 2009, Germany's constitutional court overturned a German law that sought to implement the minimum six-month data retention requirement under the Directive. In a further act of defiance to the authority of the EU, the court ruled that the data should be deleted, and even ordered some of the data to be deleted "immediately."[112] The German court overturned the law arguing that its mere existence creates a "diffuse threatening feeling of being *observed*" — an interesting and somewhat contradictory conclusion in light of studies conducted by Germany's Max Planck Institute, suggesting that frequently, German citizens really are being observed. In 2007, the police in Berlin alone monitored more than one thousand residents and nearly one million phone calls to look for ties to terrorism. Wiretaps were used by law enforcement officials some thirty times more frequently in Germany than in the US, and only .33 percent of those wiretaps were associated with subsequent prosecutions and convictions — one-fifth of the corresponding American figure.[113]

It is also interesting to note that after the political controversy surrounding the authorization of a financial data access agreement between the US and the EU, the European Parliament for the most part seems to have lost interest in their 'advice and consent' powers with regard to the selection of the European

[110] Donohue 2006, *supra* note 18, p. 387.
[111] Directive 2006/24/EC of the European Parliament and of the Council on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications or Services or of Public Communications Networks and Amending Directive 2002/58/EC, at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:NOT (July 2011).
[112] Rosenthal 2010, *supra* note 70.
[113] *Ibid*.

'overseer' of the TFTP.[114] This is perhaps because many in the European Parliament view the current access agreement as a temporary arrangement because the European Commission was scheduled to bring forward a legal and technical framework for a specifically European Terrorist Finance Tracking Program by 1 August 2011. While some Members of the European Parliament claim such a program is intended to "put an end to the data transfer to the United States," others insist that "an in-house EU system [does] not mean that transatlantic cooperation should in any way be diminished," but would in fact be "enhanced by having an extra pair of eyes analyzing data."[115] Not surprisingly, however, when the European Commission presented a communication on different options for an EU TFTP rather than a specific legal and technical framework, the German rapporteur on the TFTP from the Free Democratic Party was quick to criticize the shortcoming:

> After difficult negotiations, the European Parliament had approved the so-called SWIFT agreement last year *only* because of the commitment from the Commission to submit its own proposal for a EU TFTP to Parliament and Council within a year. We have repeatedly highlighted the fact, that we are expecting a legal proposal and *not* just a compilation of options. Our principle and principled objections to the SWIFT agreement consequently still stand. From a Liberal group perspective we would favour the option that represents the least invasion of personal privacy. We do *not* want a copy of the US intelligence system, but rather a slim, efficient, and targeted extraction system with clear access rights and the quickest possible termination of the current transfer of bulk data to the US[116]

Conclusion

Despite assertions to the contrary, claims that the Europeans are 'soft' on terrorism — or that the Americans are reckless 'cowboys' with little regard for privacy or the rule of law — can clearly be seen to oversimplify an extraordinarily complex and complicated set of issues. It is simply not the case that European governments are unconcerned with terrorist financing because

---

[114] *Ibid*.

[115] M. Weber, 'EU System on Terrorist Finance Tracking Can End Data Transfer to the US', *EPP Group Press Release*, 13 July 2011, at: http://www.eppgroup.eu/press/showpr.asp?prcontroldoctypeid=1&prcontrolid=10521&prcontentid=17756&prcontentlg=en (July 2011); T. Kirkhope, 'EU to Create its Own Terror Finance Tracking System', *ECR Press Release*, 13 July 2011, at: http://www.ecrgroup.eu/eu-to-create-its-own-terror-finance-tracking-system-news-374.html (July 2011).

[116] A. Alvaro, 'Commission "Options" for EU Terrorist Finance Tracking Fall Short of Promised Legislation', *Alliance of Liberals and Democrats for Europe Press Release*, 13 July 2011, at: http://www.alde.eu/press/press-and-release-news/press-release/article/commission-options-for-eu-terrorist-finance-tracking-fall-short-of-promised-legislation-37552/ (July 2011). Emphasis added.

they have been reluctant to support the American Terrorist Finance Tracking Program. The United States and the European Union have developed entirely different perceptions of the threat of terrorist financing, a different prioritization of the values they believe should be protected, and a radically different regulatory, legislative, and military capacity to respond to terrorist threats. It should not be surprising that many Europeans were uneasy with the public disclosure of a classified program that granted a foreign intelligence service access to their financial records. It should also not be surprising that many Americans were frustrated by what they perceived as an unwillingness to accept good faith assurances that such access would not violate privacy laws, and that the records would be appropriately used strictly for counterterrorism purposes. It seems in this case that the perception of the threat and the prioritization of values to be protected were inextricably linked to differences in the way terrorism was experienced by the populations being governed.

As the financial data the Treasury sought from the SWIFT database was ultimately to be utilized for a purpose other than the purpose for which it was originally released by the bank customers, in the eyes of many Europeans it was simply "incongruous" with the limitations of the Data Privacy Directive.[117] Because continuing to attempt to appease unsubstantiated fears over the misuse of European bank data was a significantly lower priority than the prevention of another terrorist attack, the American response would likely be that the Data Privacy Directive is simply "incongruous" with efforts to pre-empt terrorism, and slightly out of touch with reality. The United States believed that they were providing for the adequate protection of personal information in the TFTP, and therefore could only view European reluctance as stubborn and uncooperative. Given the multiple overlapping layers of control in place to protect private data, there seems to be no reason why SWIFT should be prohibited from transferring the exact same data to the US Treasury Department that European Union member states can require each other to transfer between European law enforcement agencies under the 2006 Data Retention Directive. As Donohue has suggested, the conflict over the TFTP can thus be seen as the European Union viewing themselves as the "privacy cop of the world," while the United States remains unwilling to provide detailed evidence supporting their suspicions of terrorist activities due to a fear of compromising their intelligence sources and methods. In the eyes of many American politicians and commentators, European attempts to force the termination of the TFTP are largely political in nature, and embody a refusal to acknowledge that the threat of terrorism has made our world an integrated community.[118]

When the differences in the European and American approach are understood as a fundamental disagreement over the prioritization of privacy rights, however, it becomes possible to promote genuine understanding, and increase

[117] Article 29 Working Party Opinion 2006, *supra* note 12, pp. 14-16.
[118] Donohue 2006, *supra* note 18, p. 580.

transatlantic cooperation in what must be a unified struggle against global terrorism.
