NOTE

THE TERRORIST FINANCE TRACKING PROGRAM:
ILLUMINATING THE SHORTCOMINGS OF THE
EUROPEAN UNION’S ANTIQUATED DATA
PRIVACY DIRECTIVE

Justin Santolli*

INTRODUCTION

On June 23, 2006, the New York Times, the Los Angeles Times, the Wall Street Journal, and the Washington Post disclosed the existence of a confidential Treasury Department and Central Intelligence Agency (CIA) initiative, the Terrorist Finance Tracking Program (TFTP).¹ The TFTP enables the United States to examine financial transactions that rely on the messaging infrastructure provided by the Society for Worldwide Interbank Financial Telecommunications (SWIFT) for their completion.² The United States’ ability to scrutinize financial transactions that utilize SWIFT’s messaging service allows the Treasury Department to access the amount transferred, bank account numbers, method of transfer, names of the parties, their addresses and telephone numbers, and information about the financial institutions involved in the transaction.³ Due to the widespread use of SWIFT messaging among financial institutions, the TFTP provides the United States with the potential to collect and analyze information on tens of thousands of financial transactions.⁴

* J.D. 2008, The George Washington University Law School; B.A. 2005, Marist College. I would like to thank the staff and editors for their dedicated assistance and insightful comments, and my parents for their continued support and encouragement.


2. Gellman et al., supra note 1; Lichtblau & Risen, supra note 1; Meyer & Miller, supra note 1; Simpson, supra note 1.


4. See, e.g., Lichtblau, & Risen, supra note 1; Privacy Int’l., supra note 3.
Six days after the press disclosed the existence of the TFTP, the U.S. House of Representatives adopted a resolution expressing its support for the program and communicating its belief that the initiative was compatible with all applicable laws.\(^5\) The Belgian Data Protection Authority and the European Union’s Article 29 Working Party, however, concluded that the TFTP was incompatible with E.U. Directive 95/46/EC on the Protection of Individuals with Respect to the Processing of Personal Data and the Free Movement of Such Data (Data Privacy Directive).\(^6\) Despite the conclusions of the Belgian Data Protection Authority and the Article 29 Working Party, President George W. Bush indicated that the United States would not voluntarily abandon the TFTP.\(^8\) In June 2007, after months of public discord, the European Union and the Bush administration reached an agreement on the additional safeguards the United States would need to add to the TFTP in order to secure the approval of its European allies.\(^9\)

Resolving the conflict over the TFTP and SWIFT’s participation in the program will have far-reaching consequences. The European Union’s Data Privacy Directive, on the strength of its ability to create a potential information embargo,\(^10\) is becoming the world’s first universal data privacy regime.\(^11\) Countries developing their own data privacy regulations are attempting to structure their regulations to satisfy the “adequacy” standards of the Data Privacy Directive.\(^12\) There has been speculation that the United States has

---

10. See EU Directive, supra note 6, art. 25.
agreements with numerous multinational corporations requiring them to turn over any information in their possession that the United States deems relevant to the war on terrorism.\textsuperscript{13} These developments create potential for frequent disputes involving many of the same issues presented by the TFTP. Thus, the resolution of the controversy surrounding the TFTP will serve as a global precedent in determining the appropriate balance between the need for data privacy and the need for information to combat terrorism.

Part I provides an overview of the United States’ war on terrorist financing and examines the development of the TFTP. Part II examines the intricacies of the TFTP and the safeguards built into the program to protect individual privacy. Part III scrutinizes the European Union’s Data Privacy Directive and summarizes the Article 29 Working Party’s report. Part IV will demonstrate why the Data Privacy Directive is an anachronistic relic that has ceased to be beneficial. Ultimately, this Note concludes that the European Union’s attempt to unilaterally impose its vision of data privacy protection on the world is misguided because the conditions which led to the adoption of the Data Privacy Directive reflect values and experiences not shared by other countries.\textsuperscript{14}

I. THE HISTORY OF ANTI-TERRORIST FINANCING IN THE UNITED STATES

On September 11, 2001, Al Qaeda attacked the financial and the military centers of the United States.\textsuperscript{15} Prior to the September 11 terrorist attacks, the United States did not actively concern itself with terrorist financing.\textsuperscript{16} It failed to make active attempts to disrupt the conduits of terrorist financing because the minimal costs associated with conducting terrorist operations convinced law enforcement that there were more efficient mechanisms to combat

\begin{thebibliography}{9}
\end{thebibliography}
terrorism. The United States considered it futile to monitor Al Qaeda’s money trail because of the erroneous belief that Osama bin Laden, through his personal fortune, financed all of the organization’s operations.

The ability of the September 11 hijackers to utilize the global banking system to facilitate their enterprise was extremely disconcerting to both the American populace and the federal government. When the hijackers arrived in the United States, they opened bank accounts in their real names and transferred amounts ranging from $5,000 to $70,000 among the various accounts. Wire transfers from banks in the United Arab Emirates and Germany to a SunTrust branch in Florida, totaling $130,000, provided the seed money for the hijackers’ enterprise.

Before the September 11 terrorist attacks, the United States’ regulatory regime focused on combating money laundering connected to drug trafficking. It was apparent to both the Bush administration and members of Congress, however, that a regulatory regime focused on money laundering was insufficient to combat terrorist financing. This pre–September 11 regime had limited usefulness in combating terrorist financing because “terrorist financing dirties clean money” while money laundering


18. See Roth, Greenburg & Wille, supra note 17, at 20.


20. Roth, Greenburg & Wille, supra note 17, at 53. The transaction escaped notice under then existing banking regulations because the transaction was consistent with the student profile. See id.

21. See, e.g., id.; Gerth & Miller, supra note 19 (repeating the statement of the United Arab Emirates’ central bank governor that the transaction should have attracted suspicion in the United States).


2008] The Terrorist Finance Tracking Program 557

attempts to “clean dirty money.”

Thus, the United States sought to develop a regulatory regime focused on “starving the terrorists of funding.”

A. Post–September 11 Initiatives to Combat Terrorist Financing

Two weeks after the September 11 attacks, President Bush issued Executive Order 13,224. The motivating factors behind this order were the government’s desire to prevent Al Qaeda from receiving funding and to allay the populaces’ fears by taking public action against terrorism. Executive Order 13,224 declared a national emergency, thereby enabling President Bush to utilize the powers of the International Emergency Economic Powers Act (IEEPA). To implement the two goals of this executive order, President Bush gave the Treasury Department the ability to freeze the assets of foreign and domestic organizations within the United States’ jurisdiction, including assets of financial institutions. This decision was motivated by his administration’s desire “to avoid not

24. John D.G. Waszak, The Obstacles to Suppressing Radical Islamic Terrorist Financing, 36 Case W. Res. J. Int’l L. 673, 675 (2004); see Caroline Drees, US Banks Struggle to Spot Terrorist Financing, Reuters, Mar. 9, 2004, available at http://www.forbes.com/business/newswire/2004/03/09/trt1291602.html (quoting an unidentified Bush administration official that “[u]nless you already know who the terrorists are, it’s hard to figure out what would be a distinguishing birthmark. . . . The only way so far that we can think of to identify terrorist financing is for the government to identify who the terrorists are.”).


27. See, e.g., Roth, Greenburg & Wille, supra note 17, at 45.


just criminal law but the judicial system altogether in its efforts to prevent the flow of funds.\textsuperscript{31}

One of the most infamous American initiatives to combat terrorism is Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT Act).\textsuperscript{32} Title III of the PATRIOT Act sets forth the regulations governing anti-terrorism financing.\textsuperscript{33} This Act revolutionized the United States’ ability to combat terrorist financing by strengthening the executive branch’s capacity to freeze and seize assets, broadening the President’s power under the IEEPA, and expanding the United States’ extraterritorial jurisdiction.\textsuperscript{34} These changes led David Aufhauser, the Treasury Department’s general counsel, to proclaim Title III of the PATRIOT Act “the smart bomb of terrorist financing.”\textsuperscript{35} Together, the PATRIOT Act and Executive Order 13,224 have ensured that the United States has achieved some success in its attempt to disrupt the flow of terrorist financing.\textsuperscript{36}

The PATRIOT Act and Executive Order 13,224 have also substantially increased the federal government’s power to require financial institutions to cooperate with law enforcement.\textsuperscript{37} The PATRIOT Act enables law enforcement to compel financial institutions to search their records in order to determine if they have had dealings with any individuals matching a certain generalized description.\textsuperscript{38} Those financial institutions refusing to cooperate with law enforcement face the possibility that the Treasury Department will freeze their assets under Executive Order 13,224.\textsuperscript{39} If a financial institution cooperates and finds a match, it must provide

\begin{itemize}
  \item \textsuperscript{31} Donohue, supra note 16, at 307.
  \item \textsuperscript{34} Donohue, supra note 16, at 371-72.
  \item \textsuperscript{35} Terrorism Hearing, supra note 33 (internal quotes omitted).
  \item \textsuperscript{36} See, e.g., Victor Mallet, Terrorists Funds “Being Squeezed,” FIN. TIMES (London), Apr. 11, 2002, at 12 (repeating then Secretary of Treasury Paul O’Neil’s assertion that the United States was victorious in its war on terrorist financing); Philip Shannon, 9/11 Panel Issues Poor Grades for Handling of Terror, N.Y. TIMES, Dec. 6, 2005, at A24 (noting the Treasury Department received the highest grade from the September 11 Public Disclosure Project).
  \item \textsuperscript{37} See, e.g., Donohue, supra note 16, at 372; 50 U.S.C. § 1861.
  \item \textsuperscript{38} Eric Gouvin, Are There Any Checks and Balances on the Government’s Power to Check Our Balances? The Fate of Financial Privacy in the War on Terrorism, 14 TEMP. POL. & CIV. RTS. L. REV. 517, 531 (2005).
  \item \textsuperscript{39} See, e.g., Donohue, supra note 16, at 372.
\end{itemize}
that individual’s name, account number, social security number, date of birth, or other unique identifying information to law enforcement.\footnote{31 C.F.R. \textsection 103.100(b)(2)(ii) (2004). If an institution fails to provide the requested information, it faces the prospect of criminal and civil penalties. \textit{See} Gouvin, supra note 38, at 530-34 (detailing the lack of oversight and transparency in the Patriot Act).} Under the PATRIOT Act, law enforcement can request information about an individual with only an administrative subpoena, and if it is investigating one of the 200 proscribed offenses, it can broadly disseminate any information it receives to other federal agencies.\footnote{41. \textit{Donohue, supra note 16, at 407. According to Michael Chertoff, the Director of Homeland Security, the PATRIOT Act authorizes the Attorney General and Secretary of the Treasury to obtain foreign bank records through administrative subpoenas. \textit{The Financial War on Terrorism and the Administration’s Implementation of the Anti-Money Laundering Provisions of the USA PATRIOT Act, Before S. Comm. on Banking, Housing and Urban Affairs, 107th Cong. (2002).}}}  

\textbf{B. The Development of the TFTP}

In 1973, a consortium of European financial institutions formed SWIFT to supply standardized messaging services and interface software to the global financial community.\footnote{42. \textit{See} \textit{About SWIFT, Company Information}, http://www.swift.com/index.cfm?item_id=1243 (last visited July 14, 2008); \textit{Simpson, supra note 1}.} Presently, thousands of financial institutions have an ownership interest in SWIFT.\footnote{43. \textit{See, e.g., About SWIFT, Company Information, supra note 42; \textit{Anita Ramasastry, The Treasury Department’s Secret Monitoring of International Fund Transfers: Why It Is Probably Legal, at Least in the U.S.}, FIND LAW, http://writ.news.findlaw.com/ramasastry/20060707.html (last visited Feb. 28, 2008). The National Bank of Belgium and the central banks of the G-10 countries are responsible for overseeing SWIFT’s business operations. Oversight of SWIFT, http://www.swift.com/index.cfm?item_id=57001 (last visited Mar. 5, 2008).} SWIFT is headquartered in La Hulpe, Belgium, a suburb of Brussels, but it has offices in at least sixteen countries.\footnote{44. \textit{Privacy Int'l, Pulling a SWIFT One? Bank Transfer Information Sent to U.S. Authorities 2 (2007).}} Approximately 8,000 financial institutions in 206 countries and territories currently utilize SWIFT’s messaging services.\footnote{45. \textit{See generally Lichtblau & Risen, supra note 1; SWIFT in Figures-SWIFTNET Fin Traffic, August 2006 YTD, available at http://www.swift.com/index.cgm?item_id=66437.}} It handles approximately 15 million transactions on a daily basis.\footnote{46. \textit{Simpson, supra note 1. In 2005, 1.6 billion out of the 2.5 billion messages SWIFT handled originated from Europe, while 467 million were from the United States. \textit{Id.}}} Two-thirds of the traffic on SWIFT’s messaging infrastructure originates in Europe.\footnote{47. \textit{Id.}} As a messaging institution, SWIFT does not handle money, but rather processes transfer instructions and confirmations for finan-
cial institutions. In an effort to explain SWIFT’s operations, the Belgian Data Privacy Commission analogized its services to a series of envelopes and letters. The envelopes contain information about the sending institution, the bank’s identifier code, the date and the time of the proposed transfer, and information about the other financial institution involved in the transaction. The letters are encrypted messages disclosing the amount to be transferred, the method of transfer, the identity of the parties to the transaction, and the participating financial institutions. The information sent over SWIFT’s network is stored for 124 days in both the United States and the Europe Union.

The TFTP is an integral component of a concerted effort by the American government to address a perceived intelligence deficiency in monitoring wire transfers. In attempting to address this intelligence gap, the Treasury Department’s Financial Crime Enforcement Network issued subpoenas to the New York branch of the Federal Reserve Bank in an effort to access FedWire, the Federal Reserve’s large dollar electronic transfer system. Two days after the September 11 attacks, First Data Corporation, the then parent company of Western Union, voluntarily offered federal law enforcement the use of their resources to combat terrorism. The Federal Bureau of Investigations (FBI) established an office in Omaha, Nebraska, in close proximity to the company’s

49. PRIVACY INT’I., supra note 3.
50. Id.
51. Id.
52. Belgian Data Protection Authority, supra note 7.
56. First Data is the world’s leading processing of credit card and debit card transactions. SUSKIND, supra note 13, at 38.
57. Western Union is the world’s leading wire-transfer service with over 12,000 offices around the world and controls thirteen percent of the market. See, e.g., id.; Virgil Larson, First Data Helped FBI After 9/11, OMAHA WORLD-HERALD, June 21, 2006, at A1.
58. See SUSKIND, supra note 13, at 209-12.
main processing center, converting First Data’s computers into the “FBI’s own in-house search engine.”

But the TFTP was not the first time the United States had attempted to access information within SWIFT’s databases. Prior to the September 11 attacks, the Treasury Department issued numerous subpoenas to SWIFT, which the company refused to honor because they were considered untimely or unduly burdensome. During President Clinton’s second term, the CIA was able to covertly access SWIFT’s network in its effort to locate Osama bin Laden. When the Treasury Department learned of this unauthorized access, it convinced the CIA to halt its activities because of the concern over potential backlash in the financial community if this access ever became public. Immediately following the September 11 terrorist attacks, the National Security Agency began to intercept wire transfers sent over the SWIFT network.

The event that was the impetus for TFTP was a conversation between a senior Bush-administration official and a Wall Street executive. The executive stoked the government official’s interest in pointing out the potential wealth of information contained within SWIFT’s databases. If the Bush administration could convince SWIFT to share their records with federal law-enforcement officials, the United States would potentially have access to billions of financial transactions that SWIFT processed and the information needed to facilitate those transactions. Further bolstering the Bush administration’s interest in pursuing the information within these records was the belief that SWIFT’s American CEO, Leonard Schrank, would be willing to assist the Treasury Department in its war against terrorist financing.

50. See id. at 38-39, 209-11. Once First Data grew skeptical of granting the FBI unfettered access to their records, the Director of the CIA George Tenet appealed to the patriotism of the company’s executives to ensure continued participation. Id. at 209-11.
51. Meyer & Miller, supra note 1.
52. Privacy Int’l., supra note 3.
53. Meyer & Miller, supra note 1.
54. Id.
56. Lichtblau & Risen, supra note 1.
57. Id. (noting a Bush administration official who described SWIFT’s databases as the “Rosetta stone of financial data”).
II. The Evolution of the TFTP

The Treasury Department has relied on administrative subpoenas in requesting information from SWIFT. An administrative subpoena does not require prior judicial authorization and only needs to meet a reasonableness standard instead of the typical probable-cause standard required for criminal subpoenas. The most important element in determining whether an administrative subpoena satisfies the four-part test set forth in United States v. Powell is the purpose of the investigation. The Treasury Department claims the legal justification for the TFTP is Executive Order 13,224's determination "that a need exists for further consultation and cooperation with, and sharing of information by, the United States and foreign financial institutions. . . to enable the United States to combat the financing of terrorism." Such an important justification would receive a great deal of deference from a court reviewing the reasonableness of a subpoena directed to SWIFT.

The Treasury Department issued its first subpoena to SWIFT in October 2001 and has subsequently issued at least sixty-three more subpoenas. The subpoenas sought information that SWIFT had previously transferred to its operating center in the United States. By seeking access to information that was already legally transferred to the United States, the federal government was attempting to ensure U.S. law (which provides lax protection for financial information compared to the European Union’s Data Privacy Directive) governed the TFTP.

These initial subpoenas issued by the Treasury Department sought any information within SWIFT’s possession that the United States deemed relevant in investigating terrorism. The subpoen-
nas issued by the Treasury Department, however, failed to set forth any specific individuals or particular transactions that the United States believed were connected to terrorism. The wide scope of these initial subpoenas eliminated the possibility of effective oversight. In 2003, SWIFT expressed reluctance to continue participating in a program that had no specific end date and lacked effective oversight.

SWIFT’s concerns led to a meeting among its executives, then–Federal Reserve chairman Alan Greenspan, and then–FBI director Robert Mueller to allay the company’s apprehensions. The Treasury Department, in response to SWIFT’s concerns, attempted to build sufficient safeguards into the TFTP to satisfy the company while maintaining the initiative’s efficacy. Concerns about maintaining the effectiveness of the TFTP was a paramount concern of Bush-administration officials because prior to SWIFT voicing its anxiety about participating in the TFTP, information received from the TFTP played an important role in capturing Hambali, the mastermind of the 2002 Bali bombings. Additionally, the TFTP played a vital role in prosecuting individuals for providing financial assistance to terrorist organizations.

The Treasury Department’s main concession to SWIFT was narrowing the definition of terrorism. In conjunction with a narrower definition of terrorism, the Treasury Department assured SWIFT that it would only investigate individuals linked to an ongoing terrorism investigation. To satisfy SWIFT that an individual is a terrorist suspect, the Treasury Department merely has to show

---

79. Privacy Int’l., supra note 3 (calling these subpoenas “carpet-sweepers”).
80. Lichtblau & Risen, supra note 1.
81. Id.
82. Lichtblau & Risen, supra note 1.
84. See, e.g., Lichtblau & Risen, supra note 1; Ramasastry, supra note 43.
85. See, e.g., Levey Hearing, supra note 28; Lichtblau & Risen, supra note 1 (discussing the case of Uzair Parcha, a Brooklyn resident, who was convicted of attempting to launder $200,000 for Al Qaeda).
86. Privacy Int’l., supra note 3. The original definition stated that any person “who constitutes a risk of violence against Americans, American property, and U.S. and foreign interests” was a terrorist. The Treasury Department modified the definition of terrorism to encompass activities which “involv[e] a violent or dangerous act that threatens human life, property, or infrastructure; and has the goal of intimidating or threatening the civilian population; influencing the actions of government through mass destruction, kidnapping, intimidation or hostage taking.” This definition mirrors the one provided in 18 U.S.C. § 2331(1).
87. Privacy Int’l., supra note 3. However, under the Supreme Court’s plain view doctrine, if the Treasury Department discovers evidence of other criminal activity in SWIFT’s
that the United States has placed the individual on a terrorist watch list. In an effort to ensure that the Treasury Department followed these safeguards, the U.S. government and SWIFT agreed to hire Booz Allen Hamilton, an American consulting firm, to oversee the operations of the TFTP. Additionally, the Treasury Department emphasized TFTP’s inability to monitor routine financial transactions, such as using an ATM or debit card, as a further limitation on the program. The only reason, however, the Treasury Department cannot access these financial transactions is because it does not utilize SWIFT’s messaging network.

To access the information provided by SWIFT, the Treasury Department has to go through a multi-step process. Initially, SWIFT transfers information from its operating center in Europe to its storage facility in the United States. The Treasury Department then sends a subpoena to SWIFT’s facility in the United States. The information provided in response to the subpoena is placed inside a “black box.” To view the information in the “black box,” the Treasury Department designed a software program that enables it to search SWIFT’s data for either suspicious transactions or participants in financial transactions who were suspected terrorists. Furthermore, the Treasury Department cannot perform searches in real time, as a lag exists between when SWIFT receives a subpoena and when it transfers the information. Furthermore, SWIFT retains the ability to prevent any searches they consider to be of dubious validity.


90. Levey Hearing, supra note 28. Strict controls have been put in place, and auditors have discovered one instance of an analyst running an improper search. Id.

91. Id.

92. Id.

93. PRIVACY INT’L, supra note 3.

94. Id.

95. Id.

96. Id.

97. Id. The FBI and the Treasury Department are using the information obtained from SWIFT to assist in building a comprehensive terrorist database. Lichtblau & Risen, supra note 1.

98. PRIVACY INT’L, supra note 3.

99. Id.
These extensive safeguards were still considered insufficient to provide appropriate safeguards for protecting individual privacy by many within the European Union.100 The outrage expressed by many Europeans was greater than the limited media attention and criticisms directed at the TFTP in the United States.101 Many journalists assumed the strong negative European reaction to the TFTP was the product of resentment towards the Bush administration’s policies in the war on terror.102 This explanation only partially accounts, however, for the strong reaction towards the TFTP because it fails to recognize that failing to protect an individual’s data privacy rights within the European Union is seen as a failure “to respect the fundamental rights of citizens.”103

III. Evaluating the TFTP Under the European Union’s Data Privacy Directive

A. The Fundamentals of the Data Privacy Directive

The European Union explicitly recognizes privacy as a fundamental human right.104 The Data Privacy Directive, adopted in 1995, and which took effect shortly thereafter,105 embraces this view of privacy.106 The European Union enacted a comprehensive legislative scheme to govern data privacy because it believed the


102. See Risen, supra note 9 (singling out the operation of secret CIA prisons in Eastern Europe and the process of extra- rendition).

103. Fred Cate, Privacy in the Information Age 42 (1997) (quoting Spiros Simitis, Unpublished Address on Information Privacy and the Public Interest (Oct. 6, 1994)).


105. EU Directive, supra note 6, art. 32(1).

Commentators claim that the motivation for viewing data privacy as a fundamental right originates from the Continent’s memory of Nazi Germany and other totalitarian regimes that used personal information to identify individuals as members of disfavored groups and then persecute them. The Data Privacy Directive was enacted to promote two sometimes conflicting objectives: first, protecting an individual’s right to privacy in their private data and second, to promote the free flow of information amongst member states of the European Union. The real concern of the Data Privacy Directive is to prohibit selling consumer preferences and profiles to companies.

The Data Privacy Directive contains eight core principles: purpose limitation, data quality, data security, sensitive data, transparency, data transfer, independent oversight, and individual redress. These principles are designed to ensure that an individual has the ability to control his or her “public image.” These core principles were developed in an effort to protect an individual against the media—who may publicize unpleasant or distorted details about his or her life. Professor James Whitman is quick to point out that this threat to an individual’s right to “informational self-determination” is not limited to the media but extends to “[a]ny other agent that gathers and disseminates information.” Thus, the Data Privacy Directive is an attempt to empower an individual with the tools necessary to regulate what personal information is disseminated to the public.

107. Id. at 85 (detailing why data privacy is a public good).
109. EU Directive, supra note 6, art. 1.
110. James Q. Whitman, The Two Western Cultures of Privacy: Dignity Versus Liberty, 113 YALE L.J. 1131, 1192-93 (noting that Europeans see consumers as “need[ing] more than cheap goods and services”).
111. Cate, supra note 11, at 185-86. Underlying these eight core concept is the proportionality principle, which requires “the government’s legitimate interference with privacy be proportional.” Bignami, supra note 14, at 642.
113. Id.
114. Id.
115. Id.
The Data Privacy Directive “covers all private sector processing of personal data.” However, the Data Privacy Directive does not apply to transfers undertaken for public or state security. In fact, the European Court of Justice invalidated an agreement between the United States and the Council of the European Union that provided for direct transfer of trans-Atlantic passenger information from airlines to the Department of Homeland Security because the Data Privacy Directive did not cover the activity. However, the structure of the TFTP (where SWIFT transfers information to its storage center in the United States, and only thereafter does the Treasury Department subpoena the information) keeps the program within the purview of the Data Privacy Directive.

Viewing data privacy as a fundamental right has led the European Union to attempt to impose this view on other countries in order to ensure that the protections afforded under its Data Privacy Directive cannot be circumvented. Under the Data Privacy Directive, the European Commission has the ability to prohibit data transfers to non-E.U. countries who fail to provide “an adequate level of protection” for an individual’s personal data. The United States’ approach to protecting personal data fails to provide an adequate level of protection. In an effort to prevent the European Union from effectively imposing an information blockade, the Department of Commerce and the European Commission agreed upon regulations, known as the “Safe Harbor Principles,” which govern how the Data Privacy Directive applies to American countries.

\[\text{Shaffer, supra note 106, at 13.}\]
\[\text{See EU Directive, supra note 6, art. 3(2) (providing a list of limited activities to which the Data Privacy Directive does not apply).}\]
\[\text{See Shaffer, supra note 106, at 85.}\]
\[\text{EU Directive, supra note 6, art. 25. Article 25(2) provides that the determination of whether a third party country provides a sufficient level of protection “shall be assessed in light of all the circumstances surrounding a data transfer operation or set of data transfer operations particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.” Id.; see Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive (July 24, 1998), available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_en.pdf.}\]
businesses. American financial institutions, however, cannot avail themselves of the protection afforded by the Safe Harbor Principles because they apply only to industries regulated by the Department of Commerce.

B. The Article 29 Working Party Evaluates the TFTP

The Data Privacy Directive established the Article 29 Working Party. The Article 29 Working Party is responsible for examining the effectiveness of the Data Privacy Directive in protecting “the rights and freedoms of natural persons with regard to the processing of personal data.” The findings of the Article 29 Working Party are only advisory in nature; however, they are accorded substantial deference in determining the European Union’s position.

In evaluating the TFTP, the Article 29 Working Party reached three distinct conclusions about the legality of the program. It concluded that SWIFT’s decision to store information in the United States violated the Data Privacy Directive. It also determined that the TFTP was invalid under the Data Privacy Directive. The third, and perhaps most controversial, conclusion was that any financial institution utilizing SWIFT’s services, after the public disclosure of the TFTP, had violated the Data Privacy Directive. In response to these findings, the European Data Protection supervisor informed the European Central Bank that it had until April 2007 to bring SWIFT into compliance with the Data Privacy Directive.

123. George et al., supra note 122. There are seven Safe Harbor Principles which a company must comply with (1) notice; (2) choice; (3) onward transfer; (4) security; (5) data integrity; (6) access; and (7) enforcement. U.S. Dep’t of Commerce, Safe Harbor Workbook, available at http://www.export.gov/safeharbor/sh_workbook.html (last visited Mar. 2, 2007).
125. See EU Directive, supra note 6, art. 29.
126. Id. art. 30(1)(c).
129. Id.
130. Id.
131. Id. at 12-13 (finding that the presence of representatives of financial institutions on SWIFT’s board of directors should have enabled the institutions to have a significant input into SWIFT’s decision to cooperate with the United States).
Under Article 26 of the Data Privacy Directive, personal information can be transferred to a third-party country without adequate protections for an individual’s private information if the transfer falls within one of six safe harbor provisions. The only safe-harbor provision with the potential to legitimize SWIFT’s transfer of data under the TFTP was that “the transfer is necessary or legally required on important public interest grounds...” In previously interpreting this safe harbor, the Article 29 Working Party indicated that this provision must be strictly interpreted, stressing that a simple public interest was insufficient. This gloss was an attempt to ensure that third-party countries could not easily avoid the strictures of the Data Privacy Directive.

The Article 29 Working Party also concluded that SWIFT’s transfer of data to its operating center in the United States and the subsequent transfer to the Treasury Department failed to serve a crucial public interest. This conclusion built upon a decision issued by the German Constitutional Court in April 2006, which showed some apprehension about whether the possibility of future terrorist attacks were sufficient to justify antiterrorism data mining. Although the TFTP was an innovation in combating terrorist financing and has been instrumental in helping to thwart terrorist plots, the Article 29 Working Party felt that it was a luxury given the existing international mechanisms to combat terrorist financing. Furthermore, the Article 29 Working Party also

133. EU Directive, supra note 6, art. 26(1). The six safe harbor provisions are: the data subject has consented to the transfer, the transfer is essential to protect vital interests of a data subject, the transfer is necessary for the performance of a contract between the data subject and the financial institution, the transfer is necessary to fulfill a contract between the financial institution and a third party, the transfer is necessitated by an important public interest, and the transfer is made from a register which is intended to provide information to the public and which is open to consultation by the public. Id. art. 26(1)(a)-(f).
134. Id. art. 26(1)(d).
135. Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, supra note 121, at 25.
136. See Shaffer, supra note 106, at 5.
137. Article 29 Data Protection Working Party, supra note 7, at 24-25.
138. Bundesverfassungsgericht [BVerfG], Apr. 4, 2006, 1 BVerfGE para. 158 (requiring evidence indicating an “imminent and specific endangerment” of a terrorist attack to justify antiterrorism data mining).
139. See Lichtblau & Risen, supra note 1.
140. Article 29 Data Protection Working Party, supra note 7, at 25. The International Convention for the Suppression of the Financing of Terrorism made it a criminal offense to provide or collect money with the knowledge that the funds would be used in the commission of terrorist offenses. International Convention for the Suppression of the Financing of Terrorism, Dec. 9, 1999, 39 I.L.M. 270 (2000). In 1989, the G7 established the Financial Action Task Force to establish an international legal regime to combat money laundering. The Financial Action Task Force’s mandate was expanded after the Septem-
examined SWIFT’s interest in having two information storage centers to guarantee operational efficiency. Although the Working Party recognized the need for dual storage centers, it found that SWIFT’s interests could still be served by storing the information in a country with a data privacy regulation regime approved by the European Union.

Data transfer and mining occurring under the TFTP would have still been permissible if these activities were undertaken to further a legitimate interest of the United States or SWIFT, and the interests being pursued outweighed an individual’s right to be protected from unwanted intrusions into his or her private life. The report of the Article 29 Working Group recognized that the United States has a legitimate interest in combating terrorism. The Article 29 Working Party concluded, however, that the large amount of data being clandestinely transferred to the Treasury Department was indicative of a program that significantly invaded the privacy rights of individuals. Further supporting this conclusion was SWIFT’s failure to inform financial institutions, their customers, and the appropriate national data privacy commissioners about the company’s participation in the TFTP. Also, underlying these concerns was the belief that antiterrorism data mining relied heavily on a stereotypical terrorist profile.

Article 6 of the Directive specifies that personal information can only be processed for a specified purpose, utilized in accordance with the original reason why an individual released the data, and retained for no longer than necessary to fulfill that original purpose. The Article 29 Working Party concluded that the TFTP was simply incongruous with these limitations of the Data Privacy Directive. The data transferred to the Treasury Department from SWIFT was information necessary to facilitate and complete
2008] The Terrorist Finance Tracking Program 571

financial transactions. The United States’ mining of SWIFT’s data to identify terrorists violates the purpose limitation, because the information is not being used to further the original purpose for which the information was originally released—to complete a financial transaction. Furthermore, long-term retention of the information transferred by SWIFT to the Treasury Department is problematic because the information may become inaccurate over time.

For SWIFT processing and transferring personal data in conjunction with the TFTP to be considered lawful, its activities needed to fulfill one of the conditions set forth in Article 7 of the Data Privacy Directive. Under Article 7, the best justification for SWIFT’s activities was that its participation in the TFTP was necessary to comply with the company’s legal obligations. Because SWIFT has an operations center in the United States, it was subject to the United States’ legal requirements and was thus required to respond to the compulsory subpoenas issued by the Treasury Department. In evaluating the implementation of whistle-blowing schemes mandated by Sarbanes-Oxley, the Article 29 Working Party concluded that “an obligation imposed by a foreign legal statute or regulation . . . may not qualify as a legal obligation by virtue of which data processing in the EU would be made legitimate.” Therefore, under the Article 29 Working Party’s prece-
dent, SWIFT’s obligation to respond to the Treasury Department’s subpoenas was insufficient to satisfy the requirements of the Data Privacy Directive.\textsuperscript{158} At the conclusion of its report, the Article 29 Working Party set forth a series of ideas to help to ensure SWIFT’s compliance with the Data Privacy Directive.\textsuperscript{159}

The June 2007 agreement between the European Union and the Bush administration provides that the Treasury Department will attempt to respect the Data Privacy Directive, retain information it receives from SWIFT for a maximum of five years, and strictly limit the use of the TFTP to investigating terrorism.\textsuperscript{160} The European Union will compel financial institutions that utilize SWIFT’s messaging services and that are within its jurisdiction to inform their customers of the United States’ ability to access the personal data in that institution’s possession, and appoint an individual to assure the Treasury Department honors these safeguards.\textsuperscript{161}

But as demonstrated in the controversy over the transfer of airline passenger information to the U.S. Customs and Border Protection Agency, such ad hoc agreements have been viewed skeptically within the European Union.\textsuperscript{162} This skepticism is a product of viewing data privacy as a fundamental right which cannot be “bargain[ed] about.”\textsuperscript{163} Such absolutism, however, is misplaced and dangerous because it both fails to allow for the necessary flexibility to address the substantial challenges that have arisen since the Data Privacy Directive’s enactment as well as overlooks the myriad of circumstances in which a person’s interest in their personal information are implicated.\textsuperscript{164}

\begin{footnotesize}
\begin{itemize}
\item Accounting Controls, Auditing Matters, Fight Against Bribery, Banking, and Financial Crime (Feb. 1, 2006) at 8. The motivating factor behind this ruling is concern that these external legal obligations would be used a pretext to evade the strictures of the Data Privacy Directive. \textit{Id.}
\item 158. Article 29 Data Protection Working Party, \textit{supra} note 7, at 18-19.
\item 159. \textit{Id.} at 28-29 (stressing the need for the eleven central banks overseeing SWIFT to clarify their role and for financial institutions which use SWIFT’s messaging service to inform clients that their information may be accessed by the United States).
\item 160. Risen, \textit{supra} note 9.
\item 161. \textit{Id.}
\item 163. \textit{Fred Cate, Privacy in the Information Age:} 42 (1997) (quoting Spiros Simitis, Unpublished Address on Information Privacy and the Public Interest (Oct. 6, 1994)).
\item 164. \textit{See} Shaffer, \textit{supra} note 106, at 20 (detailing equity and efficiency concerns that arise from making data privacy a fundamental right).
\end{itemize}
\end{footnotesize}
IV. The Failings of the Data Privacy Directive

A country possesses the greatest authority to infringe upon its citizens’ civil liberties during wartime. But controversy often arises when the government attempts to achieve the appropriate balance between protecting civil liberties and ensuring the safety of the populace. The United States’ experience has shown that measures sacrificing civil liberties during times of war—most notably the internment of Japanese-Americans during World War II—are often unjustified or insufficiently tailored to meet a particular crisis. In evaluating these measures, critics are afforded the opportunity to review the government’s conduct after the crisis has passed and no further attacks have occurred. The United States has not been alone in curtailing civil liberties after the September 11 terrorist attacks. The European Union has also attempted to restrict the protection of civil liberties afforded the citizens of its member states.

The Data Privacy Directive is also engaged in a balancing act, attempting to protect the privacy rights of individuals while allowing for a seamless stream of information. By balancing the wrong interests, the Data Privacy Directive and those regulations

165. See, e.g., Haig v. Agee, 453 U.S. 280, 307 (1981) (stating it is “obvious and unarguable that no governmental interest is more compelling than the security of the Nation”) (internal quotations omitted); WILLIAM H. REHNQUIST, ALL THE LAWS BUT ONE: CIVIL LIBERTIES IN WARTIME 218 (2000).


168. See Duncan v. Kahanamoku, 327 U.S. 304, 351 (1946) (Burton, J., dissenting) (accusing the majority of using the hindsight of 1946 to overturn the convictions of civilians by military tribunals in Hawaii while the territory was under military rule).

169. See Gross, supra note 166, at 77-88.

170. See, e.g., Council Directive 2006/24 2006 O.J. (L105) 54 (EC) arts. 4, 6 (requiring companies which provide electronic communication services to retain data relating to phone calls, emails, and other communications for up to two years and make the information available to the national police). The motivation behind this Council Directive was to provide law enforcement with the information needed to combat terrorism. Id. art. 1.

171. See, e.g., Loring, supra note 124, at 432; Shaffer, supra note 106, at 20 (listing the interests the Data Privacy Directive balances against data privacy).
modeled after it are hindrances in the war on terror and impediments to global economic development.\textsuperscript{172}

President Bush has commented that the September 11 terrorist attacks “changed everything.”\textsuperscript{173} As demonstrated by Executive Order 13,224 and the PATRIOT Act, Americans have been willing to give the government the allegedly necessary tools for law enforcement to protect the populace against another terrorist attack.\textsuperscript{174} The European Union, however, has been unwilling to embrace extensive anti-terrorist monitoring initiatives for fear of infringing on an individual’s right to data privacy.\textsuperscript{175} In protecting information voluntarily shared with a third party, the Data Privacy Directive should emulate the level of protection afforded in the United States.\textsuperscript{176} This deferential approach is justified for programs like the TFTP, which represent only limited intrusions into an individual’s privacy and provide sufficient operational safeguards to ensure the initiative is not mismanaged.

A. The United States’ Approach to Voluntarily Conveyed Data

The safeguards that the U.S. Constitution affords to individual data privacy are sufficiently malleable to adapt to varying circumstances.\textsuperscript{177} Under the Fourth Amendment,\textsuperscript{178} a search occurs

\begin{itemize}
\item \textsuperscript{172} See Shaffer, supra note 106, at 17-20 (explaining the impact the Data Privacy Directive has on businesses and the deleterious impact it has on efficiency).
\item \textsuperscript{174} See James X. Dempsey & Lara M. Flint, Commercial Data and National Security, 72 Geo. Wash. L. Rev. 1459, 1477-82 (2004) (detailing the changes wrought by the USA PATRIOT Act to federal data privacy legislation).
\item \textsuperscript{175} Whitman, supra note 110, at 1160-62.
\item \textsuperscript{176} Some may disagree with the conclusion that the sharing of information with a financial institution is not a private event because the privacy law of the European Union intends to shield individuals from public indignity. Whitman, supra note 110, at 1160-62. However, providing the full panoply of protection under the Data Privacy Directive is inappropriate for information that is voluntarily disclosed.
\item \textsuperscript{177} See Orin Kerr, Four Modes of Fourth Amendment Protection, 60 Stan. L. Rev. 503, 507 (2007). U.S. law is especially relevant to the dilemma faced by companies in a situation comparable to that faced by SWIFT because multinational businesses have a connection to the United States and thus provides a basis for the United States to seek to apply its laws. See Bignami, supra note 14, at 674 (detailing the economic leverage the United States has exerted in the controversy over the TFTP and the transfer of airline passenger data).
\item \textsuperscript{178} The Fourth Amendment states “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the places to be searched, and the persons or things to be seized.” U.S. Const. amend. IV.
\end{itemize}
when the government intrudes on a person’s “reasonable expectation of privacy.” To determine whether an individual has a “reasonable expectation of privacy,” an individual must have a subjective expectation of privacy in the information and society must recognize such expectation as reasonable. The Supreme Court has concluded that an individual does not have a reasonable expectation of privacy in information that he or she “voluntarily conveys” to a third party. Thus, in United States v. Miller, the Supreme Court held that financial information conveyed to a bank did not qualify for Fourth Amendment protection.

Two years after the Supreme Court’s decision in Miller, Congress passed the Right to Financial Privacy Act (RFPA) in an effort to provide some privacy protections to customers of financial institutions. The RFPA typically requires the government to obtain a customer’s consent prior to accessing an individual’s financial records. Under the RFPA no notice is needed, however, if an individual’s financial records are “sought for foreign counter intelligence purposes to protect against international terrorism or clandestine intelligence activities.”

Under the United States’ legal regime, administrative officials have defended the program on the belief that the TFTP did not infringe on the privacy of financial customers. In a lawsuit filed in the U.S. District Court for the Northern District of Illinois, Chief Judge James F. Holderman denied SWIFT’s motion to dismiss the

180. See id. at 361-62.
181. See Miller, 425 U.S. at 443. Commentators have concluded there is no distinction between information that is given directly to the government and the government “mining” data provided to computer databases. See, e.g., Chris Jay Hoofnagle, Big Brother’s Little Helpers: How Choicepoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement, 29 N.C.J. INT’L & COM. REG. 595, 622 (2004); Daniel J. Solove, Digital Dossiers and the Dissipation of Fourth Amendment Privacy, 75 S. CAL. L. REV. 1083, 1137-38 (2002).
182. Miller, 425 U.S. at 442-43 (finding the defendant by utilizing the bank’s services assumed “the risk . . . the information will be conveyed to the government”).
185. Id. § 3414(a)(5)(A).
case, finding that the plaintiffs’ allegations could proceed without ruling on the merits.\textsuperscript{187} When reviewing the voluntary conveyance of information to an institution for the purpose of initiating financial transactions, courts have found that customers assume the risk that the information could be used for purposes inimical to the owner’s intentions.\textsuperscript{188} In \textit{Walker v. S.W.I.F.T. SCRL}, the court found this principle inapplicable because unrestricted access to individuals’ bank records through a secret government initiative operating outside the legal system is constitutionally problematic.\textsuperscript{189} The opinion in \textit{Walker} significantly downplays the fact that SWIFT released information only in response to subpoenas from the Treasury Department\textsuperscript{190} and that SWIFT had the ability to challenge the validity of these subpoenas in federal court.\textsuperscript{191}

The United States has given law enforcement great latitude to pursue those that finance terrorism.\textsuperscript{192} In an effort to ensure financial institutions cooperate with law enforcement, Executive Order 13,224 provides the Treasury Department with the option of freezing a company’s assets.\textsuperscript{193} Thus, it would appear foolish for a company to try to resist cooperating with the United States in the war on terror because of concerns about violating the legal rights of their customers.\textsuperscript{194} While some may be wary of this power of persuasion, it provides a meaningful tool for the United States to

\textsuperscript{187} Walker v. S.W.I.F.T. SCRL, 491 F. Supp. 2d 781, 790-92 (N.D. Ill. 2007). The case was subsequently transferred to the Eastern District Virginia and SWIFT has brought a motion for a reconsideration of Judge Holderman’s ruling. Lichtblau, supra note 186.

\textsuperscript{188} See Miller, 425 U.S. at 443.

\textsuperscript{189} Walker, 491 F. Supp. 2d at 790-91. The Court found the Fourth Amendment applied to SWIFT even though a private actor because of the allegation that SWIFT had turned over all of its record to the Treasury Department in response to the subpoenas it received. \textit{Id.} A recent decision from the U.S. District Court for the Southern District of New York addressing a legal challenge to the TFTP dismissed the case because the plaintiff lacked standing. Amidax Trading Group v. S.W.I.F.T. SCRL, No. 08 Civ. 5689(PKC), 2009 WL 361949, at *1 (S.D.N.Y. Feb. 13, 2009).

\textsuperscript{190} SWIFT Statement on Compliance Policy, http://www.swift.com/index.cfm?item_id=59897 (June 23, 2006) (“In the aftermath of the September 11th attacks, SWIFT responded to compulsory subpoenas for limited sets of data . . .”).

\textsuperscript{191} See United States v. Bailey, 228 F.3d 341, 348 (4th Cir. 2000) (holding that an administrative subpoena initiates the adversarial process thereby allowing a court to review the subpoena before the party that received the subpoena is penalized for noncompliance).

\textsuperscript{192} See Donohue, supra note 16, at 372-75.

\textsuperscript{193} Id. at 377-78.

\textsuperscript{194} See Ramasastry, supra note 43, at 3.
guarantee that a corporation will cooperate in a program that the United States deems relevant to its national security.\footnote{195}

In the United States, the PATRIOT Act and Executive Order 13,224 have tipped the balance between law enforcement and civil liberties firmly in the direction of law enforcement.\footnote{196} Both conservatives and liberals have criticized the PATRIOT Act as an unjustified intrusion into the private lives of Americans.\footnote{197} Advocating that the European Union adopt the United States’ approach to data privacy protection does not require member states to embrace legislation like the PATRIOT Act.\footnote{198} Instead, it requires the European Union to weaken the protection it affords certain information voluntarily shared with a third party, which would not undermine the Data Privacy Directive’s concern for protecting an individual’s right to “informational self-determination.”\footnote{199}

**B. The Inconsistencies of Applying the Data Privacy Directive to the TFTP**

The right of an individual to control publicly available information about themselves must have limits.\footnote{200} If an individual has an unfettered right to control the information disclosed to the public, it would inhibit the ability of the government to carry out many of its core functions.\footnote{201} Although the Data Privacy Directive recognizes the importance of these core governmental functions, European courts and advocates of privacy downplay their importance by

\footnote{195. SWIFT’s participation in the TFTP despite concerns about violating the Data Privacy Directive and Belgian law shows how powerful this leverage can be. See Bignami, supra note 14, at 674.}

\footnote{196. See, e.g., Gouvin, supra note 38, at 540-41; Gross, supra note 166, at 73.}

\footnote{197. Amy Borus, When Right and Left See Eye-to-Eye, Bus. Wk., Nov. 5, 2001, at 88.}

\footnote{198. On October 2, 2001, the European Commission proposed a regulation allowing funds of suspected terrorists to be frozen and denying access of the financial system to suspected terrorists. In order to fulfill this obligation, member nations of the European Union were provided with the authority to make financial institutions to provide any relevant information. Proposal for a Council Regulation on Specific Restrictive Measures Directed Against Certain Persons and Entities with a View to Combating Terrorism, COM (01)569, art. 12.}

\footnote{199. Whitman, supra note 110, at 1161.}

\footnote{200. See Richard Posner, The Right to Privacy, 12 Ga. L. Rev. 393, 399 (1978) (“Much of the demand for privacy . . . concerns discreditable information concerning past or present criminal activity or moral conduct at variance with a person’s professed moral standards. And often the motive for concealment is . . . to mislead those with whom he transacts.”).}

\footnote{201. The Data Privacy Directive recognizes that a right to control a person’s publicly available information is often inconsistent with a Country’s security concerns and thus tends to exempt the processing of personal data for “public security, defense, State security . . . and the activities of the State in areas of criminal law.” EU Directive, supra note 6, art. 3(2).}
employ[ing] a fundamental rights discourse . . . to enhance the relative importance of their concerns.”202 This undervaluation, coupled with an emphasis on the potential deleterious consequences of governmental information gathering203 indicates that absent specific information identifying a specific target and date, the government’s ability to combat terrorism could be significantly curtailed. Such stringent restrictions are inappropriate for antiterrorism programs like the TFTP, which contain comprehensive safeguards and seek information a person has voluntarily shared with others.

The information that the Treasury Department accesses from SWIFT is simple factual data, such as a person’s name or date of birth, which people routinely reveal to governmental agencies, credit card providers, and websites.204 It seems arbitrary to afford protection to some voluntary conversations, such as a conversation with a bank teller to complete a financial transaction, but not to impose similar restrictions on conversations with friends.205 Recognizing this untenable position, the European Council and Parliament now requires all lawyers, accountants, and notaries to inform law-enforcement authorities of suspicious financial transactions.206

The member nations of the European Union have a valid concern that foreign jurisdictions may not provide the same level of protection afforded by the Data Privacy Directive.207 Nevertheless, this concern, which was a factor behind the adoption of the Data Privacy Directive,208 should not apply to the U.S. government when it is asking for information to combat terrorism. Terrorism threat-

202. Shaffer, supra note 106, at 21. See Bundesverfassungsgericht [BVerfG], Apr. 4, 2006, 1 BVerfge, para. 158 (applying German privacy law to police data mining and concluding due to the importance of data privacy such police activity was only acceptable if law enforcement had facts to demonstrate an “imminent and specific endangerment of a terrorist attack”).

203. See, e.g., Bignami, supra note 14, at 637-38.

204. See, e.g., Levey Hearing, supra note 28; Christopher Slobogin, Transaction Surveillance, 75 Miss. L. Rev. 139 (2005). The Data Privacy Directive imposes added safeguards when the information may reveal an individual’s political opinions, religious beliefs, race, ethnicity, and sexual preferences. EU Directive, supra note 6, art. 8.

205. Contra Miller, 425 U.S. at 451 (Brennan, J., dissenting) (claiming that communicating information with a bank is not voluntary because it is a prerequisite to participating in modern society).


207. Loring, supra note 124, at 435.

208. Id.
ens both the United States and the European Union. Thus, a mutual interest exists in exchanging intelligence that may help to prevent a terrorist attack. The European Union should not have concerned itself with the activities of the TFTP because the restraint of the Treasury Department in conducting searches, combined with the important national security interests served by the TFTP as well as the extensive safeguards that were in place prior to June 2007 to satisfy SWIFT, mitigates such concerns.

The steps the Treasury Department must go through before accessing the information transferred from SWIFT ensure an individual’s privacy is respected. Requiring the Treasury Department to limit its searches to ongoing terrorism investigations and providing SWIFT with the opportunity to object to any search helps minimize the risk of false positives and sharpens the focus of an investigation. These two features combine to make the TFTP superior to the European Union’s decision to rely on the accountants, notaries, and lawyers to protect the integrity of its financial system. As demonstrated by the United States’ experience—requiring financial institutions to file Suspicious Activity Reports for questionable transactions—this approach leads to law enforcement being inundated with information about individuals that have no connection to terrorism because of concerns about being subjected to liability.

The United States’ desire to protect itself against terrorist attacks is a weighty interest that should override the protection afforded by the Data Privacy Directive to factual information that was voluntarily conveyed to a third-party. The need to “starve the ter-


210. There has only been one instance of an improper search being conducted. Lichtblau & Risen, supra note 1. Furthermore, there has been independent oversight of the TFTP. See id.


212. See Lichtblau, supra note 8.

213. See Statement of Treasury Secretary John W. Snow on Disclosure of the Terrorist Finance Tracking Program, supra note 211.

214. See, e.g., PRIVACY INST’l., supra note 3; Levy Hearing, supra note 28.

215. See, e.g., Donohue, supra note 16, at 374; Gouvin, supra note 38, at 527 (noting both Rush Limbaugh and Senator Bob Dole were investigated for money laundering).

216. Many claim the September 11 terrorist attacks and the War on Terror have created a threat “to the national and constitutional survival of the United States.” See Michael
rorists of funding” has been a central focus of the war on terror, as indicated by legislation adopted in the United States and the international community. The information SWIFT provides to the Treasury Department should be indistinguishable from the information member nations of the European Union can require to be turned over to law enforcement under European Parliament and Council Directive 2001/97/EC. Thus, the conflict over the TFTP is a product of the European Union viewing itself as the “privacy cop of the world” and the United States being unwilling to provide detailed evidence supporting its suspicions of terrorist activity.

The feelings of distrust between the European Union and the United States influenced the Article 29 Working Party’s recommendations on the TFTP and the implementation of the requirements of Sarbanes-Oxley in the affiliates of American business located in Europe. The Article 29 Working Party itself manifested a distrust of the United States when its report claimed that the TFTP enabled the Treasury Department to access any information held by SWIFT. This characterization misrepresents the Treasury Department and SWIFT safeguards, which only allow access to the information related to an ongoing terrorism investigation. E.U. attempts to force the United States to terminate the TFTP embody a refusal to acknowledge that “terrorism has made our world an integrated community.”


217. U.S. Dep’t of the Treasury, supra note 54.

218. See, e.g., Donohue, supra note 16, at 382-89 (detailing various regional and multilateral efforts to combat terrorist financing); U.S. Dep’t of the Treasury, supra note 54.

219. See Directive 2001/97/EC OJ 2001 L344/76 art. 6 (requiring the affected profession to provide national law enforcement “with all necessary information. . . .”). If an accountant notices a suspicious transaction while auditing financial information he or she would conceivably provide factual information like the person’s name, the date of the transaction, the amount involved, and the individual’s address to the police. See id.


221. Donohue, supra note 16, at 381 (noting the obstacle which has prevented the United States from securing the assistance of its allies in the financial war on terror is its reluctance to provide evidence because of a fear of compromising sources and intelligence gathering activities).

222. See Article 29 Data Protection Working Party, supra note 7.

223. See id. at 6 (expressing concern that the TFTP was subterfuge for the United States to engage in economic and industrial espionage).

224. Privacy Int’l, supra note 3.

V. Conclusion

In evaluating any initiative that seeks to combat terrorism, it is important to strike an appropriate balance between protecting civil liberties and providing law enforcement with sufficient resources to combat terrorism. The TFTP is an example of an initiative that can accommodate these competing interests. The responses of the members of the European Parliament to the disclosure of the TFTP, however, demonstrate an unwillingness to compromise their commitment to data privacy protection.

As countries model their data privacy regulations on the Data Privacy Directive, they must be aware of the limitations inherent in the European Union’s approach. The Data Privacy Directive was drafted in a world that was largely ignorant of the failures of globalization. If countries blindly copy the Data Privacy Directive to ensure that the European Union cannot halt the flow of information to their country, they are enshrining economic protectionism by overprotecting an individual’s privacy in financial information voluntarily transmitted to third parties. This economic protectionism, besides having a deleterious economic impact, is preventing the United States from having access to the necessary tools to fight the war on terror.

In a globalizing world, the Article 29 Working Party’s decision that a foreign subpoena cannot serve as a legal justification under the Data Privacy Directive is untenable. This decision places multinational companies in difficult situations; they face potential liability for complying with the subpoena under the European Union’s legal regime, whereas failing to comply with the subpoena subjects the company to liability in the United States. A company placed in such a situation will attempt to avoid liability by trying to partially accommodate both the United States and the European
Union. Such an approach, however, will not satisfy either the European Union, as demonstrated by SWIFT’s participation in the TFTP,\(^{232}\) or the Bush administration, which does not look kindly upon what it considers undue restraints on its ability to fight terrorism.\(^{233}\)

The Data Privacy Directive represents the E.U. member states’ judgment that the legislation struck the appropriate balance between the competing interests of data privacy and the need for information.\(^{234}\) However, the world is more dangerous today than it was in the mid-1990s when the debate surrounding the Data Privacy Directive occurred. The United States has been able to use its economic influence to reach agreements with the European Union on the TFTP and the transfer customer information on transatlantic flights.\(^{235}\) Such agreements, which may take considerable time to negotiate, leave companies exposed to liability for assisting the United States in locating terrorists. Additionally, the liability resulting from these agreements probably hampers the willingness of other corporations to cooperate. The United States should attempt to use its market power, through the North American Free Trade Agreement or the World Trade Organization, to convince the European Union to lessen the protection afforded information voluntarily transmitted to a third-party, and to be more receptive to the transfer of that information abroad—especially when the information is helpful in combating terrorism.

---

232. See Bilefsky, supra note 100.
234. Loring, supra note 124, at 432.
235. Bignami, supra note 14, at 674.