MONEY LAUNDERING COUNTERMEASURES WITH PRIMARY FOCUS UPON TERRORISM AND THE USA PATRIOT ACT 2001

Professor Fletcher N. Baldwin, Jr.
Phone: (352) 292-2211
Fax: (352) 392-3005
E-Mail: BALDWINFN@LAW.UFL.EDU
Chesterfield Smith Professor of Law
Director, The Centre For International
Financial Crimes Studies
Levin College of Law
University of Florida
Gainesville, FL 32611-7625

I

INTRODUCTION

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism[1], euphemistically the USA Patriot Act 2001, is in direct response to terrorism world-wide as noted in United Nations Security Council Resolution 1373. The USA Patriot Act followed Congressional authorization of September 14, 2001 granting broad power to the executive to seek out and destroy terrorists. The Act is, in part, 1) intended to complement and support the military campaign in Afghanistan and elsewhere and 2) allocate to law enforcement more realistic weapons and user friendly laws to fight terrorists and terrorists funding. The two goals require a broad redesign of the United States Bank Secrecy Act and its subsequent amendments.[2]

The USA Patriot Act (hereinafter: the Act) defines terrorism and focuses upon enhancing domestic security by implementing legislation involving, among other things, computer privacy, electronic surveillance, warrants to trap and trace, no knock searches, and extra-territorial search warrants. The Act also implicates matters involving immigration and borders including bulk cash smuggling. More importantly, in Title III there are over forty complex new banking and other money transmitting regulations impacting upon extra-territoriality, off-shore correspondent banking, underground banking, as well as new predicate crimes complementing the crime of money laundering, and agency sharing.[3]

Much of the focus of the Act is international money laundering and anti-terrorism financing. The focus derives from the extreme danger the modern terrorist poses to the infrastructure, the national defense, and the International economic system.

Title III, of the Act, as well as the subsequent rules promulgated thereunder by the Treasury Department, impacts upon the illicit money trails, foreign bank correspondent accounts, foreign person private banking accounts, savings associations, credit unions, casinos and others similarly situated. In brief, Title III grants to the Secretary of the Treasury extensive powers to impose special measures against any foreign financial institution, regardless of jurisdictional considerations.

The Act permits forfeiture of proceeds even if the crime took place on foreign soil as long as the proceeds from the illicit act were transferred to or invested in the United States. The specific crimes include any crime of violence, bribing of a public official, embezzlement of public funds, munitions smuggling, or any offense which if committed in the United States would subject the perpetrator to extradition or criminal prosecution. Of significant importance, Title III permits *in rem* forfeiture of funds where illicit funds are transferred from a correspondent bank account to an interbank account and the illicit funds account is traceable to funds originally deposited in a foreign bank or other financial institution holding the account. Under the Act, the foreign bank from which the funds are forfeited has no standing in a United States court to contest the forfeiture. Only the "owner" of the funds account in the foreign bank has standing. Significant problems and conflicts may develop within the foreign bank's home jurisdiction if there is a mandated duty to pay depositors.

The United States Congress in Title III is also attempting for the first time to regulate the underground banking systems such as Hawala, or Hundi.

On October 26, 2001 President Bush signed the Patriot Act into law[4]

With the apparent lack of political will that existed prior to September 11, 2001 no longer

an obstacle federal law enforcement has moved quickly to begin the implementation of the Act. The goal was, and is, to penetrate the heart of the terrorist organizational machine, or as author Peter L. Bergen termed it: *Holy War, Inc.*[5] The goals of the Act implicate and require international cooperation, re-designation of internal laws, and enhanced cross-border cooperation. Without international cooperation, the Act will lose most of its intended impact.

II

LEGISLATIVE HISTORY

To be successful, terrorist as well as organized crime operations require sturdy support internationally and otherwise[6] "user-friendly" states citizens, and institutions are a necessity.

Banks, citing bank secrecy; nations, citing sovereignty concerns; and elected public officials, citing freedom from governmental financial controls; intentionally or unintentionally created safe havens for the transfer and hiding of the illicit funds and profits of organized crime and organized terrorists. Funds gathered within lax jurisdictions are funneled to terrorist cells around the world. Lax banking regulations and poor financial oversight provides stepping stones and networks for the financing of terrorist activity. Law enforcement world-wide had noted increased activity by terrorist groups, but had received little governmental support in their efforts.[7] Reading such recent works as *Holy War, Inc.*, one has reason to speculate that there was very little political will to encourage law enforcement to conduct an all-out assault upon the financial networking of organized terrorist groups such as al-Qaeda.[8] Nevertheless, who could have ever envisioned the catastrophic acts of September 11, 2001?

The events of September 11, 2001, appear to have changed the political posturing mileau. In the United States, the recognition of vulnerability to, and threat of, future acts resulted

in the USA Patriot Act. The Act, controversial to be sure, nevertheless signaled support from previously silent elected and appointed officials for the efforts of law enforcement in the transnational arena. Governments, democratic and otherwise, have now signaled their approval and support for an all-out assault upon the holdings of terrorist groups.

Each generation faces a defining moment – the London Blitz spanning more than two years, December 7, 1941; the Darwin Defenders and the fall of Paris, to name but a few, tested the resolve of a generation. That generation, whether the few Royal Air Force pilots over London, those prepared to sacrifice their lives to protect Australia from invasion, the United States Marines going ashore at Iwo Jima, or the free French resistance in the face of German occupation, met the threat of and challenges deemed crimes against humanity and successfully restored, installed or protected democratic governments in the hope of avoiding repetition.

September 11, 2001, was and is a defining date not only for the people of the United States, but for democratic societies everywhere. The spiraling impact of September 11 has reached and penetrated many shores.[9] Since September 11, 2001 people of many nations have demonstrated a will to deal with both the magnitude of the terrorist attack and the threat and fear of continuing terrorism.

Terrorists have learned their lessons from history. In the 19th century, terrorists became more political, no longer focusing upon the religious ideals of 12th century Ismailis, and more upon anarchism. Recently, in Bosnia, the terrorist threat to civilization finally got the attention of some nations.[10]

Terrorists have emerged who are prepared to die voluntarily, their rewards awaiting them in the after-life, unaware that they are sacrificing their lives for mortals seeking territory, profit,

and political power.[11] With extensive preparation and about $532,000 the sponsors and the actors of September 11, 2001, committed a devastating act of terror.[12]

Since the conclusion of World War II, old and new democracies appeared to grow accustomed to, and, some might argue, tolerant of global, "white collar" organized crime. However, tolerance in some arenas, does not translate into tolerance in others.[13] Terrorist activity impacts upon the very foundation of the democratic state.

Government and business in the United States, as well as elsewhere, regardless of external impressions, have a sophisticated understanding of the workings of organized crime and its transnational components. The same cannot be said of transnational terrorism. Religious and nationalist fanatical fervor have not been well understood. Gathering information regarding terrorist activity has been difficult as has sharing the information, even among colleagues. September 11, 2001, resulted in, among other alterations, a modification or redirection of government with respect to more effective law enforcement “weapons,” information sharing, reevaluation of financial secrecy programs, and implementing financial controls designed to better trace and seize the illicit money.

The reality now penetrating the political mind set is, one can only assume, that both organized crime and organized terrorism operate in similar borderless environments. Each pose a threat to the stability and security of international and national communities. Organized terrorist groups and organized crime syndicates profit from their illicit acts; the acts of the terrorists pose a far greater threat to a nation’s political psyche as well as its financial markets. The threat from organized terrorists is by far the is the more intense and the more complex.

Organized crime has in the past caused many nations to redesign their laws; the

privatization of terror is accomplishing a similar purpose. Nations have formally stated that the threat and impact of global organized crime is a threat to national security. The same can be said of organized terrorism. Organized crime and organized terrorism have a common thread, common characteristics, and perhaps some similar goals. Organized crime and organized terrorists have at times joined together for mutual benefit?[14] The victim states learn from the commonalities and react accordingly. If a distinction needs to be established between terrorism and organized crime, it would be that organized terrorism's illicit activities ostensibly focus on power or power sharing. Organized crime's activities seem to focus upon profit; though corruption of power must in many instances be factored in.

A major post September 11 attack concern is the impact upon public confidence. Public confidence in banks, and hence financial stability, can be, and has been, undermined by the adverse publicity that has resulted from the association, although perhaps inadvertent, of banks with terrorists' accounts. Some financial institutions and user friendly states are, for the most part, unwittingly functioning as links that enable intermediaries to transfer or deposit funds to be employed in exporting terrorism in all of its obscene forms. Money, including terrorist money, is attractive to financial markets. The systems are designed to make payments and transfer funds from one complex series of accounts to another.[15] Add to the mix the complexity of off-shore banking and correspondent accounts operating on September 11, as well as the underground "banking systems," and the fact that half of the approximately $550 billion in United States currency in existence is in the hands of foreigners, and further, that 90 percent of all $100 bills in circulation are held in foreign hands,[16] and one can better understand why the tracing of terrorist money is an increasingly difficult task requiring intense and complex management.

Through negligence and/or lack of diligence the failure to screen out undesirable customers results in a negative impact upon the integrity of banks and finance officers. Some well intentioned financial systems are undermined through unwitting association with the money managers of organized crime or organized terrorism.[17]

Weapons and procedures were and are available to governments, who in good faith elect to counter the threats posed by both organized crime and terrorism. One such weapon, focuses upon taking the illicit funds from the criminal. That weapon is now being applied world-wide.

International Emergency Economic Powers Act (IEEPA)

Within the United States, there are numerous legal weapons available to the government to assist in taking money from the terrorist. The goals of government are reflected in a recent government report, the *United States General Accounting Office Report to Congressional Committees on Combating Terrorism*.[18] This report was drafted prior to September 11 but released on September 20, 2001. Another important document is the *Report on Intelligence Authorization FY2002*.

Prior to September 11, the President had powers to act quickly. After September 11, the President did just that by invoking, among others powers, the International Emergency Economic Powers Act (hereinafter IEEPA).[19] IEEPA permits the Executive to identify and freeze the assets of foreign drug lords and terrorists. It also permits the Executive to apply sanctions to those who aid and abet.[20]

Anti Terrorism and Effective Death Penalty Act (ATEDP)

Another pre-September 11, 2001 weapon was enacted into law after the terrorist bombing in Oklahoma City Congress enacted the Anti-Terrorism and Effective Death Penalty Act

(hereinafter ATEDP Act).[21] The relevant provisions of the ATEDP Act authorize the Secretary of State to make findings of fact, based upon war and national emergency powers, that a targeted group is a foreign organization engaged in terrorist activity, i.e., activity that threatens the national security of the United States. Once labeled and announced, all bank accounts in the United States traced to that entity can be seized. Anyone who knowingly contributes financial support to the named terrorist group is subject to criminal prosecution. United States Courts[22] have been assigned a minor role; however they have not, to date, willingly accepted the rubber stamp role of clerk[23] and *National Council of Resistance of Iran v. Dept. of State*; the United States Supreme Court on March 5, 2001, refused to review a somewhat similar holding in the 9th Circuit: *Humanitarian Law v. Reno*.[24]

IEEPA First to be Employed

On September 23, 2001, the President issued an executive order blocking property exchange and prohibiting transactions with persons who commit, threaten to commit, or support terrorism. In so doing, the President signaled his intention to "declare war" (used in a political not a constitutional context) on illicit (terrorist) financial expenditures. Twenty-seven entities or persons were named. The President issued the executive order under the authority of IEEPA and the United Nations Participation Act.

The world has not been silent on this point; the Foreign Ministers of the leading economic nations agreed on September 25, 2001, to produce a coordinated plan to seize the assets of terrorist groups. Japan and The European Union, among others, have accelerated cooperation among nation states, especially in the arena of anti-terrorists legislation with a focus upon money laundering, banking and other money exchange centers supervision, arrest warrants

and surveillance.

Parochial preoccupation with national borders and national sovereignty has begun to give way to borderless search and seizure of persons and assets. The world-wide campaign against terrorism prompted by September 11, 2001, is defined in the President's September 23, 2001, Executive Order 132241and implemented in the United Nations Security Council Resolution 1373, as well as the NATO statements of September 12 and October 1, 2001. Full implementation of United Nations Security Council Resolution 1373 requires significant transnational counter-measures to combat organized [privatized] terror.

United Nations Security Council Resolution 1373

Security Council Resolution 1373 establishes binding obligations upon the 189 member states. It focuses upon an international security threat and a campaign to root out terrorists and terrorists assets. The language of Resolution 1373 is mandatory. The reporting back within 90 days has resulted in states adopting Anti-Terrorism Acts. The USA Patriot Act is the direct result of Resolution 1373. Organized efforts have increased as well. The International Monetary Fund, November 17, 2001 Communique speaks to matters involving international security and focuses upon implementation of Resolution 1373. The problems presented by the present cast of terrorists are basically matters of first impression. The action of the United Nations Security Council of September 28, 2001, adopting Resolution 1373, stated that the September 11, 2001 act of international terrorism was a threat to international peace and security. This was the first time such determination had ever been made.[25]

III

THE USA PATRIOT ACT 2001
AN ACT TO PROVIDE THE APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM.
THE FINDINGS

In order to extract financial resources from terrorist organizations, the United States targets businesses, front companies, charitable organizations, banks, and now, the underground money transfer systems, as well as correspondent banks, that potentially or in fact serve as a major source of funding for organized crime and terrorism. What makes the task so difficult is that some legitimate businesses and charitable organizations unintentionally commingle funds with contributions from terrorist front organizations. At present, simply distinguishing legitimate from illegitimate money sources is a formidable task. There is substantial evidence demonstrating that some Islamic charitable organizations have [in all probability] been "penetrated, exploited, and controlled by terrorists involved with al-Qaeda."[26] Islamic charitable organizations *accused* of having ties to al-Qaeda include – at this writing – multinational Gulf-based businesses that operate with multi-million dollar budgets at one end of the spectrum and small, tightly organized front cells at the other.[27] Listed in the United States President's Executive Order 13224 and its annex are Islamic charitable organizations that are accused of serving as covers for terrorist groups, groups that adopt innocuous names and co-opt legitimate causes. Terrorism engulfs many unsuspecting and well-intentioned individuals who support relief efforts for refugees through various charitable organizations. Unbeknownst to the donors, their monies may be diverted, ultimately ending up in the coffers of al-Qaeda.

Enter the USA Patriot Act 2001 A Response to Security Council Resolution 1373

It is the intent of the Congress of the United States that the Act serves as a `broad-brush'

aid to law enforcement officials in the search for and seizure of the assets of terrorists. The Act allots much wider statutory latitude to federal authorities who already possess *in rem* forfeit powers. The Act expands access to data and sharing of intercepted data among government agencies. "Today, we take an essential step in defeating terrorism while protecting the constitutional rights of all Americans," said the President during the signing ceremony.[28] The two concepts however, may be incompatible.

Implementation of programs now covered by the Act, prior to September 11, 2201, required congressional acknowledgment of the fact of past serious problems.[29] For example, Congress has long ignored bulk cash smuggling as a threat. In *United States v. Bajakajian*[30], for the first time in United States history, the Supreme Court held that the forfeiture of cash from bulk cash smuggling was prohibited under the Eighth Amendment prohibition against excessive fines. The Court found that neither the meager legislation nor the Constitution permitted an *in rem* forfeiture program where one of the so-called criminal acts in question was what Congress considered to be nothing more than a failure to declare at the border cash sums in excess of $10,000. [31] The bulk cash smuggling provision of the Act settles the matter in favor of preventing illicit bulk cash smuggling within or without the United States. Further, the Patriot Act expands forfeiture of assets when the assets are earmarked for terrorist organizations [nations will at time disagree to the designation "terrorist" to some politically active organizations]. The Act also enhances the powers of the Financial Crimes Enforcement Network and the Office of Foreign Assets Control. The Patriot Act coordinates closer cooperation through a policy coordinating committee made up of representatives from the Departments of Treasury, Justice, and State; the National Security Council; the Federal Bureau of Investigation; and the Central

Intelligence Agency. Executive Order 13224 also expands the work of the Foreign Asset Tracking Center developing as well, Operation Green Quest. The Act also focuses upon international cooperation and due diligence. There are provisions expanding long-arm jurisdiction over foreign money launderers and money laundering through foreign banks.[32]

The Act permits a federal judge or magistrate to issue a pen register or trap and trace order without specifying the service provider, leaving it to the law enforcement officer to insert the service providers as necessary to complete an investigation.[33] The order is valid anywhere in the United States.[34] An ancillary effect of this provision is that if there are challenges to the order, the challenge must occur in the jurisdiction where the order was issued. With little to gain, few service providers are likely to bring such a challenge.[35]

A troubling provision of the Act involves so-called knock and announce prior to execution of a search warrant. The Supreme Court has signaled its distrust of no-knock entries.[36] Knock and announce was established as a prerequisite to executing a search warrant. Except, of course, under exigent circumstances. In Section 213 the Act amends 18 U.S.C. § 3103(a) thus allowing federal law enforcement to enter without a homeowner's knowledge and to examine or copy papers and effects. The homeowner may not be made aware of such intrusion until weeks later. The problem is that it is not, on its face, limited to terrorists or terrorist activity. It can also apply to drug cases, tax or tax fraud cases, and in fact, any federal predicate crime appears to be included.

The Act permits enhanced surveillance by readopting the so-called "roving wiretap." Under the Act a warrant need not specify a single phone line, Any phone where the user is suspected of terrorism will suffice. The Attorney General has argued that roving wiretaps[37] do not

violate the Fourth Amendment because they do not eliminate the particularity requirements for search warrants; they "merely substitute particularity of person for particularity of place."[38]

The definition of "law enforcement officer" is amended to include federal law enforcement, national security, intelligence, national defense, protective, immigration personnel, and the President or Vice President of the United States when the issue relates to foreign intelligence. The Act also combines relevant portions of Title II, with the Foreign Intelligence Surveillance Act for purposes of domestic surveillance.[39]

The Act also authorizes interception of the contents of communications by persons deemed "computer trespassers." The interceptor must first obtain the permission of the owner or operator of the computer being unlawfully accessed. A computer trespasser is defined as a person who is not authorized to access a protected computer and, as such, has no reasonable expectation of privacy with regard to communications transmitted through the computer accessed, hence judicial oversight is not required. There must, however, be "reasonable grounds to believe that the content[s] of the computer trespasser's communications will be relevant" to a law enforcement investigation. This section is intended to provide for responses to cyberattacks that may be the work of organized crime or terrorists. Section 217 of the act also protects government from liability for warrantless wiretaps; however a caution: this provision does appear to protect from liability the service provider who has provided services or technical assistance to the government.

The Act expands the scope of subpoenas for records of electronic surveillance and amends existing law to authorize a subpoena for transactional records to determine the payment used by suspected terrorists in order to determine identities when persons are operating under

aliases.[40]

The Act also permits, though does not require, service providers to make emergency disclosure of electronic communications to protect life and limb. Thus, service providers could disclose their customers' electronic communications or records relating to such communications such as contents of stored mail and customer information. The provider must reasonably believe that an emergency involving immediate danger of death or serious bodily injury to any person requires disclosure without delay. Under preexisting law, the provider was not authorized to disclose non-content information, such as subscriber login records.

The Act amends the statutory suppression of the evidence rule under the 1968 Wiretap Statute that provides that illegally intercepted wire or oral communications cannot be used in court or in agency hearings.[41] The Act extends the statutory exclusionary rule to electronic communications and applies to both real time and stored communications.

Foreign Intelligence Surveillance Act of 1978[42]

The key impact of Title II is the amending of The Foreign Intelligence Surveillance Act of 1978 in a manner that reflects modern reality. Section 204 of the USA Patriot Act separates foreign intelligence surveillance from the criminal procedure protections afforded domestic wrong doers. The term "foreign intelligence"' means "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorist activities."[43] The term "foreign intelligence information" includes information about a United States citizen that concerns a foreign power or foreign territory and "that relates to the national defense or the security of the United States" or "the conduct of the foreign affairs of the United States." Therefore, when information about a United

States citizen's relationship with a foreign country or its government becomes available from a criminal investigation, that information is eligible to be disseminated widely as "foreign intelligence information."[44]

Investigatory authority is expanded in Section 204 of the Act by affirming the intelligence exceptions and disclosure of wire or oral electronic communications.[45] To this point, The Act grants federal agents expanded authority to conduct warrantless surveillance, provided that the primary purpose of the investigation is to obtain "foreign intelligence information."[46] The Act amends the criteria for FISA authority by "striking 'the purpose' and inserting 'a significant purpose'"[47] of the investigation, meaning any relationship of the investigation to foreign intelligence is sufficient grounds.

The Act also permits investigators to obtain, in a less complex manner, wiretaps for activity on the Internet by expanding the previously discussed "pen register" statute to include electronic communications and Internet usage. It also allows the collection of information that is more private than Internet Service Provider addresses, which are, it is argued, the Internet's equivalent of phone numbers. Additionally, Internet Service Providers must make their services more wiretap friendly, giving law enforcement the ability to capture pen register information or allowing the installation of Carnivore technology. Further, Section 209 treats voice mail messages as stored data subject to seizure under a search warrant not a wiretap order.

One concern is that when sensitive information from the investigation of criminal cases is disseminated to agencies with intelligence, military, and other national security responsibilities, risk that it will be deployed elsewhere is multiplied.[48] The Act includes a provision that is intended to guard against the expanded sharing of information from electronic surveillance. If the

government uses the electronic surveillance procedures of the FISA to monitor the conversations of a person and that information is disclosed without proper authority, under the Act the aggrieved person may have an action against and recovery of money damages from the federal government.

As a deterrent against "malicious" leaks, the Act includes procedures for administrative discipline. When a court or the appropriate agency determines that there is serious question about whether or not an employee willfully disclosed information without proper authority, disciplinary proceedings are initiated. If the agency head decides that discipline is not warranted, he or she must notify the Inspector General with jurisdiction over the agency and provide the reasons for the decision not to impose discipline. This is not new – civil and criminal sanctions for violations by individuals of improper disclosure were initially authorized under the electronic surveillance legislation in 1968 and again in 1978.[49] The Act does, however, change surveillance and intelligence gathering procedures for all types of criminal and foreign intelligence investigations, not just for terrorism investigations.[50]

The Act as well, amends 50 U.S.C. § 1804(a)(7) and § 1823(a)(7)(B). Currently, when an application is made for an order for electronic surveillance, it must be upon a written request to the F.B.I. Director, the Secretary of Defense, the Secretary of State, or the CIA Director. The request must certify that the purpose of the investigation is to obtain foreign intelligence information. The certification must be for an order against anyone that knowingly is engaging in espionage or terrorism and is not an agent of a foreign power. The Attorney General must personally review the order and foreign intelligence gathering must be the sole or primary purpose of the investigation. Law enforcement must constantly evaluate the investigation and the

courts ultimately determine whether this condition is met. Under the new rule, law enforcement has only to certify that the information gathering is a significant purpose of the investigation and a judge must review it. The provision is designed to expedite the issuance of orders for foreign information gathering, nevertheless the user friendly provision appears to have been misused by the F.B.I.[51]

Another controversial provision in the Act permits law enforcement to share information about foreign intelligence that is gathered during criminal investigations with specified law enforcement, protective, immigration, or national defense personnel when they are performing official duties. Currently, under the criminal code, it is difficult for law enforcement officials to share information (even when it is foreign intelligence information, including information from wiretaps authorized by the criminal code) with the intelligence community. Title II of the Act authorizes sharing of foreign intelligence information gathered by law enforcement in criminal investigation with those government officials who are intimately involved in transnational terrorism investigations. This would seem to also domesticate the C.I.A.

The Act lessens the government's burden by making it easier to subpoena business records. The revised law permits a national security letter to be issued when it is relevant to an authorized foreign counterintelligence investigation instead of the currently required certificate to obtain subscriber information and toll billing records of a wire or electronic communications service. The Act eliminates the showing of a nexus between the foreign agent and a possible violation of criminal laws, thereby decreasing the government's burden when pursuing investigations.[52]

In order to quell the fear of those who argue that the Act exceeds to an unacceptable

degree the values set forth in the United States Constitution such as right of privacy and protection against unreasonable search and seizure, there is a partial four-year sunset provision which applies to the expanded surveillance authorities under the FISA. However, the sunset provision is not universal within the Act.

The Act is troubling. It alters the relationship between law enforcement and intelligence agencies. Long before the current crisis, many agencies world-wide argued that there was justification for expanding authority specifically for counterintelligence to detect and prevent international terrorism. However, the greatest departure from past recommendations is the Act's authorization to share "foreign intelligence" from criminal investigations with "other" federal law enforcement, intelligence, protective, immigration, national defense, or national security personnel. For example under Section 203 of the Act "matters occurring before a grand jury.... when the matters involve foreign intelligence or country intelligence or foreign intelligence information" may be disclosed to agents of the CIA, FBI, Secret Service, IRS and OFAC to name just a few.[53] The authority to investigate United States citizens in counterintelligence investigations involving terrorism and spying activities would, most probably, not change as a result of the Act.[54]

The authority to disseminate "foreign intelligence" from criminal investigations, including grand juries and law enforcement wiretaps, appears to be an invitation to expand without special safeguards. There is, however, a provision to maintain a degree of judicial oversight of the dissemination of grand jury information. The National Security Act of 1947 had "cold war" safeguards drawing a sharp line between foreign intelligence and domestic law enforcement. The law, which established the CIA, states that the CIA "shall have no police,

subpoena, or law enforcement powers or internal security functions."[55] The Patriot Act in Title II seems to have voided this portion of the 1947 Act.

IV

TITLE III OF THE USA PATRIOT ACT

Originally intended as a separate statute amending the 1970 Bank Secrecy Act, Title III has become the center piece of the USA Patriot Act.[56] Title III is: The International Money Laundering Abatement and Anti-Terrorism Financing Act of 2001 (IMLAA). Title III amends the Bank Secrecy Act in numerous, complex ways. In doing so, some sections are self-executing while others such as section 352, require implementing regulations from the Department of Treasury. For example, interim rules promulgated by Treasury establish obligations not only for banks, but also for savings associations, credit unions, brokers, dealers and others. The Bank Secrecy's Act regulations concerning financial institutions are amended to insure increased and stronger due diligence by private banking as well as correspondent accounts. Strict "know your customer" requirements are now included. Enhanced reporting mandates and promulgates in house anti-money laundering procedures. Foreign bank correspondent accounts must now have an identifiable ownership of foreign banks maintaining correspondent accounts in the United States.

"Covered financial institutions" are subject to additional regulations, the regulations prohibit correspondent accounts of foreign "shell banks," enhance record keeping and reasonableness standards in ensuring that correspondent accounts are not employed by a foreign "shell bank." A shell bank is a correspondent account with no identifiable ownership report; it is defined as a foreign bank without a physical presence in any country. Physical presence is an

actual place of business.

It is the intent of Congress as expressed in Title III that banks and other financial institutions begin to practice "know your customer" with enhanced due diligence. If any jurisdiction or financial institution in or outside of the United States is a money laundering concern, the Secretary of the Treasury[57] will require any domestic financial institution or agency that opens or maintains an account, "payable-through account", or correspondent account to identify the customer who is permitted to use or conduct transactions through the account and to obtain information about the customer that is similar to the information obtained during the regular course of business in a financial institution.[58]

IMLAA sets forth jurisdictions, institutions,[59] and types of accounts and transactions that are of primary money laundering concern and authorizes the Secretary of the Treasury to acquire information regarding a suspect from any financial institution. Some of the jurisdictional factors that are considered include:

> (1) whether organized criminal groups, international terrorists, or both have transacted business in that jurisdiction;
>
> (2) the extent to which that jurisdiction or financial institutions operating in that jurisdiction offer bank secrecy or special regulatory advantages to nonresidents or non-domiciliaries of that jurisdiction;
>
> (3) the substance and quality of administration of the bank supervisory and counter-money laundering laws of that jurisdiction;
>
> (4) the relationship between the volume of financial transactions occurring in that jurisdiction and the size of the economy of the jurisdiction;
>
> (5) the extent to which the jurisdiction is characterized as an off-shore banking or secrecy haven by credible international organizations or multilateral expert groups;
>
> (6) whether the United States has a mutual legal assistance treaty with that jurisdiction, and the experience of the United States law enforcement and regulatory officials in obtaining information about transactions originating in or routed through or to such jurisdiction; and
>
> (7) the extent to which that jurisdiction is characterized by high levels of official or institutional corruption.[60]

The institutional factors considered are (1) the extent to which such financial institutions, transactions, or types of accounts are used to facilitate or promote money laundering in or through the jurisdiction; (2) the extent to which such financial institutions, transactions, or types of accounts are used for legitimate business purposes in the jurisdiction; and (3) the extent to which such action is sufficient to ensure, with respect to transactions involving the jurisdiction and institutions operating in that jurisdiction, that the purposes of this subchapter continue.[61]

Section 328 of the Act enlarges wire transfer provisions of the Bank Secrecy Act. IMLAA requires that the United States Attorney General and the Secretary of State encourage foreign governments to require the name of the original person in wire transfer instructions sent to and from the United States and other countries until the point of disbursement.[62]

IMLAA recognizes the high degree of usefulness of adequate records maintained by both insured depository institutions and uninsured institutions for criminal, tax, and regulatory investigations as well as for intelligence or counterintelligence activities.[63] The Act mandates the availability of these records to governmental agencies for investigative and/or counter-terrorism purposes.

Finally, bulk cash smuggling into or out of the United States is now a criminal offense.[64] The statute provides that whoever, with intent to evade a currency reporting requirement, knowingly conceals more than $10,000 in currency or other monetary instruments in the person's possession and transports, transfers, or attempts to transport or transfer such currency into or out of the United States will be punished under either or both criminal and civil liabilities.[65]

IMLAA also amends the definition of "financial institution"[66] and "money transmitting

businesses"[67] to include informal money transfer systems. Now, persons involved in the non-conventional financial market are also subject to mandatory records and reporting requirements of the Bank Secrecy Act.[68]

Non-Conventional Exchanges

Non-conventional financial institutions include underground banking. Underground banking systems are called, among other names, hawala or hundi.[69] Underground banking appears to be ideal for terrorists who want to transfer funds with virtually no record of the transaction.[70] The hawala system discretely moves funds around the world. Terrorists often use this age-old system because of the trust factor. The funds are moved by user friendly Hawala agents, a hawaladar.[71] Hawala emerged several centuries ago as a way for Asian traders to avoid being robbed on their routes.[72] Pakistan estimates that $2.5 billion flowed into Pakistan in 2001 year via hawala, as opposed to $1 billion via legitimate banks.[73]

Hawala works.[74] A person desiring to transfer money to another part of the world simply deposits money with a hawaladar.[75] Then, usually in about two or three days, the intended recipient can go to his local hawaladar and pick up the transferred funds, minus the hawaladar's fee.[76] (Sounds similar to the Black Market Peso Exchange as defined by the United States Custom Service in July, 1999.[77]) The process is quicker and cheaper than banks. Further, underground banking services parts of the world where banks may services are not readily available or not exist.[78] Major benefit to terrorists is that the Hawala system leaves virtually no paper trail; records are often kept in code and destroyed once the transaction is completed.[79] Hawala services functions in the United States, as well, usually in communities that have a significant South Asian population.[80]

Another non-conventional institutional institution is the money transfer shop In addition to Hawala, terrorists use other more familiar money transfer mechanisms to distribute money world-wide.[81] Money transfer shops have flourished in the last decades due to the large number of immigrants desiring to send cash home.[82] Money transfer businesses like Western Union and MoneyGram facilitate the transfer of funds around the world in as little as 15 minutes.[83] Western Union is the largest regulated money transfer business, with 124,000 agencies worldwide having completed 109 million transfers in 2001.[84] Those transfers amounted to over $40 billion. No bank account or background check is required, and identification is often unnecessary unless the transfer exceeds $1,000.[85] The September 11 terrorists received transfers via Western Union about a year before the attacks.[86] Before September 11, 2001, several of the terrorists used Western Union to wire $15,000 to a person in the United Arab Emirates.[87] The money transferred just days before the attacks was apparently the unspent portion of the funds used to finance the attacks. Western Union also has an agent in the UAE that operates out of an al Baraka exchange storefront.[88]

Off-Shore Banking

Although al-Qaeda may have curtailed its use of banks to move money throughout the world, banks continue to play an important role in the financing of terrorism.[89] Off-shore banking centers are considered by some to be a heaven and a haven for terrorists who are looking for a place to store large sums of money while planning how to use it.[90] Some though certainly not all of the off-shore banking centers[91] have lax regulations.[92] Furthermore, some off-shore centers have correspondent banking relationships with many of the world's largest banks.[93] These are conclusions of IMLAA. The Act now mandates strict regulations with respect to correspondent

banking. Nevertheless, unregulated banks can, it would seem, still be "user-friendly." This is why IMLAA focuses in upon banks licensed in "user friendly" states designated: (i) non-cooperative with international money laundering principles or, (ii) warranting special measures due to money laundering concerns.[94]

It is alleged that al-Qaeda moves its money through a network of under-regulated banks, and then when the source of the money is sufficiently disguised, moves it into safer G-7 financial institutions.[95] After the terrorists route their money through these under-regulated systems, often in accounts registered to shell companies or legitimate businesses, the money appears to be clean.[96]

Investigators report that bin Laden maintained accounts at the discredited Bank of Credit and Commerce International (BCCI).[97] The United States detained one person after he donated $2 billion to al-Qaeda. He was said to be a former director of BCCI.[98]

The questions remains whether the Act will be adequate to effectively counter money laundering and terrorism.[99] The Act has now placed more restrictions than ever before on domestic financial institutions and/or agencies that open or maintain private bank accounts in the United States and for foreign international banks to do away with secrecy rights, requiring these foreign international banks to identify each customer who accesses the account under similar Know Your Customer standards that are used for United States customers of United States banks. In addition, the Act requires identification and authentication of original persons in wire transactions.[100]

Consider that al-Qaeda wired large sums of money to terrorists' accounts in Florida.[101] The money, it is alleged, was then used to purchase flying lessons at numerous flying schools.[102]

The events simply point to the fact that governments face many obstacles in identifying, locating, and seizing terrorists funds. Current money laundering detection techniques have been geared toward the detection of large sums sent regularly or frequently.[103] Terrorist funding, on the other hand, seems to be transmitted in much smaller amounts and on an irregular or infrequent basis.[104]

Another major problem is that some countries' entire banking industry is built on strict bank secrecy.[105] While many countries in the past have opposed stricter regulation and greater financial transparency recent events, have caused them to recognize the impact upon world order, of continued strict bank security.[106] International cooperation has increased exponentially since September 28, 2001.[107] Some countries, however, are still reluctant to release information about some organizations designated by the United States as terrorists.[108] The reality is what constitutes a terrorist group to United States authorities might not be so designated by the European Union or others. The matter, nevertheless, is global in nature, the concerns are not local. One nation cannot successfully "go it alone".

Add to the mix the fact that prior to September 11 the procedures for detecting and reporting suspicious transfers did not work as effectively as envisioned. The suspicious activity reports sent to understaffed agencies sometimes would take a week or longer to process and in that amount of time the money may already have been put to use.[109] If nothing else is clear, it is understood that terrorists generally have a wealth of funding sources to draw from in order to finance their terror.[110] Thus, what is important under IMLAA is the emergence of enhanced due diligence policies and controls, new predicate offenses, expanded forfeiture programs, strict controls over correspondent bank accounts, long arm jurisdiction over foreign money launderers,

and increased civil and criminal penalties.

Other Provisions

There are additional provisions in the Act which invoke controversy.

Title IV of the Patriot Act defines terrorism in Section 411 and identifies terrorist organizations in Section 413 in the name of national security which permits detention of suspected non-citizen terrorists. Further this provision limits judicial review.

Title V: In addition to requiring closer cooperation and coordination among law enforcement as discussed previously, Section 507 permits disclosure of educational records under the National Education Statistics Act. The purpose is to aid in the investigation and prosecution of terrorists. Questions of privacy are not dealt with, presumably leaving the matter to judicial review.

Title VIII: Defines the federal crime of cyberterrorism and focuses upon terrorist attacks. Title VIII also expands upon the concept of terrorism, terrorists, those harboring terrorist and seizure of terrorists assets, foreign or domestic Title VIII encourages *in rem* seizure of all assets derived from, involved in, or used or intended to be used to commit any act of domestic international terrorism . . . against the United States citizens or residents of the United States, or their property." Section 806 is significant in that it places terrorists in the same category as that of organized crime.

Finally, the Act reaffirms and adds to the Critical Infrastructure Protection Act of 2001[111] as well as the Crime Identification Technology Act of 1998.[112] What is noticeably in short supply in the Act are provisions recognizing the role of Article III of the United States Constitution, that is the role and scope of United States federal courts, in the fight against terrorism. The Act

expands the numbers for the secret federal court which meets to approve or disapprove warrants requested by federal law enforcement.

VI

SELF PRESERVATION

A society has a duty to protect its own existence. The majority in the society have the right to follow their own moral convictions in defending their legal, social and economic environment from changes or assaults it opposes. Within the United States these principles implicate constitutional values. For example, prejudice based upon appearance is an unacceptable, emotion based harm (I do not like you because you are Muslim). It is unacceptable unless a factual basis for the prejudice emerges. (Privitation of terrorism impacts domestic security). Otherwise, prejudice will not be formalized into law, and indeed the law must discourage its circumvention in the name of expediency. The point is, government intrusion as well as moral conviction must, short of actual war (and in some instances defacto war), be tested within the context of constitutional credentials.

It is argued that the United States' policies established to fight terrorists stem from a desire to protect commercial and economic interests and to ensure market and social stability globally. At certain junctures since September 11, 2001, the goals and policies are at odds with notions of constitutional protections. Each day terrorists became more and more proficient in their illicit design and more world wide in scope. Just as one expects protection for arcane systems of commerce, the new challenges, and threats, appears to governmental authorities to be growing beyond Constitutional and human rights parameters.

Self Preservation and Privacy

Privacy is a major concern. For example, a computer source codes which is a language that speaks and functions in similar ways to other symbol systems. Just as other languages are combinations of letters and sounds to be written or spoken in order to convey meaning, so too is a computer source code a construct of human engineering. The debate surrounding government's insistence upon an encryption key (or keys) to protect national security pits privacy versus governmental self-preservation. The battle lines have become a synthesis of international concerns about the borderless technologies and its impact upon matters of privacy as well as governmental self-preservation.[113]

The internet changes "database privacy,"[114] *i.e.* personal data, in that it eases access to numerous databases.[115] These databases may have previously been accessible, but only rarely, whereas now accessing transnational databases is as easy as pushing a computer key.[116] The issue is merely a quantitative one, but when the information is a transfer of military secrets or matter of security interest, legal concerns will be generated, indeed are being generated, where none were previously warranted.[117] Terrorists and the internet have impacted constitutional concerns about privacy. Qualitative privacy is no longer a reality.[118]

Terrorism conjures up the notion that conceptions of privacy are dependent upon society's technology. This notion has at its core the belief that the internet is not changing views of how privacy may be invaded, but how it is shaping the very idea of what expectations of privacy are or have become, especially within the context of the Act. Prior to September 11, 2001 privacy was measured by a "reasonable expectation of privacy standard."[119] Since the United States Supreme Court in United States v. Miller[120] held that there is no expectation of privacy in banking records, the question of retaining a "zone of privacy" around informational

data remains unanswered,[121] and therefore strengthens the Act's commands of Title III. Whether an expectation of privacy exists in electronic commerce transactions, electronic data collection, storage, and dissemination may ultimately depend upon how technology, the internet in particular, has been transformed and molded by terrorists organizations and user friendly states.[122]

VII

ROLE OF THE COURTS

As the changes in the current legislation are implemented, it remains to be seen whether the changes will withstand constitutional challenges in the United States or indeed whether judicial review will survive jurisdictional challenges when based upon matters involving national security. Past examples assist in answering these questions.

FISA, Challenged and Sustained

For example, the constitutionality of the Foreign Intelligence Surveillance Act has been judicially challenged and sustained on several grounds.[123] But it is important to note that first and foremost, the courts assumed jurisdiction. Those cases along with the lower court analysis of constitutional challenges and procedures support the conclusion that if the United States Supreme Court determines constitutional difficulties exist within portions of any legislation presenting a federal constitutional issue, it will not hesitate to rule. Even within the context of international terrorism, courts rule.[124] Surveillance and national security as developed in the FISA Act, are good examples. Generally, United States courts have consistently held that both the electronic surveillance and the physical search provisions of FISA are valid. In cases such as *United States v. United States District Court*,[125] the Supreme Court has concluded in dicta, since it was a

decision prior to FISA, that foreign intelligence surveillance satisfies the constraints the Fourth Amendment places upon surveillance conducted by the government. The Court noted that the standard of probable cause necessary to justify surveillance to protect national security is not necessarily the same standard as that for general criminal warrants.

Lower courts have also addressed the argument that the need for foreign intelligence surveillance does not justify an exception to the warrant requirement. In *United States v. Pelton,*[126] the Court of Appeals held that FISA has numerous safeguards that provide sufficient protection under the Fourth Amendment. The court recognized that "[t]he governmental interests in gathering foreign intelligence are of paramount importance to national security; and may differ substantially from those presented in the normal criminal investigation."[127] However, even given these differences, unlawful government intrusions upon personal civil liberties are prevented by the independent judicial review mandated by FISA and the limitations placed on the exercise of FISA powers. The courts have found that the use of FISA against terrorist organizations has been for the most part, constitutional. Innovative techniques suppress and deter terrorist are being developed including tracking terrorists and their illicit money. Changing technology continues to be addressed in the courts and it is not enough to simply argue that new techniques are required for rapid response to terrorist threats.[128]

The questions remains whether the Act will be adequate to effectively counter money laundering and terrorism.[129] The Act has placed more restrictions than ever before on domestic and foreign financial institutions and/or agencies that open or maintain private bank accounts in the United States.[130]

A recent Supreme Court case, *Kyllo v. United States*[131] although not dealing directly with

national security threats, is significant. *Kyllo* involves domestic treatment of the Fourth Amendment. The Court in *Kyllo* attempts to reconcile law enforcement with new and complex technology. The focus of the Court since, at least 1967, has been a person's expectation of privacy and whether society is prepared to honor that expectation as being reasonable in nature.[132] In *Kyllo* the majority concluded that an advanced technology, such as the Agema thermovision 210[133] if it is able to reveal details of an intimate nature from without, must give way to the Fourth Amendment demand for privacy unless the sense-enhancer device has been in general use exploring other intimate details without physical intrusion. If it has not been in general use, it is presumptively unreasonable. If it is in general use, for national security purposes the *Kyllo* Court appears prepared to permit domestic invasions without a warrant as well. The critical term is national security and whether government has successfully made its case in each individual instance.

Kyllo would seem to allow "countervailing technologies that defend against government surveillance . . . . as they improve and become more widespread, offset the privacy-threatening effects produced by the disposition of surveillance technology into general use."[134]

There is additional help in understanding just how the federal appeals courts will respond to the USA Patriot Act. Consider, for example, 8 U.S.C. § 1189 which empowers the Secretary of State to designate a foreign organization as terrorist if the Secretary finds that the organization is: 1) foreign; 2) engages in terrorist activity (as Congress had defined it); and 3) threatens the security of the United States,[135] then the ramifications of such a designation would permit the government to, among other things, freeze the organization's assets.[136] Should such designation by the Secretary be subject to review by the courts? Two recent cases illustrate the historical role

the courts serve where threats to national security are at issue.

People's Mojahedin Organization of Iran v. United States Dep't. of State (hereinafter Mojahedin) and National Council of Resistance of Iran v. United States Dep't. of State[137]

In *Mojahedin*, although the court took jurisdiction, the court did recognize its inability to gauge the accuracy of the facts the Secretary of State compiled as an "evidentiary" record regarding terrorist designation.[138] The fact is, unlike other run-of-the-mill administrative proceedings, in *Mojahedin* there was no adversary hearing, no presentation of what courts and agencies consider to be "evidence," and no advance notice to the entity affected by the Secretary's internal deliberations.[139] Because the matter involved a question of national security, the Secretary needed only to accumulate information on the targeted and terrorist organization.[140]

National Council of Resistance of Iran v. United States Dep't. of State, [hereinafter NCRI]

In NCRI, two organizations, the National Council of Resistance of Iran (Council) and the PMO petitioned the district court for review of the Secretary's designation of them as terrorist organizations.[141] The *NCRI* court determined that in this case, unlike in the *Mojahedin* case, the groups designated as 'terrorist' were denied process rights since they had acquired property in the United States (in the form of a small bank account) that the court said was placed in jeopardy by government intervention.[142]

The *NCRI* court accepted the Secretary's conclusions that the Council was merely an alias for the PMO and lumped these two organizations together as one before the court set out to arbitrate a reasoning which created due process rights for the organization.[143]

Before the Secretary of State designates an organization terrorist, he or she must notify specific members of Congress by classified written communication. The designation becomes

effective seven days later.[144] The *Mojahedin* court, as noted, rejected the PMO's and the LTTE's argument that the United States Constitution's Fifth Amendment Due Process Clause prohibits the government from condemning organizations without giving them notice and an opportunity to be heard.[145] The court recognized that the statute's "administrative record" requirement supporting the Secretary's designation was unlike the normal "run-of-the-mill" administrative proceedings of United States agency law.[146] It remained for the court to determine what substantial support[147] the Secretary would need in order to properly designate a group as 'terrorist'.[148] The 'administrative record', which a given petitioner would attack for insufficient or unsubstantiated accusations, can have classified materials not available for public discourse or review[149] or nothing more than news reports, Internet information, third-hand accounts and other hearsay which have not been subjected to any type of adversarial examination.[150] The court recognized an issue of balance of power.

Balance of power issues, such as the scope of judicial review or the discretion accorded to the executive in taking action against suspected foreign terrorist organizations, are sources of great concern to the courts.[151] If a court, upon judicial review, invokes a 'minimal' interpretation of the statute and the requirement that the Secretary compile a record that 'substantially supports' the terrorist designation, there is the possibility that such an interpretation would leave limited room for judicial review.[152] The argument is that if the court's only function is to decide whether the Secretary simply had enough information to make his or her designation, then the Secretary would have 'broad and unfettered' discretion in the fact-finding process, immune and isolated from judicial scrutiny.[153] The court would function as a mere "rubber-stamp" of the Secretary's actions, thereby allowing the reputation of the judiciary to be "borrowed by the political branches

to cloak their work in the neutral colors of judicial action."[154]

However, if courts were to take a more stringent interpretation of the statute, it would perhaps serve as an impediment to the efficiency and strength of the Secretary's determination. Arguably, it would undermine the very power of the Executive Branch, creating a precedent backlog of cases where the Secretary's findings are overturned by actively maximus courts, resulting in the judiciary's undertaking unnecessary detective work of suspicious executive decisions, in the very sensitive political arena of foreign terrorism (an area in which the judiciary lacks expertise). After the events of September 11, 2001, it is unlikely that the courts will be second guessing and engaging in critical reviews of the Secretary's designations.[155]

The *Mojahedin* court undertook the former 'minimal' approach, according a hands-off approach to the Secretary's findings.[156] The court took the sort of interpretation we will probably see much more of in the future. The *Mojahedin* court stated that:

> We reach no judgment whatsoever regarding whether the material before the Secretary is or is not true. . . . The record consists entirely of hearsay. . . . Her conclusion might be mistaken . . . something we have no way of judging.[157]

The statute was meant to give the judiciary the opportunity to analyze "terrorism" in a legal context.[158] In legal contexts, courts are used to the rules of evidence, the procedures of administrative practice, and the constitutional demands due process or notice. However, the concept and philosophy of ‘terrorism’ is usually not a legal one, but a political or religious one, rooted in desire and ideology, not necessarily money or legality.[159] As such, the politics and ideologies that are inherent in ‘terrorism’ are the paper trails that will lead the evidentiary way to the rule of law. The "terrorist battle" are fought on diplomatic and political fronts through treaties and other the fule of law intrudes by way of judicial review.[160]

Of course, the issue is not whether a terrorist organization will be brought to justice, but rather what rights they will be afforded. What organizations are entitled to the full range of United States Constitutional rights? It seems that foreign organizations that have unclear mission statements, that are engaged in undermining political schemes around the world, and that are in many ways linked to 'terrorism' are by their very definition unconventional; however if domestic links are apparent then there is entitlement to most conventional constitutional rights. Here, the standard of evidence relied on by the Secretary, and eventually a reviewing court, is what is at dispute, that includes the issue of procedural rights for foreign organization engaged in illicit activity outside the territorial limits of the United States. [161]

The LTTE and the PMO argued that they had been denied due process of law partly because the Secretary's designations had the effect of making it a crime to donate money to them.[162] However, the *Mojahedin* court pointed out that these groups did not have any United States ties including ties to financial institutions holding any of their property.[163] From the facts as presented in a non-criminal context, neither the LTTE or the PMO had any presence in the United States.[164] Thus, the court stated that a foreign entity without property or presence in the United States has no constitutional rights under the due process clause or otherwise.[165] Alien organizations are to receive constitutional protections only when they have come within the territory of the United States and developed 'substantial connections' within the country.[166] The *Mojahedin* court considered the rights which the LTTE and PMO enjoyed purely statutory.[167] These organizations had the right, for instance, to seek the court's judgment about whether the Secretary followed statutory procedures or whether she made the requisite findings, or whether she assembled a record which substantially *supported* her findings.[168] However, one of the

statutory findings which the Secretary is duty bound to make is whether the terrorist activity by the alien organization threatens the security of the United States, that conclusion is not subject to judicial review.[169] It is a political judgment reserved for the foreign policy expertise of the Executive, a judgment call beyond the aptitude, facilities, and responsibilities of judicial inquiry.[170]

The *Mojahedin* court stated that courts do not have to *assume* whether the Secretary was right or wrong,[171] only whether the Secretary had a quantitively adequate record upon which to rely (the minimalist approach).[172] This ruling is rooted in the idea that the appeals courts are designed to review judgments.[173] In the realm of administrative decisions, the courts are not to engage in the choice of deciding whether the agency engaged in the "right-result" or the "wrong reason."[174] The court's function is to remand the case back to the agency if deemed necessary to adjust its reasoning or alter its result.[175] The *Mojahedin* court was content with the minimal role that Congress intended within the national security context.[176]

In order for a foreign entity to obtain constitutional protections under due process or otherwise, that entity must have come within the territory of the United States and developed "substantial connections" with the country.[177] The court's main task is to judge [178] whether the Secretary had enough information upon which to rely for her designation.[179] But it is still left to the court to determined what "substantial connections" an organization needs to have in the United States in order to be afforded due process.[180] This is the importance of the *NCRI* case.[181]

The *NCRI* court focused upon whether the Secretary, "on the face of things," had enough information before her to conclude that a particular organization is terrorist.[182] Thus, the dynamic of judicial review in the "foreign organization" (civil) context is reduced to a

quantitative judgement of "how much" information the Secretary has relied upon rather than a qualitative judgement of "what kind" of information was relied upon.[183] The *NCRI* court focused its rationale on aspects of 'designating' that were not dealt with in the *Mojahedin* case.[184]

The *NCRI* court concluded that the Secretary's designation of the Council as an "alias" for the PMO was 'substantially supported' by the record and was neither arbitrary, capricious, nor otherwise unlawful.[185] The ramification of the *NCRI* court approving the Secretary's finding that the Council was a mere cover or alias for the PMO may have actually found more rights available than the *Mojahedin* court was willing to concede.[186]

'Constitutional presence' in the United States as found by the NCRI Court was sufficient for the court to grant the petitioners more rights than the petitioners were given in *Mojahedin*. The *NCRI* re-assessed the PMO's presence in the United States by claiming that although the PMO had not established a constitutional presence by 1997, it had established a presence by 1999, along with a record.[187]

The controversy was whether the Council had actually developed the 'substantial connections'[188] necessary to characterize a presence in the United States.[189] The *NCRI* court rationalized its decision by engaging in a review of several cases, dissecting and compartmentalizing the legal English vernacular into critical adverbs and nouns.[190] The court's interpretations of these prior cases and its reasoning came full circle. After having reviewed the entire record, the PMO had sufficient 'presence' in the United States to grant it constitutional rights.[191] Further, because the Council was merely the PMO's alias, it also had a right to Fifth Amendment due process.[192]

The court in *NCRI* ignored the fact that in dealing with 'foreign' or 'alien' organizations,

the United States has frequently exercised its inherent powers of external sovereignty, independent of the grants of the Constitution.[193]

The *NCRI* court escaped the *Sovereign v. Constitution* dilemma[194] by noting that because neither the Council nor the PMO are "governments," but merely "organizations," the Secretary's argument and authority that the United States should deal with foreign organizations through sovereign contexts, instead of constitutional ones, has no weight. The Patriot Act soon to follow would seem to take issue with the court's conclusion.[195]

The *NCRI* court concluded that the Secretary has given the court no reason not to award a "pre-deprivation" due process hearing.[196] The court seemed to take the position that 'national security'[197] was a question of 'what' kind of hearing the petitioner's should get as opposed to 'when' they should get it.[198]

In the end, at least according to the *Mojahedin* and *NCRI* cases, a given foreign organization being considered by the Executive Branch as terrorists thus subject to civil sanctions could arguably expect the following rights:[199]

1) If the foreign organization has some form of property interest in the United States (perhaps a small bank account or even a closet-size office with a telephone and chair would suffice), they are entitled to the constitutional rights of Fifth Amendment due process which includes:
   – Pre-deprivation notice of unclassified evidence pointing toward the organization in question as 'terrorist' (unless the Secretary can prove a particular need or urgency to not give early notice).
   – The opportunity to present (at least in written form) evidence which can rebut the administrative record or negate the 'terrorist' proposition.[200]

2) If the organization cannot prove some sort of property interest in the United States, it will not be afforded Fifth Amendment due process rights and will at best receive a post-designation notice.[201]

The point is that reasonable measures to protect against international terrorism implicates

all three branches: the executive, legislative and judicial, as well as the International community.[202]

VIII

CONCLUSION

Overall, the USA Patriot Act is designed to support law enforcement in addressing complex issues regarding the role of money laundering, asset forfeiture, intervention into foreign affairs, and control of complex technology in terrorism. The Act is not intended to implement a due process model of constitutional adjudication. It is instead a crime control model, a model which receives its signals from modern United States Supreme Court jurisprudence. The President speaks in terms of a "War on Terrorism." This is, however, an "undeclared" war. The President suggests that this "war will require patience, determination, and resolve. Judicial review and world-wide concerns cannot be ignored. Judicial review is constitutionally mandated where constitutional issues emerge. World wide input is reflected in the United Nations Charter, as well as UNSC 1373. The traditional role of the United States federal judiciary is in part, to focus upon law enforcement and ensure that any attempt, even temporary, at derailing legitimate constitutional human rights freedoms is itself considered an affront to democratic values.[203] The traditional Constitutional role cannot be eroded by fear or "instant" fixes.

Although a society has a duty to protect its own existence, the majority in the society have the right to follow their own moral convictions in defending their social environment from assaults from within or without, and to ensure that their society works successfully. These concepts must continue to include constitutional and transnational values. It is unacceptable to infringe upon and diminish these values unless a tested factual basis for infringement emerges.[204]

It is not adequate enough to simply formalize into law through speeches to user friendly audiences, alterations to human rights values. Governmental intrusion must be tested within the context of compelling credentials.

ENDNOTES

1. *See* http://thomas.loc.gov/cgi-bin/query/C?c107:/temp/nc107qsOTGL. *See also* Bruce Zagaris, *United States Enacts Counterterrorism Act with Significant New International Provisions*, 17 INTERNATIONAL ENF. LAW REP. 522 (Dec. 2001).

2. Allison L. de Cerreno, Sec. 208 of the Patriot Act Walking a Fine Line Between Security and Fee Exchange of Scientist and Knowledge, available at http://members.nyas.org/events/policy/pol_01_1023.html. See Congressional Authorization Public Law 107-04, 116 STAT. 224 (2001)

3. Jim McGee, *An Intelligence Giant in the Making: Anti-Terrorism Law Likely to Bring Domestic Apparatus of Unprecedented Scope*, WASH. POST, Nov. 4, 2001, at A4. As to the impact of Title III, *see, for example, United States v. Swiss Amer. Bank, Ltd*, 116 F. Supp. 2d 217 (D. Mass 2000) and resulting impact of Sec. 317 of the USA Patriot Act. *See* Bruce Zagaris, *United States Appellate Court Disallows United States Jurisdiction Over Offshore Bank*, 18 INT'L ENF. LAW RPT. 103, 105 (March 2002).

4. President George W. Bush, Address at the White House signing of the USA Patriot Act of 2001, Oct. 26, 2001, *available at*: http://www.pbs.org/newshour/bb/terrorism/bush_terrorismbill.html.

5. PETER L. BERGEN, HOLY WAR, INC. (Free Press 2001). *See also*, *How the USA-PATRIOT Act Limits Judicial Oversight of Telephone and Internet Surveillance*, American Civil Liberties Union Freedom Network [hereinafter *Judicial Oversight*], available at http://www.aclu.org/congress/1102301g.html.

6. History of Terrorism, available at wysiwyg://4http://www.terrrorismfiles.org/encyclopedia/history_of_terrorism.html.

7. Martin Walker, A Brief History of Terrorism, available at http://www.eurunion.org /magazine/0110/p.26.html.

8. *Id.*

9. Peter Bergen, *supra* note 5.

10. *Id.*

11. Kurt Eichenwald, *Terror Money Trail Hard to Block*, NEW YORK TIMES, Dec. 10, 2001, at A-1; *see also* BERGEN, *supra* note 5.

12. *Id.*, at B-4. See also Comment, Responding to Terrorism: Crime, Punishment and War, 115 HARV. L. REV. 217 (2002).

13. Niall Ferguson, *Clashing Civilizations or Mad Mullahs: The United States Between Informal and Formal Empire in the Age of Terror*, 121 (Stobe Talbott and Nayan Chana ed.) (Basic Books 2001).

14. Martin Walker, *supra* note 7. *See also* Kurt Eichenwald *supra* note 11.

15. Christopher Byron, *Terrorists, Dollars and A Tangled Web* available at, www.msnbc.com/news/63212.asp.

16. *Id.*

17. *Id.*

18. United States General Accounting Office, *Combating Terrorism, Selected Challenges and Related Recommendations* (GAO 01-822), Sept. 20, 2001.

19. 18 U.S.C. § 1831 et seq (1996).

20. *See*, Kurt Eichenwald, *supra* note 11.

21. 8 U.S.C. § 1189 (1999).

22. People's Mojahedin Organization of Iran v. Dept. of State, 182 F.3d17 (D.C. Cir 1999).

23. National Council of Resistence of Iran v. Dept. of State. See also All Matters Submitted to the Foreign Intelligence Surveillance Court, Memorandum Opinion, May 17, 2002. (Docket 02-429251 F.3d 192 (D.C. Cir. 2001).

24. Humanitarian Law v. Reno *See* www.ceq.uscourts.gov/web/newopini... e30bab07f8e88256927007af33d? (no. 98-56062).

25. *See* http://usembassy.state.gov/tokyo/wwhse0840.html. Text: U.S. Report to UNSC on Counter-Terrorism Measures.

26. *See* Kurt Eichenwald, *supra* note 11 at B-4.

27. *See generally* Eichenwald, *supra* note 11, and BERGEN, *supra* note 5.

28. *Generally EFF Analysis of the Provisions of the USA PATRIOT ACT That Relate to Online Activities* (Oct. 31, 2001) [hereinafter *EFF Analysis*], available at: wysiwyg://4//http://www.eff.org/Privacy/s...s/2001103/_eff_usa_patriot_analysis.html.

29. *See* Sec. 371, USA Patriot Act. No. 10 U.S. Code, Dec. 2001: Cong. E. Adm. News pp. 272-402.

30. 524 U.S. 321, 118 S.Ct. 2028, 141 L. Ed. 2d 314 (1998).

31. *See generally* Comment, Excessive Fines Clause, 112 HARV. L. REV. 152 (1998).

32. *See generally EFF Analysis*, *supra* note 28. *See also* Congressional record: October 25, 2001 (Senate) (pages S10990-S11060) [hereinafter *Congressional Record*]. From Congressional Record online via GPO Access [wais.access.gpo.gov.] [DOCID:cr25oc01-91].

33. *How the USA-PATRIOT Act limits Judicial Oversight of Telephone and Internet Surveillance*, American Civil Liberties Union Freedom Network [hereinafter *Judicial Oversight*] available at http://www.aclu.org/congress/1102301g.html.

34. *Id.*

35. *Id.*

36. *Wilson v. Arkansas,* 514 U.S. 927, 115 S.Ct. 1914, 131 L.Ed.2d 976 (1995) and *Richards v. Wisconsin*, 5 2d U.S. 385, 117 S.Ct. 1416, 137 L.Ed.2d 615 (1997).

37. 18 U.S.C. § 1 (2001). Section 206, Roving Surveillance Authority under the Foreign Intelligence Surveillance Act of 1978.

38. Tracey Maclin, *On Amending the Fourth: Another Grave Threat to Liberty*, NAT. L. J., Nov. 12, 2001, *available at* http://www.law.com.

39. See Title II, *supra* note 29 at §§ 201-206.

40. *Id.*

41. 18 U.S.C. § 2515 (1968).

42. 50 U.S.C. § 1801 (1978).

43. *See generally* TITLE VIII. *See also* Fact Sheet 9: *Wiretapping/Eavesdropping on Telephone Conversation*, Utility Consumers' Action Network, March 1993/Revised August 2001; Bruce

Zagaris, *Counterterrorism and Economic Sanctions*, 17 INT'L ENFORCEMENT LAW REP. 480 (Jan. 2002).

44. *Id.* *See* for example the provisions of the Economic Espionage Act of 1996, 18 USC § 1831-1839.

45. 50 U.S.C. § 1801 (1978).

46. *Id.* at § 1801(c).

47. *Supra* note 45.

48. *Congressional Record*, October 25, 2001 (Senate) pp. § 10990 - § 11060) (hereinafter: *Congressional Record*).

49. *See generally* United States v. United States District Court, 407 U.S. 297, 92 S.Ct. 2125, 32 L.Ed. 2d 752 (1972).

50. 50 U.S.C. §§ 1802 and 1805(e) (1991).

51. *See* Stephen Dycus, Arthus Berkey, William Banks and Peter Reven-Hansen, *National Security Law* 455-474 (Little Brown1990).

52. *See:* In Re Matters Submitted To The: Foreign Intelligence Surveillance Court, Memorandum Opinion filed May 17, 2002 (Docket 02-429). *See also*: Stefanie Olson, Patriot Act Draws Privacy Concerns, CNET News.com. Oct. 26, 2001. http://news.cnet.com/news/0-1005-200-7671240.html

53. *See* USA Patriot Act § 203 (2001).

54. *See* the Anti-Terrorism and Effective Death Penalty Act of 1996, 8 UCS § 1189.

55. The National Security Act of 1947 (50 U.S. C. § 403(d)(3)).

56. *See* Michael Zeldin and Edward Rial, *Anti-Money Laundering, USA Patriot Act*, National Law. Jo., Monday, May 6, 2002 at A-18.

57. Section 311 amending 18 U.S.C. § 5318A.

58. Michelle Cottle, Easter Union; Hawala v. The War on Terrorism, The New Republic, Oct. 15, 2001 at 38-40.

59. 31 USC 5312 broadly defines "financial institution." *See also* Michael Zeldin and Edward Rial, *supra* note 56.

60. *See* Bruce Zagaris, *U.S. Enacts Counterterrorism Act with Significant New International Provisions,* 17 INT'L ENF. LAW REPORTER 522-526 (Dec. 2001).

61. *Id.*

62. *See* also Section 314 which requires the Secretary of Treasury to issue regulations encouraging information sharing among financial institutions, regulators, and law enforcement.

63. Further, Section 315 expands the list of specific unlawful activities considered to be crimes under 18 U.S.C. § 1956(c)(7) for money laundering.

64. *See* United States v. Bajakajian, 524 U.S. 321, 118 C. Ct. 2028, 141 L. Ed. 2d 314 (1998).

65. *See* 31 U.S.C. §§ 5316 and 5372 (Suppl. 2001).

66. Amending 31 UCS § 5312 (a)(2)(R).

67. Amending 31 U.S.C. §5330(d)(1)(A).

68. Also amending 31 UCS § 5312(a)(2)(R).

69. Sapra India Bulletin Article, Underground Banking and National Security, www.subcontinent.com/sapra/bulletin/96feb-mar/si96038.html visited 5/16/02.

70. Michelle Cottle, *supra* note 58.

71. *Id.*

72. *Id.*

73. *Id.*

74. Katherine Macklem, *Follow the Money,* MADEAN'S, Oct. 22, 2001, at 62.

75. *Id.*

76. Cottle, *supra* note 58.

77. *Id. See also* United States Department of the Treasury, *FinCEN Advisory*, Issue number 9, November 1997.

78. Tarik M. Yousef, *Terrorist Financing Mechanisms,* Congressional Testimony, Nov. 14, 2001.

79. Cottle, *supra* note 58.

80. *Id.*

81. *Id.*

82. Heather Timmons, *Western Union: Where the Money Is - In Small Bills,* BUSINESS WEEK, Nov. 26, 2001, at 40.

83. *Id.*

84. *Id. See* Richard Stevenson and Leslie Wayne, *More Regulations to Thwart Money Laundering Are Imposed*, New York Times, April 23, 2002.

85. Heather Timmons, *supra* note 82.

86. *Id.*

87. *Id.*

88. *Id.*

89. David Kaplan, How a Terror Funds Attacks- and Hides Its Tracks, U.S. News and World Report, Oct. 1, 2001, at 20.

90. Adam Cohen, *Banking on Secrecy; Terrorists Oppose Scrutiny of Offshore Accounts and So Do Many United States Bankers and Lawmakers,* TIME, Oct. 22, 2001, at 73.

91. 32 USC § 5318(1)(4)(A).

92. Adam Cohen, *supra* note 90.

93. *Id.*

94. *See* www/.oecd.org/fatf. for list of the non-cooperative countries and territories.

95. William Wechsler, *Follow the Money*, FOREIGN AFFAIRS, July/August 2001, at 40.

96. *Id.*

97. Maeve Sheehan, *Dublin Link to Heart of Terror Cash Network*, SUNDAY TIMES (London), Sep. 30, 2001.

98. *Id.*

99. *See* Bruce Zagaris, *supra* note 60; *see* also Report of the National Commission on Terrorism, *Countering the Changing Threat of International Terrorism*, available at

http://www.fas.org/irp/threat/commission/html(2001).

100. Ottawa Communique of G-7, Feb. 9, 2002, c/windows/temp/GWprint/text.htm.

101. Daniel Klaidman, *On the Trail of the Paymaster*, NEWSWEEK, Nov. 18, 2001, at 18.

102. *Id.*

103. Mike McNamaee, A Hard Slog for Financial "Special Forces," Business Week, Nov. 26, 2001 at 39.

104. *Id.*

105. Wechsler, *supra* note 95.

106. *See*, *e.g.,* Ulrika Lomas, *"Naming and Shaming,"* Tax-News.com., Brussels, Nov.14, 2001. *See also* Bruce Zagaris, *FATF Adopts New Standards to Combat Terrorist Financing*, 17 Int'l. ENF. LAW RPT. 493 (Dec. 2001).

107. United States Embassy, U.S. Report to UNSC on Counterterrorism Measures, http://usembassy.state.gov/tokyo/wwwhseo840.html Visited 4/16/02.

108. Shukovsky, *Russians Urge FBI to Close the al Qaeda Linked Bank Account with Chechen Connections,* BULLETIN FRONTRUNNER, Nov. 15, 2001.

109. Cohen, *supra* note 90 at 68.

110. Olsen, *supra* note 52; *see also* Eichenwald, *supra* note 11, at B-4.

111. Section 1016 USA Patriot Act 2001.

112. 42 USC §14601 (2000).

113. See generally, Critical Infrastructure Protection and the Endangerment of Civil Liberties, Electronic Privacy Information Center Washington (1998) http://www.epicorg/security/infowar /epic-cip.html.

114. Frederick Schauer, *Internet Privacy and the Public-Private distinction*, 387 Jurimetrics J. 555, 555-556 (1998).

115. *Id.*

116. *Id.*

117. *Id.* at 558-559.

118. *Id*. at 559.

119. *Id.* at 562 Quoting Katz v. United States, 389 U.S. at 361.

120. 425 U.S. 435, 96 S. Ct. 1619, 48 L. Ed. 2d 71 (1976).

121. *Id.* at 425 U.S. 563.

122. *Id.* at 563-564.

123. *See* In the Matter of Application of the United States for an Order Authorizing the Physical Search of Non-residential Premises and Personal Property, United States Foreign Intelligence Surveillance Court, 1981 unnumbered slip opinion; *see* Dycus, Berkey, et al., *supra* note 51 at 469.

124. See United States v. Bin Laden, 92 F. Supp. 2d 189 and 126 F. Supp. 2d 264 (S.D.N.Y. 2000).

125. *United States v. United States District Court*, 407 U.S. 297 (1972); *see also United States v. Cavanagh*, 807 F.2d 787 (9th Cir. 1987).

126. 835 F.2d 1067, 1075 (4th Cir. 1987), *cert denied* 486 U.S. 1010 (1988).

127. *Id.* citing to *United States v. United States District Court*, *supra* note 125.

128. Professor Dorothy Denning, *Cyberterrorism* (last visited Nov. 6, 2001), available at www.terrorism.com/documents/denning-testimony.shtml.

129. *See* Bruce Zagaris, *supra* note 60; *see* also Report of the National Commission on Terrorism, *Countering the Changing Threat of International Terrorism*, available at http://www.fas.org/irp/threat/commission/html(2001).

130. Ottawa Communique of G-7, Feb. 9, 2002, c/windows/temp/GWprint/text.htm.

131. 533 U.S. 27, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001).

132. *Katz v. United States*, 389 U.S. 374, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967).

133. *Kyllo v. United States,*, *supra* note 131 at 121 S.Ct. 2053.

134. Leading cases, Fourth Amendment Warrantless Searches - Surveillance Technology, 115 HARV. L. REV. 346, 354 fn. 69 (2001).

135. 8 U.S.C. § 1189 (2001).

136. *Id.* at § 1189(a)(2)(C).

137. *People's Mojahedin Organization of Iran v. United States Department of State*, 182 F.3d 17 (D.C. Cir. 1999) [hereinafter *Mojahedin*]; *National Council of Resistance of Iran v. United States Department of State*, 251 F.3d 192 (D.C. Cir. 2001) [hereinafter *National Council*].

138. *Mojahedin*, 182 F.3d at 19.

139. *Id.*

140. *Id.*

141. *National Council*, 251 F.3d at 192.

142. *Id.* at 193.

143. *Id.* at 199.

144. 8 U.S.C. § 1189(a)(2).

145. *Mojahedin*, 182 F.3d at 22.

146. *Id.* at 19.

147. 8 U.S.C. § 1189 (b)(3).

148. *Mojahedin*,182 F.3d at 24; *see also* 8 U.S.C. §§ 1189(a)(1)(B); and 182(a)(3)(ii).

149. *Mojahedin*, 182 F.3d at 19.

150. *The Shadow World of the Terrorist Is Exposed*, *in* HOW DID THIS HAPPEN? TERRORISM AND THE NEW WAR (James Hoge, Jr., & Gideon Rose, eds., Public Affairs, N.Y. 2001).

151. *See also* 8 U.S.C. § 1189, *supra* note 147.

152. Derek P. Jinks, *International Decision: People's Mojahedin Organization of Iran v. United States Department of State*, 182 F.3d 17 (D.C. Cir. 1999), 94 A.J.I.L. 396 (April, 2000).

153. *Id.* at 399.

154. *Id.* at 400; *see also Misretta v. United States*, 488 U.S. 361, 407 (1989).

155. After this date, the law will be in a process that will potentially expand it, and make it more easy to collect, gather, and adjudicate information on potential terrorist activity.

156. Jinks, *supra* note 152, at 399.

157. *Mojahedin*, 182 F.3d at 25.

158. Jinks, *supra* note 152, at 400.

159. *Id.*

160. *See* Convention for the Suppression of Unlawful Seizure of Aircraft, Dec. 16, 1970, 22 U.S.T. 1643, 860 U.N.T.S. 105; Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents, Dec. 14, 1973, 28 U.S.T. 1975, 1035 U.N.T.S. 167; International Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, Dec. 10, 1984, S. Treaty Doc. No. 100-20 (1988), 1465 UNTS 85.

161. 8 U.S.C. § 1189, *supra* note 147.

162. *Mojahedin*, 182 F.3d at 19.

163. *Id.* at 22; "Aliens receive constitutional protections only when they have come within the territory of the United States and developed substantial connections with this country." *United States v. Verdugo-Urquidez*, 494 U.S. 259, 271 (1990); *see also Regan v. Wald*, 468 U.S. 222 (1984).

164. *Mojahedin*, 182 F.3d at 19.

165. *Id.*

166. *Id.*

167. *Id.* ("Whatever rights the LTTE and the PMO enjoy in regard to these cases are statutory rights only. Because Congress so allowed, the LTTE and the PMO are entitled to contest their designations on the grounds set forth in § 1189(b)(3). Under the statute, they may for instance seek our judgement about whether the Secretary followed statutory procedures, or whether she made the requisite findings, or whether the record she assembled substantially supports her findings.")

168. *Id.*

169. *Id.* at 23; "Of the three findings mandated by § 1189(a)(1), the third (C) the terrorist activity of the organization threatens the security of the United States nationals or the national security of the United States is non-justiciable." *Chicago & Southern Air Lines, Inc. v. Waterman Steamship Corp.*, 333 U.S. 103 (1948). "It is beyond the judicial function for a court to review foreign policy decisions of the Executive Branch. These are political judgements, decisions of a kind for

which the Judiciary has neither aptitude, facilities, nor responsibilities and have long been held to belong in the domain of political power not subject to judicial intrusion or inquiry." *Id.* at 111.

170. *Mojahedin*, 182 F.3d at 23-24.

171. *Id.*

172. *Id.*

173. *Id.* In cases on appeal from the district court, courts are to review "judgments, not opinions." *Chevron U.S.A. v. Natural Resources Defense Council*, 467 U.S. 837 (1984).

174. *Mojahedin*, 182 F.3d at 23.

175. *Id.*

176. *Id. See also Jones v. United States*, 137 U.S. 202 (1890).

177. *Id.* at 22.

178. *Id.* at 19.

179. *Id.* at 25.

180. *Id.* at 22. "A foreign entity without property or presence in this country has no constitutional rights, under the due process clause or otherwise." *United States v. Verdugo-Urquidez,* 494 U.S. 259, 271 (1990).

181. *National Council*, 251 F.3d at 192.

182. *Id.* at 196, 199; 8 U.S.C. § 1189(b)

183. *National Council*, 251 F.3d at 196.

184. *Id.*

185. *Id.* at 197.

186. *Id.* at 198-99

187. *Id.*

188. *Id.* at 199.

189. *Id.* at 201.

190. *See United States v. Verdugo-Urquidez*, 494 U.S. 259, 271 (1990).

191. *National Council*, 251 F.3d at 203.

192. *Id.* at 204.

193. Jinks, *supra* note 152; *see also* Ruth Wedgwood, *Responding to Terrorism: The Strikes Against Bin Landen*, 24 YALE J. INT'L L. 559, 561 (1999).

194. *National Council,* 251 F.3d at 202-203.

195. *Id.*

196. *Id.*

197. *Id.* at 207.

198. *Id.* "Certainly the United States enjoys a privilege in classified information affecting national security so strong that even a criminal defendant to whose defense such information is relevant cannot pierce that privilege absent a specific showing of materiality." *United States v. Yunis*, 867 F.2d 617 (D.C. Cir 1989).

199. *Id*.; "The fundamental requirement of due process is the opportunity to b heard at a meaningful time and in a meaningful manner." *Matters v. Eldridge*, 424 U.S. 319, 333 (1976).

200. *Id.*

201. *Mojahedin*, 182 F.3d at 25.

202. Consider 8 U.S.C. § 1531 and *Klareldeen v. Reno*, 71 F. Supp. 2d 402 (D.N.J. 1999).

203. See Fletcher Baldwin, *The United States Supreme Court: A Creative Check of Institutional Misdirection*, 45 Ind. L. Jo. 550 (1970). See *also* Bruce Zagaris, *supra* note 1, at 526, and *Zadvyas v. Davis*, ___ U.S. ___, 121 S.Ct. 2491, ___ L.Ed. 2d ___ (2001).

204. *See generally,* H.L.A. Hart, *The Concept of Law* (Oxford University Press 1961).