2003

Bringing Out the Big Guns: The USA PATRIOT Act, Money Laundering, and the War on Terrorism

Eric J. Gouvin
Western New England University School of Law, egouvin@law.wne.edu

Recommended Citation
55 Baylor L. Rev. 955 (2003)

BRINGING OUT THE BIG GUNS: THE USA PATRIOT ACT, MONEY LAUNDERING, AND THE WAR ON TERRORISM

Eric J. Gouvin*

TABLE OF CONTENTS

I. INTRODUCTION

Imagine the following scenario.[1] The most powerful democratic nation in the world is going about its daily business in troubled times without

---

*Professor of Law, Western New England College School of Law, Springfield, Massachusetts. The author thanks Larry Cunningham and Patricia McCoy for their comments on an earlier draft of this paper. The author also thanks Robyn Carollo for her excellent research assistance. This Article is an elaboration of a presentation given at Western New England College School of Law on the Legal Responses to Terrorism, September 20, 2002.

[1]This introductory material is inspired by a column written by Jared Diamond not long after

immediate concern for homeland safety. Its major city, arguably the world capital of finance and culture, bustles with activity. The citizens of that nation and that city feel reasonably secure, protected by oceans from the tumult in other, less stable, places.

Now imagine that city is subjected to a surprise terrorist attack. Without warning comes a shocking attack completely outside the norms of human behavior. Fanatics send airborne bombs smashing into landmarks, striking fear into the hearts of the populace.

This was the scene in London, England 1940.[2] The terrorists were the Nazis launching aerial attacks into civilian targets in densely populated areas. The German attacks were not consistent with the existing law of war. They were not tactical strikes designed to knock out key facilities or to disrupt the British war effort. Instead, the bombs were tossed willy-nilly into populated areas for the primary purpose of terrorizing the citizenry and demoralizing the nation. The attacks were so unconventional that we might legitimately classify them as acts of terrorism.

---

the events of September 11, 2001. *See* Jared Diamond, *Keeping Panic at Bay*, N.Y. TIMES, Oct. 21, 2001, § 4, at 15.

[2]The complacency of England in the years leading up to World War II is captured by George Orwell in the closing paragraph of his account of the Spanish Civil War, *Homage to Catalonia.* As the narrator returns home after seeing the fighting in Spain, the book concludes:

> And then England—southern England, probably the sleekest landscape in the world. It is difficult when you pass that way, especially when you are peacefully recovering from sea-sickness with the plush cushions of a boat-train carriage under your bum, to believe that anything is really happening anywhere. Earthquakes in Japan, famines in China, revolutions in Mexico? Don't worry, the milk will be on the doorstep tomorrow morning, the *New Statesman* will come out on Friday. The industrial towns were far away, a smudge of smoke and misery hidden by the curve of the earth's surface. Down here it was still the England I had known in my childhood: the railway-cuttings smothered in wild flowers, the deep meadows where the great shining horses browse and meditate, the slow-moving streams bordered by willows, the green bosoms of the elms, the larkspurs in the cottage gardens; and then the huge peaceful wilderness of outer London, the barges on the miry river, the familiar streets, the posters telling of cricket matches and Royal weddings, the men in bowler hats, the pigeons in Trafalgar Square, the red buses, the blue policemen—all sleeping the deep, deep sleep of England, from which I sometimes fear that we shall never wake till we are jerked out of it by the roar of bombs.

GEORGE ORWELL, HOMAGE TO CATALONIA 231–32 (Harcourt, Brace & World, Inc. 1952) (1938).

Why did the Nazis wage a terrorist war? They did so for the same reason terror has been a part of warfare since the dawn of humankind—terrorist tactics often work.[3] As part of a military strategy, terrorism adds a psychological warfare component to the rest of the attack. The terrorist hopes the target population will panic and become its own worst enemy. When a terrorist act generates a sufficiently terrified response from the target population, the members of that population can be crippled by fear; their society may even self-destruct as fear disrupts normal interactions and leads to the abandonment of long-held societal norms based on trust and security. Therefore, in light of the way terrorism works, the most effective counter-terrorist act is for the target's political leadership to shore up public confidence and help prevent the population from panicking. In times of terrorist attack, leaders must remind their citizens of their deep collective resolve to see the crisis through.

This is exactly what the British did in 1940. Winston Churchill repeatedly addressed the people in terms designed to steel the nation's resolve.[4] To back up the Prime Minister's words with action, the British deployed a number of highly visible and very noisy anti-aircraft guns around London and near the English Channel. Although military experts knew the big guns had a very low chance of actually intercepting the German aerial campaign, they also intuitively understood that the terrorist strategy is most effective in demoralizing a population when it appears that the target's government is incapable of responding to protect its people against the threat.[5]

This is how terrorist warfare works. Like the terrorist attack itself, the countermeasures against terrorism have a psychological value far out of proportion to their effectiveness. During the Battle of Britain, the people of England did not self-destruct because their leaders' response to the psychological warfare was on target. Their implacable Prime Minister kept

---

[3]*See* ALAN M. DERSHOWITZ, WHY TERRORISM WORKS: UNDERSTANDING THE THREAT, RESPONDING TO THE CHALLENGE 6 (Yale Univ. Press 2002) (providing a perspective on how terrorist acts by the Palestine Liberation Organization (PLO) have been quite effective in promoting the Palestinian cause); Brad E. O'Neill, *The Strategic Context of Insurgent Terrorism*, *in* TERRORISM & POLITICAL VIOLENCE: LIMITS & POSSIBILITIES OF LEGAL CONTROL 77 (Henry H. Han ed., 1993) (discussing various strategic considerations in terrorism).

[4]For example, in his first statement to the House of Commons as Prime Minister on May 13, 1940, Churchill stated, "Victory at all costs, victory in spite of all terror, victory however long and hard the road may be; for without victory there is no survival." BARTLETT'S FAMILIAR QUOTATIONS 620 (Justin Kaplan ed., Little Brown & Co., 16th ed. 1992).

[5]*See* Diamond, *supra* note 1.

a brave face, and the noisy, visible anti-aircraft guns stood in bold defiance of the German air attack.

Fast forward to September 11, 2001. Again fanatics sent airborne bombs smashing into landmarks in the largest cities of the most powerful nation on Earth in violation of the norms of human behavior and the laws of war.[6] The destruction of the World Trade Center towers and the attack on the Pentagon had a huge psychological effect on the United States. As reprehensible, cold-blooded, and inhumane as these terrorist acts were, they were brilliant strategic moves. The attacks had the capacity to terrify the most important cities in the world. They almost succeeded, but the people of New York and Washington did not buckle; instead they rallied.

Like Churchill before them, key government officials—President Bush, Governor Pataki, and Mayor Giuliani—knew they had to be highly visible and reassuring.[7] They discharged that duty admirably. The approval ratings of all three shot skyward. Yet lurking in the back of people's minds in the immediate aftermath of the attacks was a keen sense of helplessness and vulnerability. The political leaders knew that if left unaddressed, the terrorists could exploit those thoughts of vulnerability for further disruption of the social order.

Knowing the lessons of previous terror campaigns, after September 11 the government had to act to show the people the United States was not entirely helpless against the terrorist threat. Bringing the terrorists "to justice" would have been an excellent way to make that demonstration. Unfortunately, fighting the human combatants in a terrorist war is extraordinarily difficult. Although the United States did eventually take military action, neither Mullah Mohamed nor Osama bin Laden have been captured. In the psychological war, military action alone would not give

---

[6]For a general analysis of the question of whether the acts of September 11 were "acts of war," see Derek Jinks, *September 11 and the Laws of War*, 28 YALE J. INT'L L. 1 (2003); Noah Feldman, *Choices of Law, Choices of War*, 25 HARV. J.L. & PUB. POL'Y 457 (2002).

[7]Following Churchill's example, if not his oratorical style, President Bush rallied the people through highly visible photo ops. For example, on September 14, 2001, just three days after the attack, President Bush visited Ground Zero to address the men and women aiding in the rescue. He stood aboard a fire truck accompanied by dirty and tired firefighters, emergency servicemen and construction workers. One of the construction workers yelled out: "We can't hear you." And the President, raising his bullhorn, yelled: "Well, I can hear you; the whole world hears you. And pretty soon those evildoers will be hearing from us." *See* Press Release, Office of the Press Secretary, President Receives World Trade Center Bullhorn, Remarks by the President During Presentation of World Trade Center Bullhorn, The Oval Office (Feb. 25, 2002), *available at* http://www.whitehouse.gov/news/releases/2002/02/20020225-4.html.

the kind of reassurance required to keep our citizens on a solid psychological footing.

The government needed to open new fronts in the "War on Terrorism" to assure the people that something could be done to stop the terrorists. In the month following September 11, the government took dramatic action, such as cracking down on immigration and rounding up terrorism suspects without full attention to civil rights. In addition, perhaps to show that it could do something, the government ratcheted-up the money laundering rules to make terrorist financing more difficult.

President Bush responded on September 24, 2001, less than two weeks after the attack, with Executive Order 13,224 to freeze the assets of and prohibit transactions with persons who commit, threaten to commit, or support terrorism.[8] The order also picked up a very nebulous group of persons who are "otherwise associated" with any designated terrorist.[9] The White House maintained that the order gave the Treasury Department power to "block the U.S. assets of, and deny access to U.S. markets to, foreign banks who refuse . . . to freeze terrorist assets."[10] Such a sweeping power is an unconventional position, because as a matter of international law the idea of "guilt by association" seems at odds with the notion that nationals of neutral countries have the right to maintain commercial relations with the belligerents in a war.[11]

The United States soon rallied international support for tougher world-wide money laundering standards. The G-7 finance ministers agreed on September 25, 2001[12] to pursue a comprehensive strategy to disrupt terrorist financing and implemented an action plan on October 6, 2001.[13] At a meeting on October 29 and 30, 2001, the Financial Action Task Force (FATF), an international intergovernmental anti-money laundering body

---

[8]*See generally* Exec. Order No. 13,224, 66 Fed. Reg. 49,079 (Sept. 25, 2001) (hereinafter "E.O. 13224").

[9]*Id.* § 1(d)(ii).

[10]Press Release, The White House Office of the Press Secretary, Fact Sheet: Executive Order on Terrorist Financing (Sep. 24, 2001), *available at* http://usinfo.state.gov/topical/pol/terror/01092413.htm.

[11]Mark Kantor, *The War on Terrorism and the End of Banking Neutrality*, 118 BANKING L. J. 891, 895 (2001).

[12]*Statement of G7 Ministers of Finance* (Sep. 25, 2001), *available at* http://www.g7.utoronto.ca/finance/fm010925.htm.

[13]*Statement of G7 Finance Ministers and Central Bank Governors* (Oct. 6, 2001), *available at* http://www.g7toronto.ca/finance/fm100601.htm.

associated with the G-7, agreed to develop special guidance for financial institutions to help detect the techniques and mechanisms of terrorist financing.[14]

On the home front, efforts to dry up the sources of terrorist financing culminated in the passage of the USA PATRIOT Act[15] (Patriot Act). The law's title is an almost Orwellian acronym for "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism."[16] Title III of the Patriot Act is the International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001.[17] Although it appeared to be a response to the terrorist attacks, the proposed law was not new. Precursors of the various components of the Patriot Act, including the money laundering provisions, had been floating around Congress for years prior to September 11, 2001.[18] Concerned about reports that the federal approach to terrorism was fragmented across several agencies with little coordination, and that intelligence and law enforcement agencies had inadequate resources, Congress held hearings on enhanced money laundering rules prior to 2001. Proponents of the legislation did not make the case for its passage. Largely due to civil liberties concerns, Congress did not pass legislation to resolve the problems that would

---

[14]Press Release, Organization for Economic Co-Operation and Development, FATF Leads International Effort to Combat Terrorist Financing (Oct. 9, 2003), *available at* http://www.oecd.org.

[15]Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107–56, 115 Stat. 272 (2001) (codified as amended in scattered sections of 12, 15, 18, and 31 U.S.C.) [hereinafter USAPA].

[16]A reporter for the Financial Times characterized the Patriot Act as being "coercively" named. Patti Waldmeir, *Inside Track: Unaccustomed Warriors: A New Law in the United States Will Draft Thousands of Businesses into the Fight Against Terrorism*, FIN. TIMES, Mar. 21, 2002, at 17.

[17]There have been several excellent summaries of the provisions in Title III of the Patriot Act. See, for example, Paul Schott Stevens & Thomas C. Bogle, *Patriotic Acts: Financial Institutions, Money Laundering and the War Against Terrorism*, 21 ANN. REV. BANKING L. 261 (2002); Todd Stern et al., *The Money Laundering Abatement and Anti-Terrorist Financing Act of 2001*, 119 BANKING L.J. 1 (2002).

[18]For example, H.R. 3886 was a bipartisan proposal before the House Banking and Financial Services Committee in June of 2000. *See generally* International Counter-Money Laundering Act of 2000, H.R. 3886, 106th Cong. (2000). The legislation would give the Secretary of Treasury additional tools to root out international money laundering havens, used to funnel dirty money into the legitimate international financial network. It was defeated. Press Release, James A. Leach, Chairman, Committee on Banking and Financial Services, Opening Statement on Markup of HR 3886 (June 8, 2000), *available at* http: //financialservices.house.gov/banking/6800lea.htm.

ultimately be addressed in the Patriot Act.[19] The events of September 11, however, provided a convenient justification for the passage of the law.

The Patriot Act was enacted with remarkably little deliberation. The huge anti-terrorism package, covering 350 different subject areas and forty different agencies, was pushed through Congress in less than a month. The law was hammered out in private negotiations between the Justice Department and party leaders; there were no final hearings to allow dissenters a voice in the process, no committee reports, no conference committee, and indeed, most members of Congress did not even have the opportunity to read the legislation.[20]

Just one Senator, Russell Feingold of Wisconsin, and only sixty-six representatives voted against the Act.[21] While the 342 page Act passed overwhelmingly, representatives across the political spectrum had grave concerns about the potential abuse of power and loss of privacy.[22] President Bush signed the legislation into law on October 26, 2001, less than six weeks after the September 11 attacks. Shortly thereafter, news reports giving dollar figures for terrorist assets seized domestically and around the world began appearing in various media outlets, suggesting the battle against terrorism being waged by the financial services industry was being won by the United States.[23]

---

[19]Jake Taper, *Don't Blame it on Reno*, (Jan 2, 2002), *available at* http://www.archive.salon.com/politics/feature/2002/01/02/reno.

[20]Robert A. Levy, *The USA Patriot Act: We Deserve Better*, *available at* http://www.cato.org/current/terrorism/pubs/levy-martial-law.html. The accelerated timetable of five weeks bypassed the committee process and floor debate. Proponents of the legislation claimed the streamlined adoption process was necessary to prevent future attacks feared to be imminent. *See Homeland Defense: Hearing Before the Senate Comm. on the Judiciary*, 107th Cong. (Sept. 24, 2001), *available at* www.house.gov/judiciary/75288.pdf, at 15. The overall hazy understanding of what was being pushed through Congress was aggravated by the fact that many lawmakers and their staffs were preoccupied with the anthrax contamination in congressional offices, many Congressman not able to return to their offices, and therefore, had less or no time to consider the legislation fully. *See* Gia Fenoglio, *Jumping the Gun on Terrorism?*, 33 NAT'L J. 3450 (2001), *available at* 2001 WL 25926351.

[21]Robert E. Pierre, *Wisconsin Senator Emerges as a Maverick; Feingold, Who Did Not Back Anti-Terrorism Bill, Says He Just Votes His Conscience*, WASH. POST, Oct. 27, 2001, at A8.

[22]Amy Borus, *When Right and Left See Eye-to-Eye*, BUS. WK., Nov. 5, 2001, at 88 (noting that the opponents of the Patriot Act included ultra-conservative Rep. Bob Barr and ultra-liberal Rep. Barney Frank).

[23]*See, e.g.*, Glenn R. Simpson, *U.S. Says al Qaeda Has Begun to Feel Financial Squeeze*, WALL ST. J., Nov. 15, 2001, at A28.

This Article addresses the question of whether the money laundering provisions in the Patriot Act will be effective tools in the effort to intercept terrorist financing to prevent future attacks like those suffered on September 11, 2001, or whether the legislation is instead the modern equivalent of a big noisy anti-aircraft gun—psychologically useful for showing that something is being done, but not very effective in actually doing the task. This Article concludes that the Act's money laundering provisions will not be effective in intercepting terrorist financing. It reaches that conclusion after examining the current state of United States money laundering regulation, the changes wrought by the Patriot Act, and the realities of terrorist financing.

II. A BRIEF HISTORY OF AMERICAN MONEY LAUNDERING LAW

Money laundering is nothing new.[24] Our financial and legal systems have been wrestling with the problem of dirty money for ages. Over the past thirty years or so we have been trying to find the right balance between legitimate expectations to financial privacy and legitimate law enforcement access to financial records.

While money laundering is nothing new, the September 11 attacks put a new twist on the problem. Our anti-money laundering laws have been primarily geared toward tracing the proceeds of crime—to stop the drug dealer or the mob boss from making ill-gotten gains look legitimate. In the new war against terrorism, however, we expect our money laundering regime to do something very different—to intercept the financing of criminal acts. Even with the Patriot Act in place, our financial system is not set up to handle this new task. To appreciate why, a brief review of existing money laundering legislation is in order.

---

[24]Money laundering has been defined as "the process by which one conceals the existence, illegal source, or illegal application of income, and disguises that income to make it appear legitimate." It has become a virtual requirement for large organized crime groups to engage in money laundering, because it is the sustaining force that enables drug dealers, terrorist groups and other organized crime units to hide substantial amounts of wealth and to perpetuate further criminal activity. Kelly Neal Carpenter, *Eighth Survey of White Collar Crime: Money Laundering*, 30 AM. CRIM. L. REV. 813, 814 (1993).

A. The Bank Secrecy Act

The first serious anti-money laundering statute enacted by the federal government was the Bank Secrecy Act[25] (BSA), which was passed in 1970. The BSA requires banks and other "financial institutions"[26] to keep certain records and authorizes the Secretary of the Treasury to require such institutions and persons participating in transactions for such institutions to report financial transactions to the Secretary.[27] The stated policy rationale for the record-keeping requirements of the BSA is that "such records and reports are of a high degree of usefulness in criminal, tax, and other regulatory investigations."[28]

The regulations implementing the BSA require covered financial institutions to report each deposit, withdrawal, exchange of currency, or other payment or transfer that involves a transaction in currency of more than $10,000.[29] The legislation also requires regulated institutions to: (1) establish internal controls to ensure compliance with the BSA; 2) monitor the implementation of compliance procedures; 3) designate one or more individuals as responsible for supervising day-to-day compliance; and 4) provide training for personnel.[30]

It is fair to say that bankers have never much liked the BSA and for good reason. Compliance with the law is very technical and detailed. The paperwork requirements on banks can be quite burdensome, especially for small institutions. Moreover, the failure to accurately report a currency transaction is a strict liability offense which can lead to forfeiture of funds even if the error was inadvertent.[31] The Treasury Department can require officials of depository institutions to appear personally, to produce records and to testify under oath in connection with a money laundering or compliance investigation.[32]

---

[25]12 U.S.C. §§ 1829(b), 1951–1959 (2003); 31 U.S.C. §§ 5311–5322 (2003).

[26]31 U.S.C. § 5312(a)(2) (defining "financial institution" to include, among other things, banks and depository institutions, casinos and card clubs, broker-dealers and investment companies).

[27]*Id.* § 5313(a).

[28]12 U.S.C. § 1829b(a)(1); 31 U.S.C. § 5311.

[29]The regulations promulgated by the Department of Treasury under the Bank Secrecy Act are found at 31 C.F.R. § 103.22(b)(1) (2002).

[30]31 U.S.C. § 5318(h)(1); 12 C.F.R. § 21.21(c) (2003) (describing minimum requirements for BSA programs at national banks).

[31]31 U.S.C. § 5321(a)(3)

[32]*Id.* § 5318(a)(4).

In addition to the regulation's burdensome compliance requirements, bankers soon suspected that the law would be ineffectual in stopping dirty money from going through the legitimate banking system. As a general proposition, a substantial percentage of crooks who have more than $10,000 in cash to deposit are clever people; they quickly learned to make small deposits. The increased regulatory scrutiny of large cash transactions, resulted in money launderers breaking up their deposits into several transactions in amounts less than $10,000. This technique of BSA avoidance became known as "smurfing."[33] Banks are now required to institute compliance procedures to aggregate transactions in order to detect and prevent smurfing.[34]

The development of smurfing made regulators face up to the fact that a bright line rule based on an arbitrary dollar amount could never be effective in smoking out criminal activities. This realization led to a change in money laundering regulation designed to make bankers detect "suspicious" activities. If a transaction is suspicious it must be reported if, in the aggregate, $5,000 in funds or other assets is involved.[35]

While coverage under the BSA was far-reaching, it was far from universal. Some financial intermediaries were subject to it, but others were not. Not all intermediaries that were subject to the BSA were subject to the same requirements. For instance, Western Union was required to report all transactions over $3000, but unlike banks, was not required to maintain records and tracking data.

Again, criminals with large amounts of cash to move are not, generally speaking, stupid. In time, cash transfer services like MoneyGram and Western Union became favorite tools of terrorists.[36] These networks move cash very quickly, and users liked the relative informality—no account to set up and minimal ID requirements.[37] The Patriot Act has, however,

---

[33]*See* Bill Atkinson, *Treasury Asks Mandatory System To Tighten Laundering Detection,* AM. BANKER, Sept. 7, 1990, at 2 (noting the use of the term). One smurfing technique is the "starburst." In a starburst, tainted money on account in a bank is sent out in random, small chunks to other accounts all over the world. Tracking it all down wears down investigators, who must contend with many different jurisdictions to trace small amounts of money. *Getting to them through their money*, ECONOMIST, Sept. 29, 2001, at 67.

[34]31 U.S.C. § 5324.

[35]31 C.F.R. § 103.18(a)(2).

[36]*See* Heather Timmons, *Terrorist Money by Wire*, BUS. WK., Nov. 5, 2001, at 94.

[37]*See* Heather Timmons, *Western Union: Where the Money is—in Small Bills*, BUS. WK., Nov. 26, 2001, at 40.

changed the attractiveness of non-bank money transfers. In what was clearly a shot across the bow of the entire industry, New York's banking regulators brought charges against Western Union alleging violations of state and federal currency transaction reporting laws.[38] The parties settled the action with Western Union paying a fine of $8 million without admitting any wrongdoing.[39]

B. Right to Financial Privacy Act

When it was first enacted, the BSA created quite a stir. United States banking customers were not used to the idea that their banks might be required to tell the government about certain transactions in which they engaged. Indeed, the BSA was challenged as an unconstitutional invasion of privacy. Ultimately, the United States Supreme Court declared that the BSA was constitutional because there was no reasonable expectation of privacy in the bank-customer relationship with regard to information required by the government.[40]

To counteract some of the invasive aspects of the BSA, however, Congress passed the Right to Financial Privacy Act of 1978 (Privacy Act).[41] The Privacy Act provides broad coverage for financial privacy, but that protection is subject to many exceptions. In general, the Privacy Act prohibits disclosure of an individual[42] customer's records by a financial institution to a government authority without the customer's consent.[43]

---

[38]Paul Beckett & Carrick Mollenkamp, *In Wake of Sept. 11, Regulators Crack Down on Money-Transfer Industry,* WALL ST. J., Dec. 28, 2001, at A9.

[39]Paul Beckett & Carrick Mollenkamp, *Western Union Tripped by Patriot Act,* WALL ST. J., Dec. 20, 2002, at A3.

[40]*See* United States v. Miller, 425 U.S. 435, 443–45 (1976) (holding there is no Fourth Amendment expectation of privacy in a person's bank records when a government agency has an interest in examining those records); Cal. Bankers Ass'n v. Schultz, 416 U.S. 21, 45–54 (1974) (holding the Bank Secrecy Act's recordkeeping and reporting requirements do not deprive financial institutions of due process, nor does the implementation of the BSA constitute an illegal search and seizure in violation of the Fourth Amendment).

[41]Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, tit. XI §§ 1101–1121, 92 Stat. 3697 (1978) (codified at 12 U.S.C. §§ 3401–3422).

[42]The law protects individuals and partnerships consisting of five or fewer individuals but does not extend to corporations. 12 U.S.C. § 3401(4) (2003).

[43]*Id.* § 3402(1). Among other exceptions, the Act does not prohibit disclosure in the following situations: (1) where the financial information is not individually identifiable; (2) where the financial institution itself is being investigated; and (3) where the disclosure is in accordance with Internal Revenue Code provisions or other federal statutes or rules. *Id.* § 3413.

While the Privacy Act makes clear that the government does not have unfettered access to customer bank accounts, it provides that a customer may authorize disclosure of financial records to a government authority, subject to revocation.[44] Despite the broad protection afforded by the Privacy Act, the government may obtain disclosure without the customer's consent pursuant to an administrative subpoena, a search warrant, a judicial subpoena and, in certain circumstances, a formal written request.[45]

The Privacy Act attempted to rein in a bit of the invasiveness of the BSA without completely hobbling law enforcement interests. Therefore, a customer is ordinarily entitled to notice before disclosure to a government authority.[46] In addition, the customer has the right to challenge the disclosure.[47] The notice to the customer may, however, be delayed pursuant to court order if such notice would result in the customer fleeing from prosecution, the destruction of evidence, the intimidation of potential witnesses, or would seriously jeopardize an investigation or proceeding.[48] Special procedures govern certain intelligence activities,[49] and we might expect those provisions to be invoked more frequently in the war against terrorism.

C. The 1980s

With the BSA and the Privacy Act in place by the end of the 1970s, the cornerstones of the United States scheme were settled and the battle between legitimate interests in privacy versus legitimate law enforcement interests was framed. The money laundering reporting scheme received some fine tuning in the 1980s as policy makers perceived that some transactions of legitimate interest to law enforcement might be falling through the cracks. The Money Laundering Control Act of 1986[50]

---

[44]*Id.* § 3404(a)(2).

[45]*Id.* § 3402(2)–(5).

[46]*Id.* § 3408(4).

[47]*Id.* § 3410 (containing the exclusive judicial challenges available to object to the disclosure of financial records).

[48]*Id.* § 3409.

[49]*Id.* § 3414.

[50]Money Laundering Control Act of 1986, Pub. L. No. 99-570, 100 Stat. 3207-18 (1986) (codified as amended in scattered sections of 18 and 31 U.S.C.).

established money laundering as a crime, making the United States one of the first countries in the world to criminalize the practice.[51]

In 1988 Congress passed the Money Laundering Prosecution Improvements Act.[52] The main thrust of this law was to expand the reach of the BSA by broadening the definition of "financial institution."[53] It also introduced the innovation of giving Treasury the power to target the nation's money laundering compliance program by requiring additional reporting obligations for certain geographic areas.[54]

D. The 1990s

Congress tinkered with the federal money laundering scheme several times during the 1990s. In 1992, Congress passed the Annunzio-Wylie Anti-Money Laundering Act,[55] (Annunzio-Wylie Act) which further bolstered the requirements of the BSA. This law required the filing of "Suspicious Activity Reports" (SARs) that were "relevant to a possible violation of law or regulation."[56] SARs were an attempt to fine tune the money laundering reporting system in light of the fact that a bright line dollar amount rule or even a requirement to pick up smurfing sometimes left suspicious transactions unreported.

The unintended consequence of the increased reporting schemes was the generation of large numbers of extraneous reports. The flood of useless reports was hardly surprising given the incentives to over-report that are built into the law. The BSA imposed strict liability for failure to file appropriate reports.[57] The institutions subject to the BSA took that threat of

---

[51]*See* Steven & Bogle, *supra* note 17, at 263. The crime of money laundering includes the practice of structuring transactions in order to evade BSA reporting requirements and generally prohibits the participation by a financial institution in a financial transaction with knowledge the funds involved are derived from an unlawful activity.

[52]Money Laundering Prosecution Improvements Act of 1988, Pub. L. No. 100-690, 102 Stat. 4354 (1988) (codified in various sections of 18 and 31 U.S.C.).

[53]31 U.S.C. § 5312(a)(2) (2003).

[54]*Id.* § 5326(a).

[55]Annunzio-Wylie Anti-Money Laundering Act, 102 Pub. L. No. 550, 106 Stat. 4044 (1992) (codified in various sections of 12, 18, 31 and 42 U.S.C.).

[56]31 U.S.C. § 5318(g)(1).

[57]*Id.* § 5321(a)(3). *See* United States v. Bank of New England, 821 F.2d 844, 855–57 (1st Cir. 1987) (ruling that the bank had the requisite mental state if it deliberately avoided learning CTR requirements).

liability very seriously. On the other hand, there was no liability attached to filing extraneous reports in good faith.[58] Indeed, the Annunzio-Wylie Act contained a provision holding reporting entities free from liability in connection with the filing of suspicious activity reports.[59] The Patriot Act also gives reporting institutions the same protection.[60]

In the midst of a rising tide of paperwork, Congress passed the Money Laundering Suppression Act of 1994,[61] which chiefly served to suppress the number of Currency Transaction Reports (CTRs) being filed. The Money Launering Suppression Act had a short-term effect, reducing the number of reports filed for a short while, but the effects were not long-lasting.[62] Today, the combined money laundering rules generate vast oceans of reports, leaving the government officials responsible for reviewing those reports drowning in data.

The Financial Crimes Enforcement Network (FinCEN), a unit of the Treasury, estimates that thirty percent of the twelve million currency transaction reports it received in 2001 were filed unnecessarily.[63] In a statement issued in September 2002, FinCEN said it was going to study the CTR and SAR systems to find ways to reduce the number of unnecessary

---

[58]*See* Brown v. Nationsbank Corp., 188 F.3d 579, 589 (5th Cir. 1999) ("If private businesses were not eligible for immunity from state law claims arising from assisting undercover federal operations, this would provide a major disincentive to assisting law enforcement and would undermine the needs and interests of the federal government."); Lopez v. First Union Nat'l Bank of Fla., 129 F.3d 1186, 1192 (11th Cir. 1997).

[59]"[Persons reporting suspicious activity] . . . shall not be liable to any person under any law or regulation of the United States . . . or . . . of any State . . . for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure. . . ." 31 U.S.C. § 5318(g)(3)(A) (2003). *See* Stoutt v. Banco Popular de P. R., 320 F.3d 26, 31–33 (1st Cir. 2003) (upholding summary judgment in favor of bank that filed SAR in connection with a customer who allegedly obtained funds under fraudulent pretenses on the grounds that the safe harbor of 31 U.S.C. § 5318(g)(3) protects the bank).

[60]USAPA § 351 (codified as amended in 31 U.S.C. § 5318(g)(3) (2003)).

[61]Money Laundering Suppression Act of 1994, Pub. L. No. 103-325, 108 Stat. 2243 (1994)(codified in scattered sections of 31 U.S.C.).

[62]One of the problems with the Act was that it did not provide a procedure to determine the legitimacy of offshore bank customer transactions. Several recent legislative efforts have been directed at this area of concern. *See, e.g.*, Money Laundering and Financial Crimes Strategy Act of 1998, Pub. L. No. 105-310, 112 Stat. 2941, 2942–47 (1998) (codified in 31 U.S.C. §§ 5341–42, 5351–52 (2000)).

[63]Rob Garver & Michele Heller, *In Brief: FinCEN Seeks Streamlined Filing Process*, AM. BANKER, Sept. 5, 2002, at 3 (quoting FinCEN press release).

reports.[64] The concern with over-reporting goes beyond worrying about the innocent trees that have given their lives in vain and extends to the very heart of the reporting regime. According to the FinCEN press release, "These millions of excess forms have little value for law enforcement purposes and, we believe, impose substantial compliance costs upon financial institutions. . . . Also, excess filings burden our intelligence analysis and impede timely targeting of money laundering, terrorist financing, and other vulnerable transactions."[65]

This admission by FinCEN calls the whole BSA-style approach to money laundering into doubt. With the Patriot Act beefing up the reporting requirements and thereby generating even more CTRs and SARs, could the reporting system be paralyzed by an overload of, mostly useless, information?[66]

The last noteworthy anti-money laundering initiative from the 1990s was the notorious "Know Your Customer" proposal. In December 1998, the federal banking agencies jointly proposed rules that would have really required banks to monitor customer activity.[67] In a sense, the regulators were looking to deputize financial institutions to snoop on customers in order to figure out who should be watched closely. The 1998 Know Your Customer proposal would have required financial institutions to determine the customer's identity, identify the source of customer funds, determine the customer's "normal and expected" transactions, monitor accounts for transactions that were not consistent with those expectations, and determine whether such transactions were unusual or suspicious.[68] In response to the proposed rules, the federal banking regulators received a flood of comment letters, most of which opposed the rules. The proposed rules were

---

[64] *Id.*

[65] *Id.*

[66] FinCEN has recently developed an electronic filing system, the Patriot Act Communication System (PACS), that will reduce the paperwork involved in the filing of CTRs and SARs but will do nothing to reduce the flow of extraneous information. For information about the PACS, see *PACS Homepage*, *available at* http://pacs.treas.gov/index.jsp (last visited Sept. 12, 2003).

[67] Membership of State Banking Institutions in the Federal Reserve System; International Banking Operations; Bank Holding Companies and Change in Bank Control, 63 Fed. Reg. 67,516 (proposed Dec. 7, 1998) (codified at 12 C.F.R. pts. 208, 211, 225); "Know Your Customer" Requirements, 63 Fed. Reg. 67,524 (proposed Dec. 7, 1998) (codified at 12 C.F.R. pt. 21) (OCC); Minimum Security Devices and Procedures and Bank Secrecy Act Compliance, 63 Fed. Reg. 67,529 (proposed Dec. 7, 1998) (codified at 12 C.F.R. pt. 326); Know Your Customer, 63 Fed. Reg. 67,536 (proposed Dec. 7, 1998) (codified at 12 C.F.R. pt. 563).

[68] Know Your Customer, 63 Fed. Reg. 67,536 (Dec. 7, 1998) (codified at 12 C.F.R. pt. 563).

withdrawn in March of 1999.[69] That was the last major initiative on money laundering before the terrorist attacks of September 11, 2001.[70]

III. THE USA PATRIOT ACT'S IMPACT ON MONEY LAUNDERING

The Patriot Act contains extensive provisions designed to improve the government's anti-money laundering efforts. The Act not only strengthens the existing BSA system by expanding the types of financial institutions covered, but it also vests in the Treasury broad new powers to examine financial institutions and prohibit suspect accounts. It extends the reach of the BSA to, among others, credit unions, futures commission merchants, commodity trading advisors, and commodity pool operators.[71]

One of the major innovations brought about by the Patriot Act is the implementation of a new version of the "Know Your Client" standards. The Patriot Act directs the Secretary of Treasury to promulgate regulations establishing standards for financial institutions regarding the identity of customers opening accounts.[72] The new Patriot Act regulations require, among other things, that financial institutions implement reasonable procedures for: (1) verifying the identity of any person seeking to open an account, to the extent reasonable and practicable; (2) maintaining records of the information used to verify the person's identity, including name, address, and other identifying information; and (3) determining whether the

---

[69]The FDIC received 254,394 comments with the "overwhelming majority" strongly opposed to the proposed standards. 64 Fed. Reg. 14,845 (Mar. 29, 1999) (codified at 12 C.F.R. pt. 326).

[70]Despite all of the anti-money laundering provisions of United States law, money laundering activity has reached astounding levels. By some estimates, it is the world's third largest industry by value. Current estimates are that $500 billion to $1 trillion in criminal proceeds are laundered through banks worldwide each year, one-half of that amount moved through domestic financial institutions. *See* MINORITY STAFF OF PERMANENT SUBCOMMITTE ON INVESTIGATIONIS, 106TH CONG., REPORT ON PRIVATE BANKING AND MONEY LAUNDERING: A CASE STUDY OF OPPORTUNITIES AND VULNERABILITIES, *available at* http://www.govaffairs.senate.gov/; *see also* Bill Steel, *Billy's Money Laundering Information Website*, *available at* www.laundryman.u-net.com/printversion/homepage.html (last visited Sept. 8, 2003).

[71]USAPA § 321 (codified as amended in 31 U.S.C. § 5312(a)(2) (2003)) (amending the existing definition of "financial institution").

[72]*Id.* § 326(a) (codified as amended in 31 U.S.C. § 5318(l) (2003)); Customer Identification Programs for Banks, Savings Associations, and Credit Unions, 67 Fed. Reg. 48,290-01 (July 23, 2002) (to be codified at 12 C.F.R. pt. 21); Financial Crimes Enforcement Network; Customer Identification Programs for Certain Banks (Credit Unions, Private Banks and Trust Companies) That Do Not Have a Federal Functional Regulator, 67 Fed. Reg. 48,299-01 (July 23, 2002) (to be codified at 31 C.F.R. pt. 103).

person appears on any lists of known or suspected terrorists or terrorist organizations provided to the financial institution by any government agency.[73] Prior to the Patriot Act, banks were required to know their customer in only three specific situations: (1) to "verify and record the name and address of the individual presenting a transaction" when a CTR filing was required;[74] (2) when customers purchased certain monetary instruments, such as cashier's checks and money orders;[75] and (3) in certain wire transfers.[76] Now presumably every customer is subject to the rules.

The Patriot Act also prohibits financial institutions from maintaining or administering correspondent accounts with unaffiliated foreign shell banks (i.e., banks with no physical offices or branches).[77] It requires financial institutions to take reasonable steps to ensure that a correspondent account maintained or administered by a financial institution in the United States is not being used indirectly to provide services to a foreign shell bank.[78]

The Patriot Act beefs up the BSA's requirements for institutions to maintain formal anti-money laundering programs. In a nutshell, it requires financial institutions to establish anti-money laundering programs commensurate with the size, location, and activities of the financial institutions.[79] While this is nothing new for banks, because they have been obligated to maintain these programs since 1987,[80] it has had a huge impact on non-bank financial institutions, such as broker-dealers and investment companies.

Among other things, the Patriot Act requires financial institutions to establish due diligence policies and procedures to detect suspected money laundering through correspondent accounts and private banking accounts of foreigners. It also gives the Secretary of Treasury authority to impose "special measures" on financial institutions with respect to foreign jurisdictions, financial institutions, transactions or accounts that the Secretary determines to be a "primary money laundering concern."[81] These

---

[73]USAPA § 326(a)(2).

[74]31 C.F.R. § 103.28 (2001).

[75]31 U.S.C. § 5325(a) (2000); 31 C.F.R. § 103.29.

[76]31 C.F.R. § 103.33(e)–(f) (2001).

[77]USAPA § 313(a) (codified as amended in 31 U.S.C. § 5318(j)(1) (2003)).

[78]*Id.*

[79]*Id.* § 352(a)–(c).

[80]31 U.S.C. § 5318(h).

[81]USAPA § 311 (codified as amended in 31 U.S.C. § 5318A(c)(1) (2003)). As of this writing, two countries have been identified as being of "primary money laundering concern":

special measures could include requiring the bank to: (1) maintain additional records or make additional reports in connection with specific transactions; (2) identify the foreign beneficial owners of certain accounts; (3) identify the customers of a foreign bank who use interbank "payable-through" accounts; (4) identify the customers of foreign banks who use interbank correspondent accounts; and (5) restrict or prohibit the opening or maintaining of certain interbank "payable-through" or correspondent accounts.[82]

With all this information, the Patriot Act also establishes a host of provisions designed to encourage, or in some cases compel, the sharing of information among financial institutions, regulators and law enforcement authorities.[83]

Finally, the Act strengthens the sanctions for failure to comply with the money laundering provisions by: (1) requiring federal banking agencies to consider a financial institution's record of combating money laundering when reviewing applications in connection with a bank merger or acquisition;[84] (2) subjecting financial institutions to civil and criminal penalties of up to $1 million for violations of the Patriot Act's money laundering provisions;[85] and (3) authorizing the Secretary to require a U.S. correspondent bank to sever correspondent banking relationships with a foreign bank that fails to comply with or contests a U.S. summons or subpoena.

Ukraine and Nauru. *See* Press Release, Department of the Treasury, Fact Sheet Regarding The Treasury Department's Use of Sanctions Authorized Under Section 311 of the USA Patriot Act (Dec. 20, 2002), *available at* http://www.treas.gov/press/releases/po3711.doc; *see also* OCC Bulletin, Office of the Comptroller of the Currency, Notice of Designation—Designation of Nauru and Ukraine as Primary Money Laundering Concerns (Dec. 26, 2002), *available at* http://www.occ.treas.gov/ftp/bulletin/2002-47.txt. In addition to the two countries officially designated as "primary money laundering concerns," thirteen other nations have been identified by FinCEN as "noncooperative 'in the fight against money laundering'": The Arab Republic of Egypt, Burma, The Cook Islands, Dominica, The Federal Republic of Nigeria, Grenada, Israel, Lebanon, The Marshall Islands, Niue, The Philippines, The Russian Federation, St. Kitts and Nevis, St. Vincent and The Grenadines, and The Seychelles. *See* Advisory Letter, Office of the Comptroller of the Currency, United States Department of Treasury FinCEN Advisories 28 through 32 (June 6, 2003) *available at* http://www.occ.treas.gov/ftp/advisory/2002-5.txt.

[82]USAPA § 311(b) (codified as amended in 31 U.S.C. § 5318A(b) (2003)).

[83]*Id.* § 356(b); Financial Crimes Enforcement Network; Special Information Sharing Procedures To Deter Money Laundering and Terrorist Activity, 67 Fed. Reg. 60,579 (Sep. 26, 2002) (to be codified at 31 C.F.R. pt. 103).

[84]USAPA § 327(b)(1)(B) (codified as amended in 12 U.S.C. § 1828(c)(11) (2003)).

[85]*Id.* § 363 (codified as amended in 31 U.S.C. § 5321(a)(7), 5322(d) (2003)).

Ironically, although the Patriot Act was intended to strengthen the anti-money laundering regime, the new reporting sanctions may exacerbate the over-reporting problem that regulators have battled through the 1980s and 1990s and thereby make the system *less* effective. In passing the Patriot Act, Congress recognized that over-reporting could have a detrimental effect on the usefulness of the information in promoting law enforcement, and therefore directed the Treasury Department to study ways to expand the exemptions from filing CTRs or to increase the utilization of the currently existing exemptions from filing.[86]

Even with this effort to reduce the number of extraneous filings, however, it seems likely those initiatives will be outweighed by other incentives in the Patriot Act to over-report. In addition to the harsh sanctions for non-compliance imposed by the Patriot Act, the new law also extends the safe harbors for filing SARs.[87] So with potentially large sanctions for noncompliance, coupled with a safe harbor for over-reporting, financial institutions are likely to err on the side of filing.

Having laid out the broad outline of existing law and the changes made to that scheme by the Patriot Act, we now turn to the question at hand: will this legislative scheme actually intercept the terrorist funding that it targets?

IV. WHY THE NEW PROVISIONS WON'T DISRUPT TERRORIST FINANCING

Given the legal background, it should be obvious that the task of intercepting terrorist financing stands our system of money-laundering on its head. The job of implementing the plan falls to the FinCEN, an agency in the Department of the Treasury. Since its inception, FinCEN's mission has been to trace the *proceeds* of crimes such as drug trafficking. Proceeds of crimes are somewhat easier to follow than terrorist funds because law enforcement works backwards from the crime itself. In terrorist cases, however, law enforcement is supposed to intercept the funds before a crime occurs. James Sloan, FinCEN director, has called terrorist financing "almost money laundering in reverse."[88]

---

[86] *Id.* § 366(a)(3), (b).

[87] *Id.* § 351 (codified as amended in 31 U.S.C. § 5318(g)(3) (2003)).

[88] Scott Bernard Nelson, *The Money Trail, War on Terrorism Gives Financial Crimes Unit New Stature, Challenges*, BOSTON GLOBE, Dec. 5, 2001, at F1, *available at* LEXIS, News Library (quoting James Sloan, FinCEN director)

In the post-Patriot Act world, FinCEN acts as a clearinghouse for all this financial data. Sifting through and making sense of all the financial data that comes to FinCEN is a herculean task and one which has not been successfully executed in the past. While it may be possible for FinCEN to rise to the challenge by employing state-of-the-art data mining techniques and predictive technology like that currently used in the private sector,[89] much depends on whether FinCEN will have the personnel and resources to implement such a sophisticated arrangement. If the past is any guide, however, FinCEN might very well become the handmaiden of the much more powerful Internal Revenue Service.

Even if FinCEN gives terrorist financing interception its best effort, consider what it is up against. Let us assume the next terrorist attack is another surprise on the scale of the September 11 attacks. With the benefit of hindsight, some observers suggest that the September 11 attacks could have been predicted if intelligence agencies had merely been able to "connect the dots."[90] Unfortunately the problem is not as simple as connecting dots, it is more a problem of figuring out which dots to connect. The intelligence agencies are flooded with information, the vast majority of which is worthless. If we add a torrent of financial transactions information to the mix, we may exacerbate the information overload problem. As a thought-experiment let us consider the following: if FinCEN had been looking to interrupt the September 11 attacks, for what would it have been looking?

A. Terrorist Attacks Are Not Expensive to Fund

Examination of the bank accounts of the nineteen suspected September 11 terrorists have given investigators an idea of how much the terrorist attacks cost.[91] In May 2002, the Wall Street Journal reported the results of

---

[89]*See* Mike France et al., *Privacy in An Age of Terror*, BUS. WK., Nov. 5, 2001, at 83–84.

[90]The phrase "connect the dots" is one employed by Senator Richard Shelby, R-AL, Vice Chairman of the Senate Select Committee on Intelligence, in his separately stated views to the official report of the Senate Select Committee on Intelligence on their Investigation into the Terrorist Attacks of September 11, 2001. *See* September 11 and the Imperative of Reform in the U.S. Intelligence Community, Additional Views of Senator Richard C. Shelby, Vice Chairman, Senate Select Committee on Intelligence, at 5, (Dec. 10, 2002), *available at* http://intelligence.senate.gov/shelby.pdf.

[91]The September 11, 2001, terrorists opened twenty four basic checking accounts at four different banks in the United States with the value of the accounts averaging between three and four thousand dollars. All accounts were opened at large, well-known banks because of the

an FBI investigation that showed the operation was essentially run on a shoestring. The FBI concluded very precisely that the operation had cost $303,672.[92] That is not a lot of money. That small amount would be very hard to detect in our economy where many billions of dollars change hands every day—$300,000 is not even a rounding error.

To make things even more complicated, it is obvious that the whole $300,000 did not move through the financial system all at once. The transactions that funded the hijackers' bank accounts were quite innocuous. Not surprisingly, the bank accounts were funded primarily with cash—47% of the total—wire transfers made up thirty four percent of the funds deposited, eight percent came from travelers checks and the remainder came from miscellaneous sources, including checks from individuals.[93]

Cash was also the preferred way for the terrorists to pay for things. All of these transactions were quite routine and in no way would have triggered any suspicion. The law can require all the reporting in the world, but it is very easy to move around cash the way the terrorists did without generating any concern.

Not only are the amounts small and the transactions ordinary, but the sources of the funds are hard to track in any event. While investigators think they have a good idea about how much money was involved in the September 11 attacks and how it was used, they still do not know from where the money came. It appears that the money was generated by a number of methods including the sale of honey.[94] The cash generated by these activities was then carefully (and slowly) moved by wire transfer from foreign bank accounts to United States accounts held by the hijackers.

While it seems unlikely that the Patriot Act regime would have detected the September 11 transactions, some argue that the expansion of the cash transaction reporting required by the Patriot Act could actually hinder criminal investigations. These concerns are summed up in a comment from Brad Jansen, the deputy director of technology policy for the Free Congress Foundation, a conservative think tank in Washington: "The effect of

---

anonymity that a customer may maintain at a large institution. *See* Cliff Stephens & Tom Crook, *Pressure From All Sides*, BANK SYS. & TECH., Oct. 7, 2002, *available at* http://www.banktech.com/story/BNK20021007S0002.

[92]Paul Beckett, *Sept. 11 Attacks Cost $303,672, But Few Details of Plot Surface*, WALL ST. J., May 15, 2002, at B4.

[93]*Id.*

[94]Judith Miller & Jeff Gerth, *A Nation Challenged: Honey Trade Said to Provide Funds and Cover to Bin Laden*, N.Y. TIMES, Oct. 11, 2001, at A1.

expanding these requirements is to make the haystack bigger. It is not more finely tuning law enforcement tools. It is basically throwing more paperwork at [investigators] without benefit."[95] The art of intelligence gathering has always hinged on the ability of analysts to separate the wheat from the chaff, or to find the useful signal hidden in the distracting noise of information. Adding more noise is unlikely to make that task easier.

B. The Sources of Terrorist Funding Are Hard to Identify

Another challenge facing United States law enforcement officials is identifying the sources of funds that cause serious concern. The money going into a terrorist's bank account does not necessarily come from a bad source. An important source of funds for the terrorists is the apparently legitimate businesses run by the network—travel agencies, road construction companies, and Internet firms.[96]

Complicating the picture is the fact that a significant portion of terrorist funding seems to be coming from charities.[97] Giving alms to charity is one of the central tenets of Islam. There are many charities that support Muslims around the world. Some of the recipients of the charitable largesse might be involved in terrorist activities, although it is extremely difficult to assess whether the charities are making the transfers with the intention of supporting terrorism.[98] The same holds true for individual

---

[95]Jeremy Quittner, *Gauging the New Law's Consumer Impact*, AM. BANKER, Apr. 23, 2002, at 11 (quoting Brad Jansen).

[96]*See, e.g.*, Jerry Guidera & Gary Fields, *Hamas Official, Relatives Face U.S. Charges in 'War of Audits,'* WALL ST. J., Dec. 19, 2002, at A5 (discussing InfoCom Corp. of Richardson, Texas, a computer and Internet firm identified by the Justice Department as a source of terrorist financing); Glenn R. Simpson, *Intricate Web: Tracing the Money, Terror Investigators Run Into Mr. Qadi*, WALL ST. J., Nov. 26, 2002, at A1 (listing a charity, real estate company and chemical business as sources of funding for terrorists).

[97]*The Iceberg Beneath the Charity—Charities as the Source of Terrorist Finance*, ECONOMIST, Mar. 15, 2003, at 67 (reporting that "[p]eople trying to track down al-Qaeda's money believe that charities are terrorists' biggest source of money.").

[98]Given Islam's emphasis on paying alms for the poor, finding that some donated money ends up in the hands of terrorists should not be a complete surprise. At the end of 2002, for example, it was revealed that the wife of the Saudi ambassador to the United States had donated money to a supplicant who in turn gave that money to two of the September 11 hijackers. *See* Susan Schmidt & Mike Allen, *FBI Probes Donations From Saudi; Money From Envoy's Wife May Have Aided Hijackers*, WASH. POST, Nov. 24, 2002, at A1; *see also* Glenn R. Simpson, *Al Qaeda List Points to Saudi Elite*, WALL ST. J., Mar. 18, 2003, at A7 (describing a cache of documents seized in Bosnia allegedly showing how Saudi Arabia's richest and most influential families were among

philanthropists—finding links to terrorists is easy, but establishing the intent is difficult.[99] Of course, it is worth noting that the term "terrorist" itself is hard to define, making the identification of terrorist groups even more problematic. One person's "terrorist" is often another person's "freedom fighter."[100]

Two Chicago area charities, Benevolence International and Global Relief Foundation, were raided by Treasury agents in December 2001.[101] Global Relief was targeted on the basis of a suspected link between its director and high-ranking Al Qaeda officials.[102] Global Relief claims the $5 million it raised in 2000 paid for food, health care, and other emergency services in Afghanistan, Chechyna, Kosovo, Lebanon, Pakistan, and the West Bank.[103] A problem these international charities face is that their funding is often most necessary in international hot spots, where it is hard to tell the rebels from the victims from the terrorists.

C. *Terrorists Move Money Through Hard-to-Regulate Non-Bank Channels*

Even if the reporting requirements of the Patriot Act work perfectly, the new law still will not be effective to intercept terrorist financing because terrorists do not have to use banks to move money. The lynchpin of our existing money laundering scheme is the conventional banking system. We count on bankers to file CTRs and SARs because bankers are subject to a rigorous regulatory scheme and they know they will get into trouble if they do not comply with the law. Terrorists, however, do not necessarily rely on the banking system to move money because they have access to other reliable ways to transfer funds around the world.

The Islamic world is tied together financially by a traditional banking system known as the *hawala*.[104] These ancient networks of settling

---

the first supporters of Osama bin Laden).

[99]Keith Johnson, *Reasonable Doubt? Mapping the Trail of Terror Money Proves Daunting*, WALL ST. J., May 15, 2003, at A1.

[100]The United States has supported over the years many groups that might be considered terrorists by others. *See* DERSHOWITZ, *supra* note 3, at 7–8.

[101]Hanna Rosin, *U.S. Raids Offices of 2 Muslim Charities; Groups Accused of Funding Terror*, WASH. POST, Dec. 16, 2001, at A28.

[102]Dan Eggen & Kari Lydersen, *In Michigan, Anti-Terrorism Effort Goes Public; Haddad Case Forces Rare Glimpse of Secret U.S. Campaign*, WASH. POST, May 6, 2002, at A3.

[103]*Id.*

[104]For a tidy summary of the *hawala* banking system, see Alan Lambert, *Organized Crime,*

payments have deep roots in Islamic culture. They are essentially based on trust, and involve no physical transfer of funds. For example, a *hawala* broker in one country instructed by his client arranges for a broker in another country to make a payment to the intended beneficiary.[105] Such informal systems are not designed to deal with official transactions; instead, they provide complete confidentiality and no paper trail.

Given the pervasiveness of the *hawala* system and its informality, law enforcement officials find it difficult to use the *hawala* network to fight crime. In India, Pakistan, and the Middle East where these systems are common, they create significant money laundering problems. One big problem they present is the difficulty of distinguishing between legitimate transactions and those involving money laundering.[106]

In the aftermath of September 11, the United States and other nations froze a Dubai based *hawala* called "Al Barakaat."[107] This action made headlines and significant sums were impounded, but one wonders what effect it had on terrorist operations.[108] These networks are highly adaptive entities and if currency transfers are targeted by law enforcement, they may very well change tactics. If need be, the funds to be transferred are paid in jewelry to the brokers, who later rationalize their own inter-banking levels and fund flows amongst themselves.[109]

The Patriot Act ostensibly applies to *hawala* banking,[110] but enforcement will be difficult. FinCEN has identified a strategy for dealing with *hawalas*:

Terrorism, and Money Laundering in the Americas, Underground Banking and Finance of Terrorism, 15 FLA. J. INT'L L. 9, 12–19 (2002).

[105]*Cheap and Trusted*, ECONOMIST, Nov. 24, 2001, at 71.

[106]In a bit of an ironic twist, the United States government has found that the only effective way to transfer funds into Afghanistan to aid in its reconstruction is to use the existing *hawala* banking system because no other financial infrastructure exists in that devastated region. *See* Michael M. Phillips, *Afghan Aid Flows Through Dark Channels*, WALL ST. J., Nov. 12, 2002, at A4.

[107]Glenn R. Simpson et al., *U.S. Intensifies Financial War On Terrorists*, WALL ST. J., Nov. 8, 2001, at A3.

[108]Christopher Cooper & Ian Johnson, *Ongoing Concerns: Money Network Tied to Terrorism Survives Assault*, WALL ST. J., Apr. 22, 2002, at A1.

[109]*Cheap and Trusted*, *supra* note 105, at 71.

[110]USAPA § 359 (amending 31 U.S.C. § 5312(a)(2)(R) to include any "person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system").

> Our strategy is (1) to force terrorist financiers to reduce reliance on hawala and similar systems and to channel their money into more transparent, formal financial transactions; (2) to regulate hawaladars so that legitimate hawaladars comply with financial reporting structures; and (3) to target the illegal use of hawala for intensive investigation.[111]

Although this approach is laudable, it sounds like a true clash of cultures. Given the long history of *hawala* banking, its informality, its secrecy, and its deep roots in Islam, it seems unlikely that *hawala* bankers will be enthusiastic in their compliance with the new law. More importantly, the law might never be enforced against the *hawala* because the identities of the *hawala* bankers are difficult to establish. Without knowing who is participating in the *hawala*, the regulatory scheme will be ineffective.[112]

D. Interactions with the Underground Economy

Another factor that makes tracking terrorist funding difficult is that much of it comes from activities of the underground economy which are already off the radar screen. Of course, this is the strongest argument for using the existing money laundering machinery to intercept terrorist financing.

Some observers of the international money laundering scene have noted that just as separate organized crime groups work together toward common ends—for example, the Russian "Mafia" and Colombian drug cartels—so too are terrorists and organized crime groups working together.[113] Terrorist groups, for example, have been implicated in the international narcotics trade.[114]

---

[111]U.S. DEP'T OF TREASURY & U.S. DEP'T OF JUSTICE, 2002 NATIONAL MONEY LAUNDERING STRATEGY 22 (July 29, 2002), *available at* http://www.treas.gov.

[112]*See* Lambert, *supra* note 104, at 15.

[113]*Money Laundering and Business Crime* (Proximal Consulting, Geneva, Switzerland), Oct. 2001, at 4, *available at* http://www.proximalconsulting.com/NewslettersPDF/Newsletter9.pdf.

[114]*See, e.g.*, Barry Meier, *A Nation Challenged: Drugs; Most Afghan Opium Grown in Rebel-Controlled Areas*, N.Y. TIMES, Oct. 5, 2001, at B5; Tim Golden, *A Nation Challenged: War and Drugs; Afghan Ban on Growing of Opium is Unraveling*, N.Y. TIMES, Oct. 22, 2001, at B1.

The global economy presents opportunities for both criminals and terrorists, and both groups have been savvy to exploit those opportunities.[115] Unfortunately, the sophistication of the bad guys always seems to be a few steps ahead of the cooperation of the individual countries in thwarting money laundering. One senior law enforcement official summarized the problem in these words: "[Money laundering] is a phenomenon that respects no borders. The organized crime groups and the terrorist organizations are far more attuned to the realities of the globalist century than Western governments are."[116]

E. Alternative Sources of Wealth

Yet another problem confronting counter-terrorism experts is that terrorists do not necessarily rely on currency transactions to move wealth from place to place. Some experts believe, for instance, that the recently beefed-up money laundering laws may only serve to force terrorists back to old-fashioned conduits of wealth transfer such as gold bars.[117]

As an example, there is substantial evidence that the terrorists have used the gem tanzanite, which is mined only in a remote corner of Tanzania, as a method for storing and transporting wealth.[118] The trade in the gem has been in large part taken over by Islamic extremists.[119] As a result of the link to terrorist financing, a number of United States jewelers now refuse to carry tanzanite jewelry.[120]

---

[115]For example, narcotics traffickers have acquired real property with monetary instruments that they purchased in structured amounts, under $10,000, and have also laundered cash proceeds by exchanging them for checks from a real estate company. *See* Molly McDonough, *Real Estate Lawyers Could Be Watchdogs*, 2 A.B.A J. E. REP. 17 (May 2, 2003). If narcotics traffickers have figured this out, it is likely terrorists have as well. To illustrate, in *United States v. High*, prosecutors alleged a real estate company took $35,000 in tainted cash on two different occasions, each time converting the money into five separate cashier's checks to make down payments on property. 117 F.3d 464, 467 (11th Cir. 1997). The balance was paid in cash at the realty office. *Id.*

[116]Money Laundering & Business Crime, *supra* note 113, at 4 (quoting unnamed senior official at an international law enforcement agency).

[117]*Moving Target*, ECONOMIST, Sept. 14, 2002, at 72.

[118]*See* Robert Block & Daniel Pearl, *Underground Trade: Much-Smuggled Gem Called Tanzanite Helps Bin Laden Supporters*, WALL ST. J., Nov. 16, 2001, at A1.

[119]Glenn R. Simpson & Robert Block, *Diary Offers More on Tanzanite, Al Qaeda Link*, WALL ST. J., Jan. 24, 2002, at B1.

[120]*See* Jerry Markon, *Gemstone Dealers Named in Suit Over Sept. 11*, WALL ST. J., Feb. 15, 2002, at B1.

The diamond trade may present an even more difficult situation. Tainted diamonds used to finance terror are said to come from mines controlled by various African rebel groups where the gems are mined with slave labor and sold into the black market to fuel ongoing political strife.[121] The new rules put out by the Treasury Department would require dealers in precious metals, stones, or jewels to comply with the money laundering provisions[122] as well; again, we will see how effective that is. Like the *hawalas*, the diamond business is subject to its own informal rules of conduct laid down through long-standing norms of behavior. Top-down regulatory edicts are unlikely to enjoy widespread voluntary compliance.

IV. LIVING WITH THE PATRIOT ACT

The Patriot Act, with all of its shortcomings, is nevertheless the law of the land. Even if the prospects for intercepting terrorist financing are dim, financial institutions nevertheless must comply with the law. One can anticipate some problems in applying the law to specific situations. Several obvious problems remain to be resolved.

First, how exactly does one go about knowing one's customer? The federal banking agencies have promulgated a regulation to implement the Knowing Your Customer ("KYC") provisions of the Patriot Act that require the gathering and verification of certain key items of information.[123] Although the regulation permits the use of documents to verify the information provided, it recognizes that documents alone may not be available, or if available, not sufficiently reliable in some cases.[124] We do not have any kind of official identity documents in this country. Birth certificates are notoriously non-uniform, yet drivers licenses are based on birth certificates, as are passports.[125] In addition, the regulations were watered down at the last minute at the urging of the financial services

---

[121]*See* Joseph Kahn, *A Nation Challenged: The Money Trail; House Votes to Combat Sale of Diamonds for War*, N.Y. TIMES, Nov. 29, 2001, at B6.

[122]31 U.S.C. § 5312(a)(2)(N) (2003).

[123]*See* Customer Identification Programs for Banks, Savings Associations, Credit Unions and Certain Non-Federally Regulated Banks, 68 Fed. Reg. 25,090 (May 9, 2003) (to be codified at 12 C.F.R. pts. 21, 208, 211, 326, 563, 748, and 31 C.F.R. pt. 103).

[124]Customer Identification Programs for Banks, Savings Associations, Credit Unions and Certain Non-Federally Regulated Banks, 68 Fed. Reg. at 25,099-100 (discussing 31 C.F.R. § 103.121(b)(2)(ii)(A)).

[125]Thomas P. Vartanian, *Proposed ID Regs Pose Challenges*, AM. BANKER, Jul. 19, 2002, at 6.

industry so that banks and other financial intermediaries are not required to keep copies of the documents they rely on in establishing customer identity.[126]

Terrorists are very good at identity theft, identity cloning, and impersonating legitimate people.[127] Even without manipulating identity documents, terrorists can get around the rules by accessing the financial system through a corporate shell—making it difficult for the financial institution to really know who is the beneficial owner of the entity they are dealing with in the transaction.[128] Alternatively, terrorists may fly under the radar of the KYC rules by using various "back door" techniques for establishing accounts.[129]

Bankers are skeptical that the new requirements will make any difference in apprehending terrorists.[130] What identification verification is really about in today's business world is producing enough evidence to allow someone to conclude that it is more likely than not that you are who you say you are. Complicating the process of customer identification and comparison to the watch list is the ever-present problem of transliterating Arabic names into English.[131] There may be real initiatives toward biometrics or national ID's, perhaps with some kind of coded information that would tie into a national database, but those developments are still in the future. While the KYC regulations quixotically try to trap terrorists who are exceptionally adept at sidestepping identity problems, the regulations may have the unintended consequence of stifling legitimate innovation in other payment processes, such as on the Internet, where the

---

[126]*See* Glenn R. Simpson, *Legislator Calls New Bank Rule Lax*, WALL ST. J., May 27, 2003, at A5.

[127] *See* Vartanian, *supra* note 125, at 6 (noting that the September 11 hijackers opened 35 deposit accounts using illegitimate social security numbers without being detected).

[128]*See Shell Games*, ECONOMIST, Oct. 26, 2002, at 69.

[129]Gus Blanchard, *Go Beyond Patriot Act and Close Back-Door Access to Accounts*, AM. BANKER, July 19, 2002, at 7.

[130]In the words of Richard Small, director for Global Anti-Money Laundering for Citigroup, "'For someone to suggest that we'll pick up terrorists,' through such measures, 'scares me tremendously.'" *See* Steve Cocheo, *Dousing Terrorist Funding: Mission Possible?* A.B.A. BANKING J., Aug. 2002, at 40.

[131]The experience with the "No Fly List" holds lessons for the financial services industry. Rendering names written in Arabic script into the Roman alphabet is an inexact science. In addition, how the name is translated varies considerably from one Arab country to the next. *See* Ann Davis, *Boarding Impasse: Why a "No Fly List" Aimed at Terrorists Often Delays Others*, WALL ST. J., Apr. 22, 2003, at A1.

barriers to identifying the parties with certainty are high and the costs of the transactions are small.[132]

A second major problem with the Patriot Act concerns the clash between its provisions, the provisions of the Right to Financial Privacy Act of 1978,[133] and the Gramm-Leach-Bliley Financial Modernization Act of 1999.[134] Specifically, section 314 of the Patriot Act—which authorizes the sharing of customer information between financial institutions, regulators, and law enforcement agencies—could render the protections afforded by the Right to Financial Privacy Act of 1978 ineffective and diminish the effectiveness of the Gramm-Leach-Bliley Act of 1999's privacy provisions, which prohibit the sharing of customer information between financial institutions for marketing purposes.

In the words of Assistant Attorney General Michael Chertoff in testimony before the Senate Banking Committee, "the principal provisions of the Right to Financial Privacy Act no longer apply to letter requests by a government authority authorized to conduct investigations or intelligence analysis for purposes related to international terrorism."[135] As Chertoff understands the Patriot Act, law enforcement officials investigating terrorist activities no longer have to file a subpoena when requesting bank records.[136] If the law has changed in this way, banks are placed in a very awkward position, and should legitimately worry whether the safe harbor provisions of the Patriot Act will help them avoid liability for violations of the Privacy Act.

The Patriot Act calls for information sharing between the financial services industry and the government.[137] In order to share the information, the bank must first be certified.[138] Some banking observers suggest that

---

[132]*See* Yochi J. Dreazen, *Money Transfers: Too User Friendly? Legislation Aimed at Stopping Terrorism Could Have a Devastating Impact on an Innocent Bystander: PayPal*, WALL ST. J., Oct. 21, 2002, at R9 (describing the impact of the Patriot Act on the Internet payment system PayPal, whose average payment is $57 and whose service is designed to make transfers as simple and as low-cost as possible).

[133]Pub. L. No. 95-630, 92 Stat. 3697 (1978) (codified at 12 U.S.C. §§ 3401–3422).

[134]Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified in scattered sections of 12, 15, 16 and 18 U.S.C.).

[135]Rob Garver, *Will USA Patriot Act Prove a Recipe for Trouble?*, AM. BANKER, Apr. 23, 2002, at 10 (quoting Assistant Attorney General Michael Chertoff).

[136]*Id.*

[137]USAPA § 314(a).

[138]*See Financial Crimes Enforcement Network, available at* http://www.fincen.gov/fi_infoappb.html (last visited Sept. 19, 2003).

bankers will feel a pressure to voluntarily obtain certification and share customer information in order to show that the bank is a "good citizen." That good citizen status could come in handy if the institution runs afoul of the arcane rules of money laundering and is faced with an enforcement action.[139] On the other hand, the privacy provisions of existing law make the sharing of customer information without the customer's consent problematic.[140] Bankers should be worried that once the fear of terrorism fades, customers will bring suits to assert their traditional rights of financial privacy.

Another unanswered question for financial institutions concerns what to do with tainted funds if any are discovered. One thing is clear; the institution cannot deliver those funds back to the bad guys—to do so would constitute money laundering. The likely course of action is to freeze the tainted assets. But that only raises a different serious question—how does the money get unfrozen? When it is unfrozen what happens to it? Does it go to victims of September 11? To the government? To Afghanistan? No one knows the answer to this question. Experience has shown with the frozen assets of dictators like Mobutu Sese Seko, that money frozen in foreign bank accounts is awfully difficult to thaw out.[141]

Yet another issue we will have to confront is the appropriate reach of the Patriot Act. There is a movement afoot in the Financial Action Task Force on Money Laundering (FATF) to impose the money laundering disclosure and reporting requirements on attorneys whose clients are engaging in suspicious transactions.[142] The FATF is considering requirements that lawyers identify clients suspected of money laundering, and that they report suspicious client activity to authorities.[143] The group says its object is to make it more difficult for money launderers to misuse the services of a lawyer. Of course, one could also view the requirements as yet another instance of governmental efforts to disrupt the solidarity of attorneys and their politically unpopular clients.[144]

---

[139]*See* Cocheo, *supra* note 130, at 44.

[140]*See* 15 U.S.C. § 6802 (2000).

[141]*See* Roger Thurow, *Frozen Terrorist Funds May Not Thaw Easily; Who Gets the Money?*, WALL ST. J., Nov. 14, 2001, at A1.

[142]*See* Rhonda McMillion, *Gatekeeper's Burden: Money Laundering Proposals Raise Concerns About Attorney-Client Privilege*, A.B.A. J., Dec. 2002, at 72.

[143]*Id.*

[144]For a general discussion of government efforts to disrupt attorney-client solidarity, see Peter Margulies, *The Virtues and Vices of Solidarity: Regulating the Roles of Lawyers for Clients*

The ABA Task Force on Gatekeeper Regulation and the Profession, (ABA Task Force) was created to examine the proposed international money laundering regulations. The ABA Task Force opposes laws that would require lawyers to file reports of clients' suspicious transactions.[145] The group does, however, support increased training to help lawyers identify money laundering, as well as a proposal that would require lawyers who receive and transfer client funds to verify clients' identities, and keep records of domestic and international transactions.[146]

While the ABA Task Force opposes mandatory reporting, it does not oppose sharing non-privileged information subject to a subpoena. Obviously, for United States lawyers, these reporting and disclosure requirements would pose an intractable ethical conflict. The touchstone of our system of legal ethics is the preservation of client confidences except in a few narrow instances.[147] Reporting such transactions could violate the attorney-client privilege, although the Model Rules state that a lawyer may disclose client information to the extent reasonably necessary to "comply with other law or a court order."[148] Any new money laundering requirements might fall into that category, but the creation of such a requirement is clearly inconsistent with our tradition. In addition, in most places, the bar is regulated by the judicial branch, not the legislature, because lawyers are officers of the court. The imposition of attorney disclosure rules as a matter of legislative enactment or executive order could raise difficult separation of powers questions.

Finally, the biggest challenge we face is keeping the Patriot Act in its place. In the heat of the moment, Congress passed a sweeping law that curtails some of the freedoms we cherish. Ostensibly, the law was a response to terrorism, but as the forgoing discussion has shown, the effect of the money laundering provisions on terrorist financing is tenuous. The Patriot Act tips the balance heavily in favor of law enforcement when it

---

Accused of Terrorist Activity, 62 MD. L. REV. 173 (2003).

[145] *Id.*

[146] *Id.*

[147] *See* MODEL RULES OF PROF'L CONDUCT R. 1.6 (2002) (noting that ordinarily lawyers shall not reveal information, but may disclose information to (1) prevent reasonably certain death or substantial bodily harm; (2) to secure legal advice about compliance with the rules of professional conduct; (3) to establish a claim or defense when being sued by the client; or (4) to comply with other law or court order).

[148] *Id.*

comes to financial transaction reporting. We may live to regret the quick action Congress took to respond to the terrorist threat.

While at the time of its passage the Patriot Act seemed to be focused on foreigners, aliens and suspected terrorists, the actual authority the government gained was much broader: to pursue and gather and look at and access personal information on all of us in order to find those suspects. One commentator has referred to the process by which the Patriot Act was adopted as a "bait and switch" scam.[149] The law is now in place to allow the government a lot more access to a lot more transactions than we have previously thought wise. The new money laundering rules will have limited value in stopping another September 11. On the other hand, they will be tremendously helpful for the government in putting together cases of tax evasion.[150]

Since the enactment of the Patriot Act, the administration has taken a series of steps suggesting a deliberate decision to abandon the law enforcement paradigm for government investigations of individuals in the United States and substitute an intelligence paradigm that seeks to secretly gather all information that might turn out to be useful.[151] Although "[a]lmost every other nation in the world has an internal security agency that is separate from its law enforcement agency, [and] freed from many civil liberties' constraints," that approach has not been part of the American tradition of law enforcement.[152] Florida Democrat Bob Graham, a member of the Senate Intelligence Agency, expressed concern that there is a "'fundamental difference' between a law enforcement agency such as the FBI, which tries to solve crimes, and an intelligence agency which tries to prevent crimes."[153]

The shift toward an intelligence paradigm has been made without public deliberation about whether such an approach will in fact be effective in the

---

[149]*Quittner*, *supra* note 95, at 11.

[150]*See* Glenn R. Simpson, *U.S. Tries 'Al Capone' Tax Charges in Some Terror-Financing Cases*, WALL ST. J., Oct. 10, 2002, at A1.

[151]Kate Martin, *Intelligence, Terrorism and Civil Liberties*, HUM. RTS., Winter 2002, at 5, *available at* http://www.abanet.org/irr/hr/winter02/martin.html.

[152]Philip B. Heymann, *Civil Liberties and Human Rights in the Aftermath of September 11*, 25 HARV. J.L. & PUB. POL'Y 441, 447 (2002).

[153]Carl Limbacher, *Senators Skeptical of FBI's Ability to Fight Terrorism*, NEWSMAX.COM, Dec. 2, 2002, *available at* http://www.newsmax.com/showinside.shtml?a=2002/12/2/221707 (quoting Senator Graham). Graham said he does not know whether these two agencies can be blended together. *Id.*

fight against terrorism. "It is not obvious that a dragnet approach to detaining individuals or an intelligence effort to collect all information, relevant or not, will be as effective as a focused law enforcement investigation aimed at identifying, surveilling, and arresting those involved in criminal activity."[154] Indeed, traditional techniques of law enforcement have had some success in tracking down terrorist cells while also respecting the civil liberties we hold dear.

Law enforcement on its own can perform a valuable contribution to preventing terrorism by building on their community policing networks to exchange information with citizens and gather intelligence. A federal office could assist with the development of regional task forces by providing experts to assist in the needs assessment, project planning, and training efforts. Existing anti-terrorist task forces, High Intensity Drug Trafficking Area (HIDTA) task forces, and regional crime analysis information systems provide many examples of effective collaboration without obliterating completely the distinction between law enforcement and intelligence.[155]

A good example of the kind of cooperation that respects the traditional roles of law enforcement and intelligence is the successful disruption of the *Hezbollah* tobacco smuggling ring. The investigation of the operation began in 1996 when Iredell County, North Carolina, authorities noticed people with out-of-state license plates making large cash purchases from JR Tobacco, a discount tobacco outlet in Statesville, North Carolina.[156] The smugglers were purchasing large quantities of cigarettes in North Carolina, where the excise tax is only 50 cents per carton, and then transporting them for resale to other states where the excise taxes were much higher.[157] While this tax-evading smuggling was cause for law enforcement involvement, the case became much more complicated in 1999 when intelligence officials joined the investigation after it became clear that the smuggling ring was supporting the efforts of the militant *Hezbollah* terrorist group.[158] The

---

[154]Martin, *supra* note 151, at 5.

[155]*Local Law Enforcement's Role in Preventing and Responding to Terrorism*, Chuck Wexler, Police Executive Research Forum, PERF Survey, Oct. 2, 2001.

[156]*Hezbollah Denies Involvement*, ABC News, July 22, 2002, *available at* http://www.abcnews.go.com/sections/us/DailyNews/Hezbollah000721.html.

[157]In Michigan, for example, the tax on cigarettes was $7.50 per carton. The smugglers moved millions of dollars worth of cigarettes from North Carolina to Michigan between 1996 and 1999. Gordon Fairclough, *Lebanese Immigrant Is Guilty of Smuggling, Hezbollah Aid*, WALL ST. J., June 24, 2002, at B4.

[158]Gordon Fairclough, *Alleged Donors To Hezbollah Facing Trial*, WALL ST. J., December 3,

investigation into the cigarette smuggling ring involved local, state, federal, and international police and intelligence officials.[159] Ultimately, the ringleader of the smuggling operation was sentenced to 155 years in prison.[160]

While traditional law enforcement and intelligence functions can produce results in the war on terrorism, the effort and coordination to do so is tremendous. On the other hand, having the extraordinary powers of the Patriot Act may be a strong narcotic for law enforcement authorities. It may very well make their lives easier as they pursue the many non-terrorist criminals they deal with day in and day out. If the Patriot Act's new powers only serve to bolster the cases against tax cheats and drug runners, then when the sunset provisions require the re-authorization of the law in 2005, law makers ought to remember what the Patriot Act was supposed to achieve and for what it was actually used. Unfortunately, there will be precious little information available to lawmakers in 2005 to determine the effectiveness of the Patriot Act's provisions because the law mandates no reports regarding the provisions' effectiveness. Without the necessary information about how these broad new powers have been used, Congress will be unable to evaluate whether they were needed and how they have been used in order to make an informed decision about whether and how they should continue.[161] Indeed, before the verdict is in on the efficacy of the Patriot Act, the Department of Justice has proposed an even more draconian law enforcement bill, the "Domestic Security Enhancement Act of 2003," sometimes called "Patriot II."[162]

People who believe that these provisions go too far, however, can expect the proponents of law enforcement to say that the new reach of financial reporting is a good thing and has helped shut down non-terrorist bad guys.[163] When the debate about re-authorization begins, proponents of

---

2001, at B1.

[159] *Id.*

[160] *Hezbollah Smuggler Sentenced*, N.Y. TIMES, March 1, 2003, at A11.

[161] Electronic Frontier Foundation, *EFF Analysis of the Provisions of the USA Patriot Act*, Oct. 31, 2001, *available at* http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.

[162] A section-by-section analysis of the proposed legislation is available at the website of the American Civil Liberties Union, *available at* http://www.aclu.org/SafeandFree/SafeandFree.

[163] Senator Orrin Hatch (R-UT) has already introduced legislation that would repeal the sunset provisions of the Patriot Act and make all of the new powers permanent. The idea faces strong opposition from many Democrats and even some key Republicans. House Judiciary Committee

the pre-Patriot Act standards of privacy will find themselves in the awkward position of advocating in favor of rules that serve to make it more difficult to build a case against criminals who happen not to be terrorists. Politically, that will be a tough sell, but the assault on civil liberties has created some unusual political alliances opposed to the extension of the Patriot Act.[164] It should be an interesting battle.

VI. CONCLUSION

As we continue to wage the war against terrorism we must recognize that using the money-laundering reporting scheme to shut down terrorist financing is an incredibly ambitious goal and may not be feasible. While the purported goal of the new anti-money laundering laws may be out of reach, the law will nevertheless have real consequences for financial institutions and their customers. Customers have sacrificed a measure of privacy to the government, and while the information so surrendered is supposed to help identify terrorists, there is no prohibition on it being used by the government for other types of investigations or surveillance.

The balance of power has shifted toward law enforcement in the arena of financial reporting. Recovering the standards of financial privacy enjoyed before the enactment of the Patriot Act will be politically awkward. While in the immediate aftermath of September 11 the Patriot Act may have had a calming effect on a stunned and frightened populace, upon clear examination it is frightening in its own right.

The passage of the Patriot Act may have been a response to the psychology of terrorist warfare in which "bringing out the big guns" is a way to reassure the citizenry and keep them from panicking. But viewed another way, the passage of the Patriot Act plays right into the hands of the terrorists by forcing a reaction in which the target population turns on itself and allows terror to get the better of them. It is worth considering whether

---

Chairman James Sensenbrenner (R-WI) has already voiced deep reservations about making the new powers permanent. Sensenbrenner stated that the Department of Justice has not been sharing enough information with Congress to allow a fair evaluation of how well or poorly the USA Patriot Act is working. The debate may bring needed attention to the expansion of secrecy and reduction in government accountability that has occurred under the USA Patriot Act and the Homeland Security Act. *See Permanent Patriot Act*, 4 OMB WATCHER No. 8, April 21, 2003, *available at* http://www.ombwatch.org/article/articleview/1476/1/173.

[164]Paul Magnusson & Lorraine Woellert, *Don't Tread on Us: The Revolt Against the Patriot Act*, BUS. WK., May 19, 2003, at 51 (noting that the opposition to the Patriot Act spans the ideological spectrum).

in the heat of the moment we have bargained away too much privacy in order to grasp an elusive law enforcement advantage.