A NEED FOR SWIFT CHANGE: THE STRUGGLE BETWEEN THE EUROPEAN UNION'S DESIRE FOR PRIVACY IN INTERNATIONAL FINANCIAL TRANSACTIONS AND THE UNITED STATES' NEED FOR SECURITY FROM TERRORISTS AS EVIDENCED BY THE SWIFT SCANDAL.

Courtney Shea*

Cite as: 8 J. HIGH TECH. L. 143 (2008)

In recent history, the struggle between the desire for privacy and the need for security has been affected by worldwide events. This struggle is clearly seen in the transfer of information from the European Union (EU) to the United States. In the last century, Europeans suffered from violent actions, from those such as the Third Reich, which was partly facilitated by privacy violations. Abuses like these have increased the EU's desire to enact strong data protection laws which protect the safety and identity of its citizens. With the invention of the Internet, there was a similar call for stricter privacy laws in the U.S. to protect individuals' information. However, this American trend came to an abrupt halt with the attacks of September 11, 2001. This tragic event changed American life, creating a new cry from U.S. citizens for stronger security measures. As a result, a conflict of ideals was created between the EU and U.S. where Europeans wish to protect information to avoid the follies of the past, while the American government is continually seeking information to learn of possible terrorist activities or plans of future attacks.

This struggle between privacy and security has affected the transfer of important data from the EU to the U.S. A strict European Union Data Protection Directive [hereinafter The Directive] has made it difficult for the U.S. to gather information in the post 9/11 era without violating EU law. In particular, the United States' secret collection of data from messaging services relating to international financial transactions has been found by the EU to violate the Directive. This tracking program was highlighted by the extensive use of the Belgium based bank messaging service, The Society for Worldwide Interbank Financial

* J.D. candidate 2008, Suffolk University Law School.

Telecommunication (SWIFT). Although the EU and the U.S. seem to have temporarily solved this conflict as it relates to SWIFT, a more permanent solution has yet to be negotiated. Thus, it is this author's argument that the U.S. must take immediate action to modify its Safe Harbor Provision with the EU, which provides a safe haven from some of the strict mandates of the Directive, and that the U.S. and EU should work together to create a uniform method of protecting data.

This note discusses: the development of U.S. and EU privacy law; the creation and development of the Directive; how recent actions of the U.S., namely the tracking of international financial data, violates the objectives of the Directive; and how this creates a need for action from the U.S. in order to continue the free flow of data from EU member nations to the U.S. Section I discusses the history of privacy law in the U.S. and in the EU, which led to the EU enactment of the Directive and the subsequent negotiation with the U.S. to create a Safe Harbor Provision. Section II illustrates the recent tracking of international financial transactions in collaboration with the Brussels based banking consortium, SWIFT, and how the EU has reacted. Section III analyzes this issue from both the perspective of the U.S. and the EU. This Section also discusses the solutions to the problem relating to SWIFT. Section IV is a summary of the issues discussed in the note and sets forth the author's perspective on how the overarching problem can be resolved while still respecting the United States' desire of security from terrorists and the EU desire for protection of its citizen's privacy.

I. The Development of Privacy Laws and Data Protection

A. Privacy of Personal Data in the United States

While the EU has historically enacted broad legislative protection of personal data, the U.S. has promoted the self-regulation of industries through the use of broad reaching legislation.[1] As a result of the 9/11 attacks on American soil, Americans have subsequently lived in fear of terrorism. Perhaps it is this desire for security that has made Americans more willing to forgo sweeping privacy laws as seen in the EU, and in turn, made them more willing to sacrifice the protection of their data.[2]

1. Megan Roos, *Safe on the Ground, Exposed in the Sky: The Battle Between the United States and the European Union Over Passenger Name Information*, 14 TRANSNAT'L L. & CONTEMP. PROBS. 1137, 1154-55, 1161 (2005); John B. Reynolds, III, *View from Washington, European Union (EU) Privacy Directive Enters Into Force*, archived at http://www.webcitation.org/5WBIN8Xwm.

2. *See* Roos, *supra* note 1, at 1161. Recent U.S. events, including security breaches have "resulted in suffering and fear," making Americans more willing to

Although the U.S. has taken this sectoral approach to data protection laws, the United States Constitution and interpreting case law does provide some protection of an individual's privacy.[3] Cases like *Whalen v. Roe*[4] and *Nixon v. Administrator of General Services*[5] have extended the protection of an individual's privacy, however, this is a general protection and courts have not yet interpreted the Constitution broadly enough to include a protection of information privacy from government misuse.[6] Despite this lack of overarching protection, there are some statutes that limit the use of data, using the aforementioned sectoral approach.[7] Examples of sectoral regulations enacted include: the Fair Credit Reporting Act of 1970,[8] The Privacy Act of 1974,[9], and the Drivers Privacy Protection Act of 1994.[10]

B. Privacy Protection in the European Union

Throughout the past two centuries Europeans have suffered from abuses of invasive data collection, making the issues of privacy and the protection of personal data ongoing concerns.[11] As a result the EU has taken an aggressive position when dealing with the adequate protection of data.[12] While prior to the 1980's there was no international directive

relinquish privacy protections than Europeans. *Id.*

3. *See* Roos, *supra* note 1, at 1154-55. S*ee also* Arnulf S. Gubitz, *The U.S. Aviation and Transportation Security Act of 2001 in Conflict With the E.U. Data Protection Laws: How Much Access to Airline Passenger Data Does the United States Need to Combat Terrorism?*, 39 NEW ENG. L. REV. 431, 446-47 (2005) (noting that the Constitution protects an individual's freedom from government intrusions).

4. 429 U.S. 589 (1997).

5. 433 U.S. 425 (1977).

6. *Whalen, supra* note 6, at 598-600 (extending the privacy zone to independence in important decision making of the individual and the ability to deny the disclosure of personal matters); *Nixon, supra* note 5, at 457-59 (affirming the right to information privacy which was set forth in *Whalen*); *see* Gubitz, *supra* note 3, at 446-47*:* Roos, *supra* note 1, at 1155.

7. Roos, *supra* note 1, at 1155. The U.S. has used a sectoral law creating a "fragmented and inconsistent" approach to data protection across economic segments. Gubitz, *supra* note 3, at 447-48.

8. 15 U.S.C. § 1681 (2000).

9. 5 U.S.C. §§ 2721-2725 (2000).

10. 18 U.S.C. §§ 2721-2725 (2000); *see* Roos, *supra* note 1, at 1154-55.

11. *See* Steven Salbu, *The European Union Data Privacy Directive and International Relations*, 35 VAND. J. TRANSNAT'L L. 655, 666 (2002) (Europeans' concern with privacy partly a result of "Third Reich abuses in tracking its target groups with invasive data-collection methods").

12. *See id.* at 695 (finding that the EU has taken aggressive measures and instilled strong protection laws ensuring that once the information passes to nations outside the EU, it remains protected); *see also* Gubitz, *supra* note 3, at 436 (stating that while historically some EU nations had stringent data protection laws, others

governing data privacy in the EU, there were several instruments and measures created to protect the privacy of European citizens in a general way.[13]

The United Nations (U.N.) started the international movement for privacy protection in 1948 when the U.N. General Assembly implemented the Declaration on Human Rights (UDHR).[14] This was a non-binding document, which recognized privacy as a fundamental right in need of protection.[15] Over 100 nations reaffirmed their commitment to the principles of this international declaration at the 1993 U.N. World Conference on Human Rights.[16] In 1973, Sweden paved the way for other European nations and passed groundbreaking data protection legislation.[17] In the 1970's, the U.N. strengthened its policies with the United Nations International Covenant on Civil and Political Rights (ICCPR) which "gives all individuals the right to protection of the law against...arbitrary interference with their privacy, family home or correspondence".[18] Subsequently, in 1978, the Organization for Economic Co-operation and Development (OECD) developed guidelines governing the flow of data among its member countries.[19] When the European Union was formed in 1993, this new legislative body began work to create a uniform piece of legislation to set a standard for the protection of personal data for member nations.[20]

had relatively few).

13. *See* Roos, *supra* note 1, at 1146.

14. Universal Declaration of Human Rights, G.A. Res. 217A, at 71, U.N. GAOR, 3d Sess., 1st plen. Mtg., U.N. Doc A/810 (Dec. 12, 1948).

15. *Id.* Article 12 of the document states, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." *Id.* Gubitz, *supra* note 3, at 434 (stating that while legally non-binding, this document has still become a customary part of international law).

16. Roos, *supra* note 1, at 1146.

17. Datalag (1973:289), *translated in* Office of Telecommunications, U.S. Dep't of Commerce, OT Special Pub. 78-19, Selected Foreign National Data Protection Laws and Bills 70-77 (C. Wilk ed. 1978); *see also* Salbu, *supra* note 11, at 668.

18. *See* Roos, *supra* note 1, at 1147. (The ICCPR's purpose is to ensure "a broad spectrum of civil and political rights, rooted in basic democratic values and freedoms, to all individuals").

19. Organization for Economic Co-Operation and Development, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, *archived at* http://www.webcitation.org/5WBIUqgDY [hereinafter OECD Guidelines]. The OECD guidelines require that data should be relevant, accurate, current, and collected lawfully and fairly with full awareness and consent of the data subject of the collection. Gubitz, *supra* note 3, at 435.

20. Gubitz, *supra* note 3, at 435-36.

C. The Data Protection Directive

In response to the desire for privacy from its citizens and member countries, the Declaration of Human Rights, and the OECD guidelines, the newly formed European Union created the Data Protection Directive in 1995 in order to protect the freedom and fundamental rights of individuals, while ensuring the continued free movement of data and information.[21] The Directive came into effect on October 25, 1998 and required EU countries to create legislation implementing the provisions of the Directive and regulating how personal data could be used.[22] In addition to the requirement of enacting appropriate legislation in member countries, the European Parliament and European Council established the European Data Protection Supervisors (EDPS), which is an independent supervisory authority that regulates the processing of data.[23]

The Directive applies to situations where the data of an identifiable person is processed.[24] According to the Directive, individuals must be informed that their data will be processed, who will receive it, and the purpose of collection.[25] The data must be processed in a manner that is

21. Council Directive 95/46/EC, 1995 O.J. (L 281) 31, *archived at* http://www.webcitation.org/5WBIdlrjN [hereinafter Directive 95/46]; *see* Roos, *supra* note 1, at 1153; Salbu, *supra* note 11, at 656; Lori Liermann, American Bar Association, Business Law Today, *Go Global. Get Information. Now What? All About the EU Directive and the U.S. Safe Harbor* (Jan. / Feb. 2003), *archived at* http://www.webcitation.org/5WBIhrMJF; John Sandman, *SWIFT Data Dispute Simmers: Contacts with critical EU panel limited*, SEC. INDUS. NEWS (Dec. 2006).

22. *See* Reynolds, *supra* note 1; Liermann, *supra* note 21. The Directive is not a law in and of itself, rather it is a guideline for EU member nations to use when implementing their own legislation. Salbu, *supra* note 11, at 668.

23. The EDPS works to ensure that nations comply with the Directive and informs individuals of their data protection rights. Gubitz, *supra* note 3, at 441-42. The EDPS and Assistant EDPS are appointed to serve for five years to work independently from the European Commission. Each member state also has its own data protection supervisor. *Id.*

24. Electronic Privacy Information Center, EU-US Airline Passenger Data Disclosure, *archived at* http://www.webcitation.org/5WBIl5wiP [hereinafter EPIC Passenger Data]. According to the Directive, personal data is any data that, "can identify a natural person." *Id.* The term data processing, under the directive covers a vast number of ways in which someone's personal information and data may be used for a commercial process. Liermann, *supra* note 21. The term processing includes; "collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." Directive 95/46, *supra* note 21, art. 2(b); Salbu, *supra* note 11, at 669-670.

25. Where the data is not obtained directly from the data subject the hardship provision of the Directive may make disclosure inapplicable. An exception to disclosure also applies "where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such

specific, explicit and has a legitimate purpose.[26] Under the Directive, the transfer and processing of data that relates to "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life" is prohibited.[27] The data for which processing is allowable must be accurate, up to date and stored only for the time needed for the given purpose.[28] Data that is processed only for scientific research or for creating statistics falls outside of the Directive. In addition, EU nations can lower the level of protection of data to "protect national security, defense, public security, investigations of criminal offenses, economic or financial interest, and the rights of others."[29] The penalties for non-compliance vary among EU nations, but they tend to be harsh.[30]

The Directive requires non-EU nations, such as the U.S., to have adequate data protection measures in order for data transfers to that non-EU nation to be permitted.[31] Article 25 of the Directive states, "Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with national provisions adopted pursuant to the other provisions of the Directive, the third country in question ensures an adequate level of protection."[32] To determine if a nation has adequate protection EU states will examine: "the nature of the data, the purpose and duration of the proposed processing operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional

information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law." In such exceptional situations appropriate safeguards must be set into place. Directive 95/46, *supra* note 21, at art. 11(2); Salbu, *supra* note 11, at 670.

26. *See* Gubitz, *supra* note 3, at 437; EPIC Passenger Data, *supra* note 24.

27. Gubitz, *supra* note 3, at 437-38.

28. *See* EPIC Passenger Data, *supra* note 24. According to the Directive, EU member states must ensure that an individual's data is, "1) processed in a fair and lawful manner; 2) collected for specific and legitimate purposes, 3) relevant and not excessive in regard to the purposes of data collection; 4) accurate, updated, and corrected or erased if false; and 5) stored for no longer than necessary to identify the data subjects in relation to the purpose of data collection." Directive 95/46, *supra* note 21, art. 6(1); Gubitz, *supra* note 3, at 437.

29. Gubitz, *supra* note 3, at 438.

30. *See* Gubitz, *supra* note 3, at 432 (listing various fines imposed by nations).

31. *See* Reynolds, *supra* note 1. Security measures in non-EU countries do not all meet the same level of protection as set forth in the Directive, making the transfer of data throughout the world a complicated matter. Liermann, *supra* note 21. EU member nations can block the data flow to third countries that do not meet their standard of data protection. Salbu, *supra* note 11, at 675.

32. Directive 95/46, *supra* note 21, art. 25(1).

rules and security measures which are complied with in that country."[33] Under Article 25 of the Directive, if a non-EU country does not have such suitable protection, EU member countries must block the transfer of data to the nation and the European Commission will enter into negotiations with that nation to attempt to resolve the problem.[34] These restrictions on third nations stem from a concern that the objectives of the Directive would fail if once the data left the EU it could be processed without adequate guidelines.[35] Despite this, Article 26 provides some relief from the prohibitions set out in Article 25 of the Directive, and allows personal data transfers under certain circumstances.[36]

D. The Safe Harbor Provision

When the Directive was implemented, the U.S. was one such nation that did not have accurate protections for the transfer of data.[37] In order to continue the flow of information from the EU to the U.S., the U.S. Department of Commerce negotiated the Safe Harbor Provision with the European Commission.[38] This Provision applies to U.S. companies that

33. Gubitz, *supra* note 3, at 438; Directive 95/46 *supra* note 21, art. 25(2); Salbu, *supra* note 11, at 675-76.

34. Directive 95/46, *supra* note 21, art. 25; *see also* Liermann, *supra* note 21. When the European Commission finds that a third country is not meeting the required level of data protection it will enter into negotiations to ensure that the third country either modifies its domestic laws or enters into international agreements to meet the objectives of the directive. Gubitz, *supra* note 3, at 438-39.

35. A concern that the action of third nations could undermine the data protection, despite a guideline like the Directive, has been a concern since the OECD Guidelines were issued in 1980. Therefore the Directive creates a threat that was not present in the OECD Guidelines, that a lax in protection will result in a halt in the free flow of data. *See* Directive 95/46, *supra* note 21; OECD Guidelines, *supra* note 19; Salbu, *supra* note 11, at 677-678.

36. Directive 95/46, *supra* note 21, at art. 26; *see* Salbu, *supra* note 11, at 676. These exceptions create ambiguities that create "wiggle–room" for non-EU nations, which could potentially jeopardize the efficiency of the Directive. The reasoning behind such ambiguities is to avoid prohibiting the flow of data to third nations in situations where the requirements of European member countries requirements would have been met. Salbu, *supra* note 11, at 677.

37. *See* Gubitz, *supra* note 3, at 439.

38. The safe harbor provision was negotiated by the U.S. and the EU from 1999 to 2000. The U.S. submitted a document which had a goal of meeting the standards set forth by the directive while still being "predictable and unambiguous" called the International Safe Harbor Privacy Principles. This document was rejected but the Article 31 Committee on Data Privacy eventually approved a later version which was published in the Federal Register on July 24, 2000, and by the European Commission in Decision 2000/520/EC on July 26, 2000. *See* Salbu, *supra* note 11, at 678; Roos, *supra* note 1, at 1157; Gubitz, *supra* note 3, at 439-440; Liermann, *supra* note 21; SWIFT: SWIFT Safe Harbor Policy statement on Compliance Policy, *archived at* http://www.webcitation.org/5WBIrvdqd (July 16, 2007) [hereinafter SWIFT Safe Harbor].

use personal data from EU member countries in a commercial capacity.[39] In order to continue to freely receive this personal data, a U.S. company must join the Safe Harbor and comply with specific privacy measures.[40] The Safe Harbor deals with data protection in regards to "notice, choice, onward transfer, security, data integrity, access, and enforcement".[41] The European Commission decided that if these seven measures were followed then the objectives of the Directive would be satisfied.[42] A failure to continue to meet the requirements after joining the Safe Harbor results in penalties under U.S. law.[43] Despite these measures, several groups felt that these provisions were too lenient and by approving the Safe Harbor agreement, the European Commission failed to provide adequate protection as set forth by the Directive.[44] An example of one such possible problem is that compliance with the Safe Harbor agreement is voluntary by U.S. companies who can attempt to receive data without meeting the requirements set forth in the agreement.[45] These possible loopholes that were left to be addressed have caused problems recently in regards to data transfer, in particular the tracking of international financial transactions.

39. Compliance with the Safe Harbor is voluntary and if a company decided to follow its measures it must follow specific privacy protections to continue the free flow of data from EU member nations. Liermann, *supra* note 21.

40. "To join Safe Harbor a U.S. company must take two actions: it must publicly certify its adherence to Safe harbor, and it must establish a three-step complaisance program found at www.export.gov/safeharbor/." Liermann, *supra* note 21. When a company intends to comply with the Safe Harbor it must notify the U.S. Commerce Department and publicly disclose its intent to comply with the Safe Harbor Principles." Salbu, *supra* note 11, at 680. *See* Roos, *supra* note 1, at 1157.

41. Salbu, *supra* note 11, at 680-81; Roos, *supra* note 1, at 1157-59. "If the companies agree to the principles, they have to 1) notify the data subjects of the purpose of processing; 2) give the subjects a choice to opt out or opt in; 3) allow data subjects access to the information; 4) provide adequate privacy protection before transferring the data; 5) provide reasonable security measures; 6) ensure that the data is accurate, complete and current, and used for its stated purpose; and 7) establish effective enforcement mechanisms." Gubitz, *supra* note 3, at 440.

42. *See* Roos, *supra* note 1, at 1157-59.

43. Liermann, *supra* note 21. If a company follows the safe harbor, it must do so "subject to a U.S. government body 'empowered to investigate complaints and to obtain relief against unfair or deceptive practices as well as redress for individuals, irrespective of their country of residence or nationality, in case of non-compliance with the Principles.'" Salbu, *supra* note 11, at 680 (quoting Commission Decision 2000/520/EC, 2000 O.J. art. 1(2)(b)).

44. *See* Salbu, *supra* note 11, at 679.

45. Liermann, *supra* note 21.

II. The Tracking of SWIFT Messages

A. The Need for a Financial Tracking Program

Just weeks after the September 11, 2001 terrorist attacks on America, the U.S. government, under the Administration of President George W. Bush, began a variety of emergency secret counterterrorism programs to track terrorist actions and prevent future attacks.[46] A major priority among these measures was to cut of financing to Al Qaeda terrorists, who purportedly financed their attack on 9/11 through the movement of money.[47] On September 23, 2001, President Bush issued Executive Order 13224 which authorized the Treasury Department to "use all appropriate measures to identify, track and pursue not only those persons who commit terrorist acts here and abroad, but also those who provide financial or other support for terrorist activity."[48] Under this order, the Treasury Department created the Terrorist Finance Tracking Program (TFTP) to, "identify, track, and pursue suspected foreign terrorists...and their financial supporters."[49] In order to implement this plan, the Treasury first looked to credit card companies in hopes to devise a plan where the government would be alerted any time someone purchased items that could be used in bomb building, such as fertilizer.[50] However, the credit card companies informed the U.S. government that this was a logistical impossibility and as such they could not effectively comply with the government's initiative.[51] U.S. officials then turned to money transfers in a hope to accomplish their goals, and directed the

46. Eric Lichtblau & James Risen, *Bank Data Sifted in Secret by U.S. to Block Terror*, N.Y. TIMES, June 23, 2006, at A1; *Follow the Money, and the Rules*, N.Y. TIMES, June 24, 2006, at A14 [hereinafter Follow the Money].

47. Nine of the hijackers were able to funnel over $130,000.00 into SunTrusts bank accounts in Florida from people abroad who had known Al Qaeda links. Lichtblau, *supra* note 46.

48. *See* Lichtblau, *supra* note 46. President Bush declared that we "would use all elements of national power to fight a different kind of war against terror." The Department of the Treasury: Press Room, Terrorist Finance Tracking Program Fact Sheet (June 23, 2006), *archived at* http://www.webcitation.org/5WBJ7Vgvp [hereinafter TFTP Fact Sheet]. Executive Order 13224 defines terrorism as "an activity that involves a violent act or an act dangerous to human life, property, or infrastructure; and appears to be intended to intimidate or coerce a civilian population; to influence the policy of a government by intimidation or coercion; or to affect the conduct of a government by mass destruction, assassination, kidnapping, or hostage taking." Official Journal of the European Union, *Processing of EU originating Personal Data by United States Treasury Department for Counter Terrorism Purposes—'SWIFT'*, 2007/C 166/09, at 20 (July 20, 2007) [hereinafter Processing of EU Data].

49. *See* TFTP Fact Sheet, *supra* note 48.

50. *See* Lichtblau, *supra* note 46

51. Lichtblau, *supra* note 46.

Federal Bureau of Investigation (FBI) to subpoena records from Western Union and the First Data Corporation.[52] It was not until government officials received the suggestion of a Wall Street executive that they turned to SWIFT.[53] Few government officials had known about SWIFT, but they soon found it as an unmatched way to access information regarding international financial transactions.[54] Initially government officials wanted to use the Central Intelligence Agency (CIA) to secretly gain access to the SWIFT database, however Treasury officials decided the best course of action would be to go directly to SWIFT through the use of subpoenas.[55] The government elected to keep the program secret in order to maintain effectiveness and only briefed several members of Congress, including members of the House and Senate intelligence committees, regarding the details of the TFTP.[56] The SWIFT program soon became the most far-reaching of all the U.S. government's attempts to track terrorist financing in the post 9/11 era.[57]

B. How SWIFT Works

SWIFT is an industry owned cooperative that supplies a messaging service and interface software to world wide financial institutions.[58] SWIFT is based in Belgium and despite not being a bank in and of itself, it is the nerve center of the global banking industry; routing over six

52. The First Data Corporation is the parent company of Western Union. FBI officials claimed they used narrow warrants to obtain records of credit and debit card transactions from First Data and to trace wire transfers of Western Union to locate suspects, mainly outside the United States. In the past officials had used grand-jury subpoenas or court approved warrants to gain access to financial data, but since 9/11 the FBI more frequently uses an administrative subpoena, or national security letter, to obtain such data. Lichtblau, *supra* note 46.

53. Many financial company executives wanted to help the government with programs like the Treasury created, because many individuals in the financial industry had lost friends and co-workers in the World Trade Center and viewed this attack as on the financial industry as a whole. Lichtblau, *supra* note 46.

54. *See* Lichtblau, *supra* note 46.

55. *See* Lichtblau, *supra* note 46.

56. TFTP Fact Sheet, *supra* note 48.

57. *See* Lichtblau, *supra* note 46.

58. SWIFT, SWIFT Statement on Compliance Policy, *archived at* http://www.webcitation.org/5WBJC4txK (June 23, 2006) [hereinafter SWIFT Compliance Statement]. *See also* TFTP Fact Sheet, *supra* note 48. SWIFT provides services to over 7,800 financial institutions worldwide. It is owned by over 2,200 organizations, including almost every major commercial bank. SWIFT routes over 11 million transactions daily, many over international borders. Lichtblau, *supra* note 46. SWIFT was founded in 1973 in Brussels, Belgium. Bruce Zagaris, *The Interaction of International Tax Enforcement, Money Laundering, and Other Regulatory Threats: Estate Planners Beware!* SM033 ALI-ABA 139, 174 (2006).

trillion dollars daily.[59] SWIFT is overseen by a committee that includes several major banks, such as; The U.S. Federal Reserve, The Bank of England, the European Central Bank, the Bank of Japan, and the National Bank of Belgium; which is the lead overseer on the committee.[60] This banking consortium is solely a messaging service and does not hold accounts, as it is not a bank.[61] A typical SWIFT transaction operates in a sender instructing a financial institution to send money to a recipient of choice.[62] The sender's bank then sends payment instructions to the receiver's bank through SWIFT.[63] SWIFT processes the message but does not move money with the message.[64] When the transaction is completed the sender's bank will transfer the money to the recipient's bank and it credits the amount to the recipient's account based on the message.[65]

C. The TFTP's Legal Backing

Officials within the TFTP decided that the best way to gain access to SWIFT's financial data would be through the use of administrative subpoenas.[66] These administrative subpoenas were reviewed by a high-level Treasury Department official and not by any judicial authority.[67] Treasury officials justified their actions, after consulting with the Justice Department, by rationalizing that SWIFT was not a bank, rather a banking cooperative, and therefore bank privacy laws did not apply.[68] The United States maintains that TFTP meets U.S. legal regulations and takes into consideration the sensitive nature of the data in question.[69]

59. Lichtblau, *supra* note 46; John Rega & Jones Hayden, *SWIFT's bank-data transfers to U.S. violated privacy rules, EU says; SWIFT ordered to stop infringement Action highlights security rift*, TORONTO STAR, Nov. 24, 2006, at F03.

60. TFTP Fact Sheet, *supra* note 48.

61. SWIFT Compliance Statement, *supra* note 58.

62. Lichtblau, *supra* note 46.

63. Lichtblau, *supra* note 46.

64. Lichtblau, *supra* note 46. The message includes names and number of accounts involved. *See* Lichtblau, *supra* note 46.

65. Lichtblau, *supra* note 46.

66. Such subpoenas allow for the broad review of millions of record in contrast to court-approved warrants or subpoenas which are limited to specific transactions. *See* Lichtblau, *supra* note 46; Sarah Laitner & Michael Peel, *International Economy and the Americas: SWIFT in post-9/11 breach*, FIN. TIMES, Nov. 24, 2006 at 8.

67. Electronic Privacy Information Center, Spotlight on Surveillance: Treasury's International Finance Tracking Program of Questionable Legality (June 2006), *archived at* http://www.webcitation.org/5WBJlpMmY [hereinafter EPIC Spotlight].

68. Officials further found that the law was created to protect individuals and small companies not major banking institutions. Lichtblau, *supra* note 46.

69. *See* Processing of EU Data, *supra* note 48, at 18.

Officials continue to find authority for the program "based on statutory mandates and Executives Orders, including the International Emergency Economic Powers Act of 1977 (IEEPA) and the United Nations Participation Act (UNPA)."[70] SWIFT stated to officials that the only way it would turn over its information would be in response to such subpoenas and it would not do so voluntarily.[71] Government officials represent that they only used the information collected for the purpose of battling terrorism, and even if information was or is discovered involving other unlawful activity, it will not be used for that purpose.[72] The U.S. further holds that its actions did not violate EU law because the information used in the program was not "sensitive data as referred to in Article 8 of [the] Directive..." [73]

Although U.S. officials maintained that their program was legal, over the course of the program, SWIFT executives became increasingly concerned about the TFTP 's legality and how a program they had envisioned as a short term response to 9/11 was continuing on for years.[74] SWIFT executives believed they were dealing with a "gray area of the law" and considered a potential objection to the program based on statutory or Fourth Amendment grounds.[75] SWIFT decided its best option would be to meet with top government officials.[76] SWIFT executives subsequently were invited to Washington to meet with Alan Greenspan, the then chairman of the Federal Reserve, and Robert S. Mueller III, the director of the FBI, as well as other officials.[77] At this meeting new controls were introduced for the TFTP program as it

70. *See* TFTP Fact Sheet, *supra* note 48. President Bush evoked the IEEPA after the 9/11 attacks, giving his administration a broad authority to "investigate, regulate, or prohibit foreign transactions in respond to an unusual and extraordinary threat"; Lichtblau, *supra* note 46.

71. *See* Lichtblau, *supra* note 46; EPIC Spotlight, *supra* note 67; SWIFT Compliance Statement, *supra* note 58; John Ward Anderson, *Belgium Rules Sifting of Bank Data Illegal*, WASH. POST, Sept. 29, 2006, at A14.

72. "General investigations of tax evasion, money laundering, economic espionage, narcotics trafficking or other criminal activity [are not conducted] unless in a particular instance such activity has been connected to terrorism or its financing." Processing of EU Data, *supra* note 48, at 18.

73. Such data includes "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning the health or sex life of the individual." Processing of EU Data, *supra* note 48, at 19.

74. Follow the Money, *supra* note 46. By 2003 SWIFT executives were considering ending involvement with the program because of the legal and financial risk it posed to the cooperative if the program went public. Lichtblau, *supra* note 46.

75. Lichtblau, *supra* note 46.

76. *See* Follow the Money, *supra* note 46.

77. *See* Follow the Money, *supra* note 46.

applied to SWIFT.[78] An outside auditing firm was appointed by the U.S. government to ensure that government investigators had real intelligence leads in regard to individuals whose information they requested.[79] Further, SWIFT representatives were able to block any searches from intelligence officials that seemed inappropriate or overreaching.[80]

D. The Secret is Leaked and the World Reacts

Although the government intended for this program to remain secret, on June 23, 2006, articles by the *New York Times*, *Los Angeles Times*, and *Wall Street Journal* brought the TFTP and its use of SWIFT to the public's attention.[81] SWIFT quickly responded to the release of this information in a damage control effort by issuing an official statement on its website that same day.[82] The full committees of Congress were briefed on the program a month prior to the publishing of these articles when it was discovered that the information was leaked to the press and would soon be in news reports.[83]

Once the program was discovered, different organizations and government officials began to question the possible privacy violations from the unusually large amounts of confidential data that was obtained through the TFTP.[84] Because SWIFT is based in Belgium, yet has offices in the United States and other places around Europe and the globe, it is governed by both American and European laws.[85] Foreign governments were immediately concerned that this program was in violation of EU data protection laws.[86] Numerous EU member nations and privacy watchdog groups called for an immediate investigation of the program.[87] After such preliminary investigations, on September 28, 2006, the Belgian Prime Minister, Guy Verhofstadt, announced that SWIFT had violated both Belgium and European law when it complied

78. *See* Lichtblau, *supra* note 46, at A1; Follow the Money, *supra* note 46.
79. *See* Follow the Money, *supra* note 46; SWIFT Compliance Statement, *supra* note 58. Regular audits are now conducted by Booz Allen Hamilton, Inc., a firm hired by the government. EPIC Spotlight, *supra* note 67.
80. Lichtblau, *supra* note 46.
81. EPIC Spotlight, *supra* note 67; Patrick Van Eecke and Maarten Truyens, LEGAL WEEK, Benelux: Swift Response (Dec. 14, 2006), *archived at* http://www.webcitation.org/5WBKDwOKp; *See* Follow the Money, *supra* note 46.
82. SWIFT Compliance Statement, *supra* note 58.
83. SWIFT Compliance Statement, *supra* note 58.
84. *See* Lichtblau, *supra* note 46.
85. Lichtblau, *supra* note 46.
86. EPIC Spotlight, *supra* note 67.
87. EPIC Spotlight, *supra* note 67.

with the United States subpoenas.[88] Verhofstadt stated, that although SWIFT may have been complying with American laws, it should have ensured it was also complying with European laws and informed European governments of the program.[89]

Treasury Secretary John Snow defended the program, saying that U.S. government officials only received data from SWIFT of suspected terrorists for whom the government had supporting evidence to prove such accusations.[90] Such evidence would exist if the individual's name were on a watch list or a classified cable.[91] The government also reassured that it only sought data for terrorism investigations and did not use the information for, "tax fraud, drug trafficking, or other inquiries".[92] Despite such reassurances, it was admitted that the data the Treasury received was shared with other government agencies, such as the CIA and the FBI.[93] The government further held that, despite the concerns about the program, it has found it to be very successful in tracking and disrupting terrorist activity.[94]

III. SWIFT's Current Status and How to Move Forward

A. SWIFT'S Dilemma

The conflict between American anti-terrorism law and European law placed SWIFT in an extremely difficult position.[95] SWIFT was stuck between U.S. officials who were issuing subpoenas to gain access to customer data, and European officials who were threatening sanctions

88. The Belgium Data Privacy Commission simultaneously released a report which stated that, "It has to be seen as a gross miscalculation by SWIFT that it has, for years, secretly and systematically transferred massive amounts of personal data for surveillance without effective and clear legal basis and independent controls in line with Belgian and European law." Anderson, *supra* note 71.

89. Anderson, *supra* note 71.

90. *See* EPIC Spotlight, *supra* note 67.

91. US terror watch lists include over 325,000 names and have often identified innocent people. *See, e.g.* EPIC Spotlight, *supra* note 67 (listing examples of misidentified individuals).

92. Lichtblau, *supra* note 46.

93. EPIC Spotlight, *supra* note 67.

94. *See* TFTP Fact Sheet, *supra* note 48. SWIFT data identified a man in Southeast Asia who gave financial support to a person being suspected Al Queada member which helped located the terrorist Riduan Isamuddin, known as Hambali in Thailand in 2003. Hambali was believed to be the mastermind behind the 2002 bombing of a Bali resort. Further, SWIFT data identified a Brooklyn man, Uzair Paracha who aided al Qaeda operative by agreeing to launder $200,000.00 into the United States. *See* Lichtblau, *supra* note 46; Alasdair Palmer, *The Bomber's Privacy is Paramount*, THE SUNDAY TEL., Nov. 26, 2006, at 22.

95. *See* Van Eecke, *supra* note 81; Sandman, *supra* note 22.

for SWIFT cooperating with such subpoenas.[96] SWIFT faced the penalty of EU sanctions on the one hand and the possibility of U.S. officials going after SWIFT management personally for not complying with the issued subpoenas on the other.[97]

Despite the European Union's criticism of SWIFT's actions, SWIFT's CEO, Leonard Schrank, defended SWIFT's actions, stressing how the cooperative takes data privacy very seriously and that their actions did not violate privacy laws.[98] SWIFT also tried to defend itself in the legal area by submitting a brief to both Belgian and EU officials outlining the reasoning behind SWIFT's actions and how their compliance with the subpoenas did not violate EU law.[99] SWIFT contended that because it is a messaging service and not a bank, it is a processor of personal data, rather then a controller as defined by the Directive.[100] Unlike controllers, which are firms which "keep personal data on private individuals [and] have obligations to prevent the data from being shared...[notifying] governments before any such transfers take place," processors are a conduit of data, "much like an email provider or phone company" which allows it a great deal more latitude in its use of data.[101] SWIFT further argued that if they were found to be a controller, then other telecom companies would have to be as well, something that would be "totally impractical", according to SWIFT Chief Financial Officer, Francis Vanbever.[102] Through it all, SWIFT has continued to hold that "its compliance was legal, limited, targeted, protected, audited and overseen...[and that it] also did its utmost to comply with the European data privacy principles of proportionality, purpose and oversight."[103]

SWIFT continued to attempt to rebuild its reputation by promising to work with authorities to seek solutions to international conflicts of law such as this one.[104] However, throughout the entire conflict SWIFT held that only negotiations between U.S. and EU officials to create

96. Rega, *supra* note 59 at F03; Dan Bilefsky, *Panel Says Ban Group, Aiding U.S., Broke Law*, N.Y. TIMES, Nov. 23, 2006, at A22.

97. Dan Atkinson, *Banks Face US Spy Row Fines; EU Threatens Massive Penalties Over Confidentiality Breach,* MAIL ON SUNDAY, Nov. 26, 2006, at 2.

98. Sandman, *supra* note 21.

99. *See* Just One Minute: The SWIFT Surveillance Program – Still Alive, *available at* http://www.webcitation.org/5WBKWAFXZ (Nov. 21, 2006) (last visited Jan. 28, 2008) [hereinafter Just One Minute].

100. *See* Just One Minute, *supra* note 99.

101. Just One Minute, *supra* note 99; *see generally*, Directive 95/46, *supra* note 21.

102. Just One Minute, *supra* note 99.

103. Anderson, *supra* note 71.

104. Sandman, *supra* note 21.

comparable privacy protections would alleviate the problem.[105]

B. The Compelling Reasoning

Both the U.S. and EU have compelling reasoning behind their actions.[106] The U.S. wants to keep its citizens safe from terrorists and the EU wants to protect its citizens from invasions of privacy.[107] Such clashes between U.S. and EU law have been ongoing in recent years.[108] Most recent was the debate over the use of airline passenger information.[109] In regards to that conflict, U.S. and EU officials were able to achieve a deal allowing U.S. intelligence agencies access to the personal data of passengers flying from the EU to the U.S.[110] However, such an agreement came only after the U.S. threatened to deny landing slots to planes coming from the EU.[111]

1. The Argument from the U.S. Perspective

Those who support the U.S. position in the matter argue the importance of anti-terrorism measures in today's society.[112] While an EU WP29 resolution was aimed at punishing SWIFT for allowing the U.S. to view customer information in the name of public safety, the EU commission allows tax and customs administrators to look at bank transactions without violating privacy rights.[113] Essentially, it is argued that it is a human rights violation for the U.S. to work to prevent another 9/11, yet it is permissible for the EU to ensure it receives tax payments.[114] Those supporting the U.S. position hold that the EU officials criticizing the actions of SWIFT and the United States are rigorously attempting to apply their data privacy protection laws that were created in 1995, without considering the effect this may have on third party countries such as the United States.[115] Some have questioned why the EU has waited so long to enforce its Data Protection Directive which predates the U.S. tracking program by around seven years.[116]

105. Rega, *supra* note 59.
106. *See* Laitner, *supra* note 66.
107. *See* Laitner, *supra* note 66.
108. *See* Laitner, *supra* note 66.
109. Laitner, *supra* note 66.
110. Laitner, *supra* note 66.
111. Laitner, *supra* note 66.
112. Palmer, *supra* note 94.
113. Palmer, *supra* note 94.
114. *See* Palmer, *supra* note 94.
115. *See* Van Eecke, *supra* note 81.
116. Sandman, *supra* note 21.

The U.S. government holds that the TFTP is necessary in order for America and its allies to fight the world-wide war on terror and that the citizens of the world are safer for it.[117] The government further believes that tracking of terrorist financing is particularly important because it enables the government to analyze "how terrorists...earn, move, and store money."[118] Terrorists need a steady supply of funds in order to "pay operatives, arrange for travel, train new members, forge documents, pay bribes, acquire weapons, and state attacks."[119] With this information law enforcement can combat terrorism more effectively.[120]

The U.S. Department of the Treasury believes that it has been transparent with its program.[121] The government's efforts to track terrorists have been discussed in "congressional testimony, public speeches [and] communications with the news media."[122] Despite the transparency of its mission the Treasury explains that it is necessary, as with any national security program, to keep some measures out of the public eye to maintain effectiveness of the program.[123] In fact, President Bush called the disclosure of the program by the media "disgraceful."[124] Although the exact details of the TFTP program were not provided to the European Union and the public at large, the world knew that the U.S. government was using surveillance methods to fight the war on terror.[125]

The U.S. acknowledges that electronic surveillance without a court order would be illegal, however here the U.S. served SWIFT with subpoenas and those in charge of the messaging service were fully aware of the actions taken by the U.S. and even asked for input on the program.[126] In additional support of the program, officials assert that similar programs have been under way in the U.S. for years.[127] The President has authority over financial transactions made by America's enemies through the 1977 International Economic Emergency Powers Act.[128] In addition the U.S. has taken international initiatives against money laundering for over a decade which have been focused on "drug cartels, corrupt foreign officials and a host of criminal organizations" in

117. TFTP Fact Sheet, *supra* note 48.
118. Processing of EU Data, *supra* note 48, at 19.
119. Processing of EU Data, *supra* note 48, at 19.
120. *See* Processing of EU Data, *supra* note 48, at 19.
121. *See* TFTP Fact Sheet, *supra* note 48.
122. TFTP Fact Sheet, *supra* note 48.
123. *See* TFTP Fact Sheet, *supra* note 48.
124. Anderson, *supra* note 71.
125. *See* TFTP Fact Sheet, *supra* note 48.
126. Richard A. Clarke and Roger W. Cressey, *A Secret the Terrorists Already Knew*, N.Y. TIMES, June 30, 2006, at A23.
127. *See* Clarke, *supra* note 126.
128. Clarke, *supra* note 126.

addition to terrorists.[129] In the domestic arena, since 2001 U.S. banks have been required to report transactions within the U.S. that are believed to involve illegal activity.[130]

Additionally, the Bush Administration feels its actions were in line with what U.S. citizens expected in order to fight terror.[131] The U.S. Treasury Department has stated that, "[t]he 9/11 Commission was critical of the government for its failure to have this kind of program – one that uses all available information to connect the dots—in place prior to the September 11th attacks. In fact, in its final report card the 9/11 Commission's Public Discourse Project awarded the government-wide effort to combat terrorist financing the highest grade, citing the government's significant strides in using terrorism finance as an intelligence tool."[132]

Even if the program was hidden, at the insistence of SWIFT, the U.S. has taken actions to ensure that the privacy violations which concern the EU are limited.[133] Booz Allen Hamilton, an outside auditing firm, was appointed to safeguard the system and guarantee that the data is used only in situations where there is intelligence that the individual is linked to terrorists.[134] The U.S. also allows SWIFT and the auditing firm an opportunity to object if they believe a search may be used for other purposes or is unwarranted.[135] The Treasury Department likewise ensures that "searches of records must identify the terrorism-related basis, which is systematically logged and auditable" and that it is not an overbroad system affecting ordinary European citizens.[136] Even if the auditing taking place was not up to EU standards, it is the U.S. position that the subpoenas to SWIFT do not violate the Directive because SWIFT is not a bank, rather it is a messaging service used by banks.[137]

Although the TFTP has been widely criticized, the U.S. government points to the results it has achieved from the program.[138] Numerous terrorists have been tracked and arrested as a result of TFTP.[139] The U.S. government believes that "going after terrorists money is a necessary element of any counterterrorist program" and has been a

129. Clarke, *supra* note 126.
130. Clarke, *supra* note 126.
131. *See* TFTP Fact Sheet, *supra* note 48.
132. TFTP Fact Sheet, *supra* note 48.
133. *See* Zagaris, *supra* note 58, at 175.
134. Zagaris, *supra* note 58, at 175.
135. Zagaris, *supra* note 58, at 175.
136. TFTP Fact Sheet, *supra* note 48.
137. *See* Zagaris, *supra* note 58, at 175.
138. Clarke, *supra* note 126.
139. *See e.g.*, *supra* note 90 and accompanying text (illustrating known terrorists that have been captured as a result of TFTP).

tactical element employed by the government since well before 9/11.[140] In the previous Administration, President Bill Clinton used the tracking of terrorist finances in presidential directives in 1995 and 1998.[141] The rational behind such tactics is that although "individual terrorist attacks do not typically cost very much...running terrorist cells, networks, and organizations can be extremely expensive."[142] "Al Qaeda, Hamas, Hezbollah and other terrorist groups have had significant fundraising operations involving solicitation of wealthy Muslims, distribution of narcotics and...sales of black market cigarettes..."[143] Even if terrorists are not found directly through such tracking it still makes operations for terrorists more difficult.[144] The U.S. government has found this program so successful that Congress has asked the Treasury's Financial Crimes Enforcement Network to investigate the development of a similar program that reviews "all cross-border financial transactions."[145]

2. The E.U. Position

After SWIFT's actions came to light, the issue still remained of what repercussions SWIFT and the nations involved should face, and how to find a solution to SWIFT's continuing compliance with U.S. subpoenas.[146] Belgium, the nation in which SWIFT is headquartered, and EU financial institutions were among those accused for being responsible for not forcing SWIFT to refrain from allowing the U.S. to view the financial data of EU citizens.[147] EU officials said that the banks that used SWIFT had a legal obligation to remedy SWIFT's illegal actions and to make sure SWIFT and the banks were in full compliance with the Directive.[148] EU officials instructed SWIFT to immediately remedy the continuing infringement.[149] The WP 29's report stated that "Belgium and European privacy legislation had been

140. Clarke, *supra* note 126.
141. Clarke, *supra* note 126.
142. Clarke, *supra* note 126.
143. Clarke, *supra* note 126.
144. *See* Clarke, *supra* note 126.
145. TFTP Fact Sheet, *supra* note 48.
146. *See* Bilefsky, *supra* note 96, at A22; Atkinson, *supra* note 97, at 2.
147. Atkinson, *supra* note 97, at 2. The EU commission is currently determining whether Belgium will be taken to court for its failure to monitor SWIFT and force the cooperative to comply with EU data protection directives. Bilefsky, *supra* note 96, at A22. EU banks are facing the threat of an unlimited amount of fines for allowing the US access to their customer's accounts. Any bank that used the SWIFT system could be punished because of SWIFT's dealing with the US government. *See* Atkinson, *supra* note 97, at 2.
148. *See* Atkinson, *supra* note 97, at 2.
149. Rega, *supra* note 59, at F03.

seriously infringed because the hidden, systematic, massive and long-term transfer of personal data by SWIFT to the [U.S. Treasury] in a confidential, non-transparent and systematic manner for years constitutes a violation of the fundamental European principles..."[150] Prime Minister Verhofstadt added that, "SWIFT is also clearly responsible because they made all the crucial decisions regarding data communication to the U.S. Treasury, behind the back of its 7,800 clients."[151]

In addition to the actions taken against SWIFT by the European Union, many individual human rights groups and privacy watchdog groups filed complaints against SWIFT and EU banks which used SWIFT's services.[152] The human rights group, Privacy International, filed complaints in at least thirty-two nations, including the twenty-five countries that make up the EU.[153] Many privacy groups have associated the TFTP with the national Security Agency's program of wiretapping international calls from the U.S. to Europe and other areas abroad, both of which these groups claim violate civil liberties.[154] In response to the Bush administration's claim that having the program publicized would alert the terrorists, some have responded that terrorists already know that their funds may be tracked.[155] As one critic wrote, "[t]hey [the Bush administration] want the public to believe that it had not already occurred to every terrorist on the planet that his telephone was probably monitored and his international bank transfers subject to scrutiny."[156] In fact, because many terrorists assume their actions may be tracked by a large number of countries, terrorists for years have used nontraditional ways to communicate and transfer funds such as "the ancient Middle Eastern hawala system" which involves a network of couriers and money brokers.[157]

Another concern of both the European Union and privacy watchdog groups was how the information was being used.[158] Although the U.S. government claims that the data is only tracked for the purpose of finding terrorist funding, critics feared that such information could be used in other areas.[159] Some contend that the use of government

150. *See* Van Eecke, *supra* note 81.
151. Anderson, *supra* note 71.
152. *See* Atkinson, *supra* note 97, at 2.
153. Katrin Bennhold, *Parliament Tells Europeans to Explain What They Knew About U.S. Tracking of Bank Data*, N.Y. TIMES, July 7, 2006, at A10.
154. *See* Clarke, *supra* note 126, at A23.
155. *See* Clarke, *supra* note 126, at A23.
156. Clarke, *supra* note 126.
157. Clarke, *supra* note 126.
158. *See* Follow the Money, *supra* note 46, at A14.
159. *See* Follow the Money, *supra* note 46, at A14 (stating that a danger of the

agencies to regulate such investigations may violate the privacy of Americans as well as EU citizens.[160]

A further concern of the European Union was "whether other wholesale banking and payment networks, such as the New York Clearing House's Chips and Federal Reserve System's Fedwire, have been subject to similar subpoenas or other data requests... and if so, how they responded."[161] Although officials from the treasury and networks like the ones discussed have failed to comment on whether such subpoenas have been issued, the Senior Vice President of the Federal Reserve Bank of New York, Calvin Mitchell has commented that they have responded to some subpoenas for transactions that took place over Fedwire.[162]

Although EU officials recognize that terrorists threats are a real problem in the world today, their view differs from that of the U.S. over the methods that should be used to combat terror.[163] EU officials feel that the U.S. government should have informed them of a program that affected EU citizens.[164] The EU parliament adopted a resolution saying "it is 'implausible' that 'certain European governments' were unaware... [of what was] taking place."[165] Jean-Marie Cavada, a French Liberal lawmaker stated, "'[n]ow we discover that our powerful friend and ally is rifling through our private bank accounts'.... Freedom...'is not the enemy of our citizens, and it is high time the United States decided which camp they belong to'."[166] Italian lawmaker, Giusto Catania, has likewise criticized the SWIFT situation saying that the U.S. objective is to "extort information."[167]

C. A Solution to the SWIFT Problem

Many individuals and groups suggested possible solutions to the SWIFT dilemma.[168] However most of these solutions addressed the

US government going through individuals' financial transactions is "mission creep").

160. *See* Follow the Money, *supra* note 46, at A14.
161. Sandman, *supra* note 21, at 29.
162. Sandman, *supra* note 21, at 29.
163. Bennhold, *supra* note 153.
164. *See* Bennhold, *supra* note 153.
165. Bennhold, *supra* note 153.
166. Bennhold, *supra* note 153.
167. Bennhold, *supra* note 153.
168. Sandman, *supra* note 21, at 28. An EU monitoring committee, comprised of data protection supervisors from all 25 EU nations found that numerous financial institutions, in addition to SWIFT, were in breach of European civil liberties through their cooperation with US tracking programs. Bilefsky, *supra* note 96, at A22.

SWIFT situation particularly and were not aimed to solve the overarching problem at hand.[169] One of the possibilities examined was to move the SWIFT headquarters to Canada to avoid U.S. legal control over SWIFT.[170] Others suggested the U.S. government retain the ability to monitor SWIFT, however, these efforts should "be done under a clear and coherent set of rules, with the oversight of Congress and the courts."[171] There was also a discussion of the possibility of the U.S. and the EU sharing oversight of the program as well as an outside auditing firm.[172] It was further recommended by groups that the encryption system used on the financial data be strengthened so that the U.S. would be unable to view the information of EU citizens.[173]

SWIFT took internal initiative and developed a re-architecture of its structure in order to quell the concerns of the EU.[174] SWIFT has worked to change its methods in order to qualify for protection under the EU-U.S. Safe Harbor Agreement.[175] In order to meet the demands of the Safe Harbor, "SWIFT has set up a data privacy working group composed of data privacy and compliance experts from European and non-European banks.[176] The group has been asked to propose contractual solutions to further enhance compliance and transparency, where appropriate, for the processing of financial messaging data, including for the banks' customers."[177]

Subsequent to its decision to meet Safe Harbour provisions, SWIFT took further action and its Board of Directors has begun an initiative "to move to a multi-zonal messaging architecture."[178] This will include a new global Operating Centre in Switzerland and a command and control center in Hong Kong to enable SWIFT to be run from Asia as well.[179] SWIFT sites numerous reasons for the change, but it is highlighted by the ability to "overcome data protection concerns" by having a European

169. *See generally* Bilefsky, *supra* note 96.
170. Bilefsky, *supra* note 96.
171. Follow the Money, *supra* note 46, at A14.
172. Just One Minute, *supra* note 99.
173. Jeremy Shrader, *Secrets Hurt: How SWIFT Shook up Congress, The European Union, and the U.S. Banking Industry*, 11 N.C. BANKING INST. 397, 406 (2007).
174. SWIFT, SWIFT Announces Plans for System Re-architecture, *archived at* http://www.webcitation.org/5WBKi45Nq (June 15, 2007) [hereinafter SWIFT Re-architecture].
175. *See* Swift Re-architecture, *supra* note 174.
176. *See* Swift Re-architecture, *supra* note 174.
177. *See* Swift Re-architecture, *supra* note 174.
178. SWIFT, SWIFT Board approves messaging re-architecture, *archived at* http://www.webcitation.org/5WBKpHtZX (Oct. 4, 2007) [hereinafter SWIFT Board Approves Re-Architecture].
179. *See* SWIFT Board Approves RE-Architecture, *supra* note 178.

Operating Center.[180]

Initially, SWIFT plans on creating a European and Trans-Atlantic message processing zone, with the possibility of extending beyond these two zones if so required in the future.[181] This system will ensure that intra-European messages will remain in Europe which will overcome some data protection concerns.[182] The Swiss Operating Center will work in conjunction with the U.S. Operating Center in the processing and storage of the Trans-Atlantic messages which will hopefully increase the amount of data protection for these messages.[183]

The U.S. has also made efforts to work with the EU to help ensure that sufficient safeguards are in place.[184] In a letter from the U.S. Department of the Treasury to the General Minister of Finance and Vice-President of the European Commission, the U.S. maintained that it would "shar[e]... information about the TFTP with an eminent European to be appointed in consultation with the Treasury Department".[185] This person would work to ensure that all EU-originating personal data is protected.[186]

D. Solving the Problem at Large

Although the issue as it relates to SWIFT seems as if it will shortly be resolved once SWIFT has completed the process for entering the Safe Harbor Agreement and has created its European Operating Center, the U.S. and EU have failed to solve the overarching problem.[187] During the investigation of SWIFT and the action of the TFTP, it was made clear that this kind of gathering of data in an attempt to track terrorist financial transactions was not just limited to SWIFT.[188] If such other entities have not joined the Safe Harbor, they also are at risk of acting in a way that the EU may find violates the Directive.[189] Further, the U.S. should not put itself in the position where companies feel they cannot do

180. SWIFT Board Approves RE-Architecture, *supra* note 178.
181. *See* SWIFT Board Approves RE-Architecture, *supra* note 178.
182. *See* SWIFT Board Approves RE-Architecture, *supra* note 178.
183. *See* SWIFT Board Approves RE-Architecture, *supra* note 178.
184. *See* Processing of EU Data, *supra* note 48, at 20.
185. Official Journal of the European Union, *Notices from Third Countries: Letter from United States Department of Treasury regarding SWIFT/Terrorist Finance Tracking Programme*, 2007/C 166/08, at 17 (June 28, 2007), *archived at* http://www.webcitation.org/5WrGPPV5j [hereinafter June 28, 2007 Letter].
186. *See* June 28, 2007 Letter, *supra* note 185.
187. *See* Swift Re-architecture, *supra* note 174; SWIFT Board Approves RE-Architecture, *supra* note 178.
188. *See*, Sandman *supra* note 21, at 28.
189. *See* Salbu, *supra* note 11, at 678; *see* Roos, *supra* note 1, at 1157; *see* Gubitz, *supra* note 3, at 439-440.

business within the U.S. and need to move their centers to Europe for fear of U.S. privacy violations.[190] Although the U.S. has assigned an eminent European to monitor the TFTP, this does not guarantee that the Treasury department will monitor the new program.[191] Further it has been evident that actions by U.S. entities violate the Directive across a broad spectrum not solely limited to financial tracking but to tracking of other personal forms of data.[192] If the U.S. wishes to continue to protect its citizens and prevent terrorist attacks while still keeping businesses within its borders, it has to work in a way that will take into consideration the EU's concerns for its citizens.[193]

In a world that is becoming more connected due to technological advances, it is important that different nations work together to guarantee that the rights and needs of not only one's own country are met, but also that the rights of those in other nations are respected.[194] In order for the EU and U.S. to continue an amicable relationship in regards to the passing of data between the two nations, it is imperative that they continue to have talks and develop new solutions to the problems that will assuredly arise in this ever changing and growing area.[195]

There are several ways in which the U.S. can act in order to increase the protection of the data of EU citizens while still protecting Americans from the threat of terrorism.[196] One such way would be for the U.S. to mandate that companies who receive sensitive personal data from the EU must join the Safe Harbor.[197] This would ensure that U.S. entities were properly using the data received as in accordance with the Directive.[198] Another option would be for the U.S. to move away from its sectoral approach of regulating data privacy and to pass legislation that would take the U.S. closer to the EU's data protective regulations.[199] The EU must also attempt to work with the U.S. and understand the compromising position the nation has been put in since

190. *See* SWIFT Board Approves RE-Architecture, *supra* note 178.
191. *See* June 28, 2007 Letter, *supra* note 185 (lacking a statement of guarantee that new programs will be monitored).
192. *See*, Laitner, *supra* note 66, at 8.
193. *See generally* Sandman, *supra* note 21; *See* SWIFT Board Approves RE-Architecture, *supra* note 178.
194. *See* Salbu, *supra* note 11, at 685.
195. *See* Rega, *supra* note 59, at F03.
196. *See generally* Sandman, *supra* note 21.
197. *See* Salbu, *supra* note 11, at 678; *see* Roos, *supra* note 1, at 1157; *see* Gubitz, *supra* note 3, at 439-440.
198. *See* Salbu, *supra* note 11, at 678; Roos, *supra* note 1, at 1157; Gubitz, *supra* note 3, at 439-440.
199. *See* Roos, *supra* note 1, at 1155.

9/11.[200] The government must work diligently to protect its citizens from another terrorist attack on its soil, and the only way to successfully do so is to have as much information as possible about foreign terrorist networks.[201] If the EU could impose less stringent regulations that are required for a nation to be acceptable for passing on information then the U.S. would have an easier time complying with these regulations.

IV. Conclusion

As a result of the TFTP, the U.S. and EU were placed in conflicting positions. The U.S. wanted to monitor international financial transactions to prevent terrorists from funding another 9/11 while the EU wanted to ensure that the privacy and rights of its citizens were protected. The U.S. backed its position by saying that proper precautions were in place, such as an outside auditing firm, to prevent abuse of this program. The U.S. maintained that the program was very successful, leading to the arrest of numerous terrorists. The EU on the other hand found the U.S. program to be too broad and sweeping and a blatant violation of the Directive they had created to prevent such violations as this one.

The TFTP has not been the only area where these conflicts have arisen. In several other U.S. tracking programs such as the tracking of passenger data and wiretapping, the EU has claimed that the U.S. has violated its Directive. Under the Directive the U.S. should not be able to receive data of EU citizens because its privacy protection laws are not up to par with those of the EU. It is only by the grace of the Safe Harbor provision that the U.S. still receives such information. The U.S. must now work to renegotiate this provision and maintain a constant data flow guarantee with the EU and to ensure that businesses will keep their operating centers within the U.S. Although SWIFT will soon conform with the Safe Harbor provision and create additional centers abroad, solving the dilemma in regards to that cooperative, this is not a permanent solution to the problem at large. The U.S. and the EU need to work together to create a system where all data sent to the U.S. falls within an acceptable EU standard, and not just the information sent to a few select companies and organizations who have applied to fall within the Safe Harbor provision. If the U.S. and EU work together to create a broader solution this will solve the conflicts that exist not only in finance such as the SWIFT situation, but also in areas such as passenger data on international flights, and international phone calls. Today we

200. *See* Roos, *supra* note 1, at 1161.
201. *See* Palmer, *supra* note 94.

live in a global environment where international data transfer is a part of everyday life. There will continue to be legal battles unless some mutually satisfying agreement is reached by both parties.

Instead of the focus of this conflict zeroing in on ways to punish SWIFT for its actions, the parties should be looking for a solution. The U.S. should perhaps try to narrow its searches and subpoenas. EU banks could lessen its restrictions and let its citizens know what their personal information is being used for in order to ensure that their human rights are protected. Whenever an issue arises in which one group's rights must be compromised for another, problems will occur. In this case the U.S. and EU are looking out for the rights of their own citizens. The U.S. and EU must compromise; otherwise, these entities will not be able to have a functional and diplomatic co-existence.