George Ackerman

Independent Study/Thesis (Required to complete NSU Law Degree)

Summer Semester Professor John Anderson

The USA Patriot Act: An Overview and Its Effect on Constitutional Rights

Introduction

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USAPA) came into effect on September 17, 2001, when Attorney General John Ashcroft presented Congressional leaders with the Bush administration's proposal to enhance and strengthen terrorism legislation due to the September 11, 2001 attack on the World Trade Centers in New York. On October 26, 2001, President Bush signed the USA Patriot Act (USAPA) into law. The USAPA was created to deter and punish terrorist acts in the United States and around the world and to enhance law enforcement investigatory tools to prevent future terrorist activities. Furthermore, the legislation entitled

> [T]he Mobilization Against Terrorism Act, was to enhance the ability of the government to eliminate terrorist organizations, prevent terrorist attacks, and punish terrorists. The key issues of the proposal included intelligence gathering, immigration, criminal justice, and money laundering. Primarily, the administration meant to broaden the intelligence community's abilities to conduct roving searches of people suspected of terrorism, to detain and deport persons suspected of terrorist involvement, and to remove any statute of limitations on crimes of terrorism. The proposal also expanded the ability of the Department of Justice to place wiretaps on telephones and computer terminals of anyone suspected of terrorism or of having connections to suspected terrorist organizations. This proposal provided the framework for the introduction of the Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act of 2001 introduced by the House of Representatives and the

> Uniting and Strengthening America (USA) Act of 2001 introduced by the Senate, which eventually became the USA PATRIOT Act of 2001.

Jennifer C. Evans, *Hijacking Civil Liberties: The USA Patriot Act of 2001*, 33 Loy. U. Chi. L.J. 933 (2002).

More importantly to note, is that the USAPA also set forth more powers for Presidential authority when the United States is engaged in armed hostilities or has been attacked by a foreign country or foreign nationals, confiscate any property, subject to the jurisdiction of the United States, of any foreign person, foreign organization, or foreign country that the President determines has planned, authorized, aided, or engaged in such hostilities or attacks against the United States.

Since the introduction of the USAPA, the government has taken actions that could place many restrictions and limitations on the Bill of Rights and damage the various fundamental liberties enjoyed under the Constitution. The war on terror has seriously compromised the First, Fourth, Fifth, Sixth and Fourteenth Amendment rights of citizens and non-citizens alike. From the USAPA, comes a reevaluation of domestic terrorism, to the FBI's new powers of search and surveillance, the indefinite detention of both citizens and non-citizens without formal charges, and the problematic undermining of the principles of the freedom of speech, due process, and equal protection under the United States Constitution.

The Effect of the USAPA

The USAPA was designed to allow law enforcement officials to track down and punish those responsible for terrorist attacks, funding and supporting terrorist activities and to protect against any and all future terrorist attacks. The Act also grants federal

officials greater power to trace and intercept terrorist communications both for law enforcement and foreign intelligence purposes. The USAPA has created a balancing test between the Fourth Amendment of the Constitution, which prohibits unreasonable searches and seizures, and the President's constitutional authority to protect America from any national security threat. These expansive "intelligence and surveillance laws may restrict precious civil liberties, and, therefore, they will not survive unless the government can find a constitutionally acceptable balance between national security and civil liberties." Michael F. Dowley, *Government Surveillance Powers Under the USA Patriot Act: Is It Possible to Protect National Security and Privacy at the Same Time? A Constitutional Tug-of-War*, 36 Suffolk U. L. Rev. 165 (2002).

Additionally, the USAPA reinforces federal anti-money laundering laws and regulations in an effort to deny terrorists the resources necessary for future attacks and to tighten the U.S. immigration laws to close its borders to foreign terrorist and to expel those within the United States. Furthermore, the USAPA creates new federal crimes such as outlawing terrorist attacks on mass transit, increases penalties for many citizens, and provides for a longer statute of limitations for crimes of terrorism. The USAPA creates judicial safeguards for electronic mail monitoring and grand jury disclosures, recognizes innocent owner defenses to forfeiture and entrusts enhanced ant-money laundering powers to those regulatory authorities whose concerns include the well being of our financial institutions.

With the USAPA in effect, the law provides for new sweeping powers to both domestic law enforcement and international intelligence agencies and has eliminated the checks and balances system that previously gave courts the opportunity to ensure that

these powers were not abused by the Executive and Legislative branches of government. The USAPA expands surveillance laws including the use of wiretaps, search warrants, pen/trap orders and subpoenas.

> The first wiretapping case decided by the Supreme Court was *United States v. Olmstead*. Federal prohibition agents suspected Olmstead of violating the National Prohibition Act. They overheard incriminating conversations by setting up a wiretap to intercept telephone calls between Olmstead and his attorney. The Supreme Court held that the wiretap was not subject to Fourth Amendment restrictions because it was established without any physical intrusion into the homes or offices of the defendants. Moreover, no physical objects were seized. Thus, neither a search nor a seizure had taken place. In his famous dissent, Justice Brandeis argued for recognition of a right to be let alone so that "every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."

Robert A. Pikowsky, *An Overview of the Law of Electronic Surveillance Post September 11, 2001,* 94 Law Libr. J. 601 (2002). The counterpart to the USAPA, which deals with foreign affairs, is the Foreign Intelligence Surveillance Act (FISA), which allows for spying in the U.S. by foreign intelligence agencies, has also been expanded. FISA allows the government to view private Internet searching of Americans so long as the governmental viewing of the information relevant to an ongoing criminal investigation, which means that the person spied on, does not have to be the target of the investigation. Since the passing of the USAPA in Congress, the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA) have the power to use nationwide roving wiretaps. They can go from phone to phone, computer to computer without demonstrating that each is even being used by a suspect or target of an order. Moreover, the government may now serve a single wiretap order on any person or entity nationwide, regardless of whether that person or entity is named in the order. The government need not make any showing to a court that the particular information or communication to be

acquired is relevant to a criminal investigation. In conclusion, the USAPA provides for surveillance which may have violated a citizen's rights in the past, but the USAPA comes in response to the preservation of national security. Terrorism has played a large part in society. With the USAPA enacted, the government has the ability to use any means to protect the United States from terrorist threats.

The USAPA and the United States Code's Interpretation of Terrorist Acts

The USAPA and the United States Code have codified the various forms of terrorism into three categories: domestic, international and federal. Under § 2331 of Title 18 of the United States Code and amended in § 802 of the USAPA defines domestic terrorism as "activities that involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any state and appears to be intended to intimidate or coerce a civilian population to influence the policy of a government by intimidation or coercion; or to affect the conduct of a government by mass destruction, assassination, or kidnapping; and occur primarily within the territorial jurisdiction of the United States." 18 U.S.C. § 2331 (2003). Furthermore, § 2331 of Title 18 of the United States Code defines international terrorism as activities that involve

> violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State that appear to be intended to intimidate or coerce a civilian population, to influence the policy of a government by intimidation or coercion; or to affect the conduct of a government by mass destruction, assassination or kidnapping; and occurs primarily outside the territorial jurisdiction of the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum.

Id. Additionally, under § 2331 of Title 18, federal terrorism has been defined as calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct; and violates sections indicated under 18 USCS § 2332 (b)(5)(b)(i), including:

> destruction of aircraft or aircraft facilities, violence at international airports, arson within special maritime and territorial jurisdiction, relating to biological weapons, relating to chemical weapons, relating to nuclear materials, to protection of computers, relating to acts of terrorism transcending national boundaries, bombing of public places and facilities, relating to harboring terrorists, providing material support to terrorists, providing material support to terrorist organizations.

Id. The USAPA has recreated the meaning of these terms and allowed the government to expose more citizens to surveillance as well as harboring and material supporting liability. Domestic terrorism causes a lot of economic, emotional, and physical devastation to a country. Nations are sorely tempted to spend more on fighting homeland terror than international terror. In doing so it exceeds the capacities of most deficit spending wartime budgets. Following September 11, Congress has been most concerned about protecting the critical infrastructure of the United States from disruption and destruction. The threats to these infrastructures fall into two categories: physical threats to tangible property (physical threats) and threats of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures (cyber threats). The eight critical infrastructures of the U.S. include the electric power system, gas and oil (storage and transportation), telecommunications, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire and rescue) and continuity of government services. Congress has recognized that any terrorist threat on any of these vital infrastructures could create havoc internally within the United States. However, in

ensuring the preservation of these infrastructures, the Legislative and Executive branches may have overstepped their authority by infringing on individual civil liberties and rights.

Overbreadth of the USAPA and FISA

Many of the USAPA changes have been overbroad and have not aided the cause in fighting terrorism yet it has fundamentally altered citizen's rights. Some of the USAPA's impact on regulations includes the government's ability to view citizen's Internet searching without a court order which may violate their Fourth Amendment right of privacy as afforded by the U.S. Constitution. In United States v. Truong Dinh Hung, the United States Court of Appeals for the Fourth Circuit held that the

> [E]xecutive should be excused from securing a warrant only when the surveillance is conducted "primarily" for foreign intelligence reasons . . . . Once surveillance becomes primarily a criminal investigation, the courts are entirely competent to make the usual probable cause determination, and because, importantly, individual privacy interests come to the fore and government foreign policy concerns recede when the government is primarily attempting to form the basis for a criminal prosecution. Many scholars argue that "when intelligence gathering has ended and law enforcement begun, the proscriptions of the Fourth Amendment apply and any analogy to the administrative search is misplaced."

Alison Bradley, *Extremism in the Defense of Liberty: The Foreign Intelligence Surveillance Act and the Significance of the USA Patriot Act*, 77 Tul. L. Rev. 465 (2002). Additionally, the wiretapping and intelligence provisions in the USAPA improperly minimize the role of judges in ensuring that law enforcement wiretapping is conducted legally and permits intelligence authorities to bypass procedures that protect an individual's right to privacy as protected under the Fourth and Fourteenth Amendments.

Under the Foreign Intelligence Surveillance Act (FISA), searches are always secret, the target of a FISA surveillance does not know when a search occurs and cannot obtain discovery of the FISA court order application. Therefore, in a criminal

prosecution, if the state uses evidence gathered through a FISA search, the target of the search does not have notice of the search, violating the Fourth and Fourteenth Amendments. In criminal investigations, the Fourth Amendment requires that law enforcement officials have probable cause to believe that a crime has been or is being committed in order to conduct a search. FISA searches, however, do not require a showing of probable cause. Thus when FISA was enacted

> Congress required that the primary purpose of the search or wiretap was to gather foreign intelligence and not to gather information relating to a criminal investigation. The USAPA ignores the probable cause requirement of the Fourth Amendment when obtaining a court order. This is too great of an invasion into the privacy of innocent individuals and into the areas of the lives of targeted individuals that are of no relevance to the government's investigation.

Jennifer C. Evans, *Hijacking Civil Liberties: The USA Patriot Act of 2001*, 33 Loy. U. Chi. L.J. 933 (2002).

The USAPA also allows the government to collect DNA of terrorists, but then inexplicably also added a collection for the broad, non-terrorist category of any crime of violence, allows for wiretaps for suspected violations of the Computer Fraud and Abuse Act, which includes anyone suspected of exceeding the authority of a computer used in interstate commerce that causes over five thousand dollars worth of combined damage, as well as adding to the penalties for computer fraud and has expanded laws that may allow citizens to be interpreted in an easy fashion by U.S. foreign intelligence agencies such as the FBI and CIA. The USAPA also provides for the expansion of the Foreign Intelligence Surveillance Act (FISA) and its authority to spy on Americans or foreign persons within the U.S. Domestic law enforcement and foreign intelligence's ability to share information has also become more readily available. In the 1970's, the FBI and CIA had been conducting investigations of Americans which went beyond the powers of

each respective organization. The USAPA now allows wiretap results and grand jury information and other information collected in a criminal case to be disclosed to the intelligence agencies when the information constitutes foreign intelligence or foreign intelligence information, the latter being a broad new category created by this law. The USAPA affords the opportunity for the FBI and the CIA to share vital information to protect the nation's security. Additionally, the USAPA states that the FBI may apply for an order requiring the production of any tangible things, including books, records, papers and documents, for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the First Amendment.

Moreover, the USAPA enhances domestic security against terrorism by establishing a counter-terrorism fund. This fund was established in the Treasury of the United States by reestablishing the operational capability of an office or facility that has been damaged or destroyed as the result of any domestic or international terrorism incident; providing support to counter, investigate, or prosecute domestic or international terrorism, including, without limitation, paying rewards in connection with these activities; and conducting terrorism threat assessments of federal agencies and their facilities. The USAPA also strives to eliminate discrimination and has incorporated a broad range of laws to counter-terrorism. Congress condemned discrimination against Arab Americans and Muslim Americans after September 11, 2001. The acts of violence that have been taken against Arab and Muslim Americans since the September 11, 2001,

attacks against the United States should be and are condemned by all Americans who value freedom.

Furthermore, the USAPA called for increased funding for the technical support center of the FBI, requests for military assistance to enforce prohibition in certain emergencies and the expansion of national electronic crime task force initiative. All of these proclamations were set to increase awareness of the battle against terrorism.

The USAPA's Effect on the Computer Fraud and Abuse Act and Electronic Communications Act

The USAPA amended the Computer Fraud and Abuse Act and the Electronic Communications Privacy Act to work more effectively with current technology. Both of these Acts provide examples of how Attorney General Ashcroft's objectives will be met. The Computer Fraud and Abuse Act (CFAA) was the first piece of legislation designed to address computer crime. Currently, the CFAA is the main federal cyber-crime statute, which addresses

> computer crimes in which the computer is the "subject' - that is, computer crimes for which there is no analogous traditional crime and for which special legislation is needed." Such crimes include the use of "sniffers," "worms," "Trojan horses," "logic bombs," and "viruses." The CFAA has been used to prosecute "malicious code authors, ... "outside' hackers who penetrate computers, steal information and/or cause damage to the system, and people who use computers to commit fraud.

Tammy J. Schemmel, *Justice In A Changed World: How The USA Patriot Act Combats Cyber-Crime,* 29 Wm. Mitchell L. Rev. 921 (2003).

The Electronic Communications Privacy Act (ECPA) is the federal law that protects electronic communication users against unauthorized interception, use, or disclosure of electronic communications while in transit or in storage. The ECPA's

purpose is to update privacy protections and standards with the changes in computer and telecommunications technologies. Since its inception, additional technology updates have included electronic mail, the Internet, cellular phones, and paging devices. Since most terrorist activities and planning stem from the use of computer use, computer crime presents new challenges to law enforcement agencies. The most troublesome challenge is that the cyber-world is much larger than any country's borders. The main challenge is that in a computer crime, government officials cannot track physical evidence as easily as they would to find a bank robber who robbed a bank in Florida. To give these officials the tools they need to stop cyber-crime, "the laws need to change as technology changes. The USAPA provides such tools by eliminating jurisdictional boundaries of courts [and] permit[s] Internet service providers to share information with law enforcement agencies." Id.

In passing the USAPA, Congress and President Bush substantially altered the government's ability to carry out electronic surveillance. Although prosecutors and law enforcement agents have embraced the USAPA, many legal scholars have vehemently criticized the Act's procedural insufficiencies and unconstitutional invasion of individual rights. The crux of this analysis concerns

> whether surveillance permitted by the PATRIOT Act constitutes a reasonable search under the confines of the executive branch's national security authority, subject to Fourth Amendment safeguards. Although provisions of the Act may inadvertently infringe on precious civil liberties vital to this nation's survival, its implementation may ensure America's continued existence by allowing government agents to keep pace with technological advancements and monitor elusive terror networks within this country's borders. Future judicial review may more neatly tailor the Act to satisfy the government's interests without infringing on civil liberties with such severity. As enacted by Congress, however, the Act is reasonable, constitutional, and necessary for the protection of America and its citizens.

Michael F. Dowley, *Government Surveillance Powers Under the USA Patriot Act: Is It Possible to Protect National Security and Privacy at the Same Time? A Constitutional Tug-of-War*, 36 Suffolk U. L. Rev. 165 (2002).

Congress's intent also provided for enhanced surveillance procedures which could possibly infringe on citizen's constitution rights. The authority to intercept wire, oral, and electronic communications relating to terrorism was expanded and the authority to intercept wire, oral, and electronic communications relating to computer fraud and abuse offenses were added. The FBI and CIA are now authorized to share criminal investigative information like never before. With the USAPA, as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401(a)), any investigative or law enforcement officer, or attorney for the government, who by any means authorized, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived there from, may disclose such contents to any other federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence. In monitoring and conducting the various forms of surveillance, local and federal governments must keep in mind that in conducting their respective duties, they must avoid infringing upon civil rights and liberties as protected under the United States Constitution.

Privacy Versus Protection: Congress Strikes a Balance

The Fourth Amendment to the United States Constitution guarantees that individuals shall be free from unreasonable searches and seizures. The Framers of the Constitution intended the Fourth Amendment to protect individuals from unreasonable

governmental intrusion into their private lives. Generally speaking, the U.S. Supreme Court has interpreted the Fourth Amendment to require a warrant supported by probable cause for each search and seizure. "While the Fourth Amendment's purpose is to protect individual privacy rights and prevent unwarranted government intrusions, it is not intended as a general restraint on all police practices but only those that are unreasonable." Jennifer C. Evans, *Hijacking Civil Liberties: The USA Patriot Act of 2001*, 33 Loy. U. Chi. L.J. 933 (2002). The USAPA specifies that U.S. law provides for two separate "tracks" with differing proof of standards and procedures for each of these mechanisms depending upon whether surveillance is done by domestic law enforcement or foreign intelligence. Surveillance conducted for domestic law enforcement purposes must fulfill the probable cause standard set forth under the Fourth Amendment which applies to interception orders and search warrants.

However, foreign intelligence surveillance is not based on the concept of criminality because under the Foreign Intelligence Surveillance Act (FISA), the issue is whether the intended surveillance target is an agent of a foreign power or a foreign power. Only if the target is a U.S. citizen or permanent resident alien must the government show probable cause of criminality. FISA allows a secret court to authorize U.S. intelligence agencies to conduct surveillance. FISA interception orders involving U.S. persons are issued by the secret court based on an application from the Attorney General stating reasons to believe that the surveillance target is an agent of a foreign power or a foreign power, certifying that the purpose of the surveillance is to gather foreign intelligence information, and representations. FISA's requirements are weak when the electronic surveillance is directed solely at means of communications used

exclusively between or among foreign powers and when it is unlikely that communications to which a U.S. person is a party will be intercepted. Additionally under § 213 of the USAPA,

> the government now has authority for delaying notice of the execution of a warrant and to search for and seize any property or material that constitutes evidence of a criminal offense in violation of the laws of the U.S. New access to records under the FISA as well as access to business records for foreign intelligence and international terrorism investigations has been approved by Congress to research different leads as to terrorist activity.

United States of America Patriot Act of 2001, H.R. 3162, 107th Cong. §213 (2001).

The Supreme Court of the United States has held that several exceptions to the warrant requirement exist. Those exceptions, most pertinent to electronic surveillance, include when a person consents to the search or seizure, instances that result as a consequence of emergency circumstances, and instances when the person, place, or device is in plain view. Consequently, when a party agrees to allow a law enforcement official to wiretap a telephone or electronically monitor keystrokes on a computer, that official does not need to obtain a warrant to conduct the search. Similarly, the Court has "eased the warrant requirement when facing "exigent circumstances" that could jeopardize a person's life or cause the spoliation of vital evidence . . . [or] a government official to obtain a warrant if that official can openly see the person or place from a public or otherwise legally allowed observation point." Michael F. Dowley, *Government Surveillance Powers Under the USA Patriot Act: Is It Possible to Protect National Security and Privacy at the Same Time? A Constitutional Tug-of-War*, 36 Suffolk U. L. Rev. 165 (2002).

The USAPA has modified preexisting electronic surveillance law in five significant ways. The first is where the information is obtained under FISA's provisions

for law enforcement purposes if the information is to be used in a criminal proceeding, and if the Attorney General had given advance authorization. The second is via roving surveillance. Roving surveillance is highly invasive and has been resoundingly criticized by privacy advocates. However, roving surveillance has already been upheld as constitutional in the law enforcement context. Using roving surveillance, the government may have the capacity to obtain useful information as a result of being able to monitor individuals suspected of posing a threat to the United States. Third, under FISA, pen/trap orders can be more easily obtained. To obtain a FISA order authorizing the use of a pen/trap device, the government now only has to certify that the "information sought is relevant to an ongoing intelligence or terrorism investigation. In the past, the government also had to demonstrate that the device to be monitored was likely to be used by someone involved in terrorism or intelligence activities that could violate U.S. criminal laws." Nathan C. Henderson, *The Patriot Act's Impact on the Government's Ability to Conduct Electronic Surveillance of Domestic Communications,* 52 Duke L.J. 179 (2002). Fourth, pen/trap orders now apply to both wire and electronic communications. The Patriot Act resolved this ongoing debate by clarifying that the pen/trap statutes apply to both types of communications, so long as content information is excluded. A significant number of courts had in effect already reached this same conclusion. This particular modification is unlikely to entail any significant substantive consequences other than making explicit that which was previously assumed. "It seems apparent that in enacting this provision of the Patriot Act, Congress was updating the pen/trap statutes after becoming [cognizant] of how technology has [changed over the years]." Id. Lastly, once obtained, all pen/trap orders are now valid throughout the U.S.

Under section 216 of the USAPA, it also amends the law governing pen registers and trap and trace devices. The revised language makes clear that law enforcement officials can obtain analogous information concerning e-mail, such as Internet protocol addresses. Additionally, section 216 expands the definitions of pen register and trap and trace device to include software as well as mechanical devices. "It requires law enforcement officers who use their agency's equipment or software to establish the pen register or trap and trace device to provide a report to the court under seal detailing certain information about their activities." Robert A. Pikowsky, *An Overview of the Law of Electronic Surveillance Post September 11, 2001,* 94 Law Libr. J. 601 (2002). Section 217 of the USAPA also amends a provision of the Federal Wiretap Act so as to permit an Internet Service Provider (ISP) to seek assistance from law enforcement officers in investigating the activities of a "computer trespasser." The new law enables the ISP to authorize law enforcement officers to monitor communications to or from the trespasser, but they cannot monitor the communications of authorized users. Id. With this new authorization, law enforcement officials can monitor communications only when they have reasonable grounds to believe that the communications are relevant to the investigation. Moreover, Section 220 of the USAPA "amends the Stored Communications Act to give nationwide effect to search warrants authorizing law enforcement officers to obtain stored e-mail held in a subscriber's mailbox by an ISP." Id. Previously, the Federal Rules of Criminal Procedure limited the scope of a search warrant to property within the district of the court that issued the warrant. However, under the new law, it permits a court with jurisdiction over the offense being investigated to issue a search warrant for stored e-mail held by an ISP anywhere in the country.

Therefore, law enforcement officials do not need to seek a warrant in the jurisdiction where the ISP's server happens to be located. Additionally, Section 505 of the USAPA amends the Stored Communications Act provision governing FBI access to customer records held by a wire or electronic communication service provider as it applies to counterintelligence investigations. Prior law permitted

> the FBI to order the service provider to turn over records containing the name, address, and length of service, as well as local and long distance toll billing records pursuant to a counterintelligence investigation. The FBI was not required to seek prior judicial authorization to obtain this information. Rather, the FBI needed only to certify to the service provider that the information was "relevant to an authorized foreign counterintelligence investigation" and that there were "specific and articulable facts" giving reason to believe that the information pertained to a foreign power or an agent of a foreign power.

Id.

Another important change to privacy under the USAPA was the expanded congressional oversight that has been granted to allow the Attorney General to inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests for the production of tangible things. United States of America Patriot Act of 2001, H.R. 3162, 107th Cong. §502 (2001). The FBI and the CIA now have the granted authority to request nationwide service of search warrants for electronic evidence. United States of America Patriot Act of 2001, H.R. 3162, 107th Cong. §220 (2001). The major changes under the USAPA not only affected privacy areas but also how the U.S. was able to monitor and seize funds used by terrorist organizations and those nations that funded terrorist activities.

The USAPA and the International Money Laundering Abatement and Anti-Terrorist Financing Act

Title III of the USAPA expanded the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001. This modification was designed to increase the strength of U.S. measures to prevent, detect, and prosecute international money laundering and the financing of terrorism. Furthermore, it provides "special measures for jurisdictions, financial institutions, or international transactions of primary money laundering concern, [which] would prevent terrorist funding and the U.S. could now investigate funds that were not readily available or permissible to search before hand." United States of America Patriot Act of 2001, H.R. 3162, 107th Cong. §311 (2001). By preventing the funding of terrorism, the U.S. would be able to successfully track down any countries, organizations or private citizens that sent contributions to any terrorist function or cell, and stop them before they receive the funding to attack. The U.S. now has the granted authority

> to use cooperative efforts to deter money laundering, prohibit United States correspondent accounts with foreign shell banks, provide special due diligence for correspondent accounts and private banking accounts, and the ability to confiscate assets of suspected international terrorists, may contest that confiscation by filing a claim in the manner set forth in the Federal Rules of Civil Procedure and under §316 stated as the Anti-Terrorist Forfeiture Protection.

United States of America Patriot Act of 2001, H.R. 3162, 107th Cong. §§312-316 (2001).

Under the USAPA, so long as notice is given to the Secretary, two or more financial institutions and any association of financial institutions may share information with one another regarding individuals, entities, organizations, and countries suspected of possible terrorist or money laundering activities.

> A financial institution or association that transmits, receives, or shares such information for the purposes of identifying and reporting activities that may involve terrorist acts or money laundering activities shall not be liable to any person under any law or regulation of the United States, any constitution, law, or regulation of any state or political subdivision thereof, or under any contract or other legally enforceable agreement, for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure, or any other person identified in the disclosure, except where such transmission, receipt, or sharing violates this section or regulations promulgated pursuant to this section.

United States of America Patriot Act of 2001, H.R. 3162, 107th Cong. §314 (b) (2001). This regulation was not permissible before the USAPA was passed into law. Many banks across the nation had a sense of protection and secrecy and with terrorism at a rise; the U.S. was left with no other choice then to weigh the individual freedoms of security over the protection of financial institutional secrecy.

Additional sanctions and harsher penalties were created under USAPA, which allowed harsher penalties to any person

> who is an official or employee of any department, agency, bureau, office, commission, or other entity of the federal government, and any other person who is acting for or on behalf of any such entity, who, directly or indirectly, in connection with the administration of this title, corruptly demands, seeks, receives, accepts, or agrees to receive or accept anything of value personally or for any other person or entity in return for being influenced in the performance of any official act, being influenced to commit or aid in the committing, or to collude in, or allow, any fraud, or make opportunity for the commission of any fraud, on the United States, or being induced to do or omit to do any act in violation of the official duty of such official or person.

United States of America Patriot Act of 2001, H.R. 3162, 107th Cong. §329 (2001).

Under the USAPA, there is now an international cooperation in investigations of money laundering, financial crimes, and the finances of terrorist groups. United States of America Patriot Act of 2001, H.R. 3162, 107th Cong. §330 (2001). The intent of Congress was that the President would direct the Secretary of State, the Attorney

General, or the Secretary of the Treasury, and in consultation with the Board of Governors of the Federal Reserve System, to seek to enter into negotiations with the appropriate financial supervisory agencies and other officials of any foreign country, the financial institutions of which do business with U.S. or which may be utilized by any foreign terrorist organization, and that any person who is a member or representative of any such organization or any person engaged in money laundering or other crimes, shall be brought to justice.

The USAPA allows for the viewing of any terrorist activity and stop it before the funds go to the respective targets and allows banks to disclose secret information that may be used to further a terrorist act.

> Any financial institution that makes a voluntary disclosure of any possible violation of law or regulation to a government agency or makes a disclosure pursuant to this subsection or any other authority, and any director, officer, employee, or agent of such institution who makes, or requires another to make any such disclosure, shall not be liable to any person under any law or regulation of the United States, any constitution, law, or regulation of any state or political subdivision of any state, or under any contract or other legally enforceable agreement, for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure or any other person identified in the disclosure.

United States of America Patriot Act of 2001, H.R. 3162, 107th Cong. §351 (a) (2001). Under the USAPA, anti-money laundering programs have been added and penalties for violations of geographic targeting orders and certain recordkeeping requirements have been increased and lengthened as well as the effective period of geographic targeting orders. United States of America Patriot Act of 2001, H.R. 3162, 107th Cong. §§ 352-353 (2001). Furthermore, any data concerning money laundering efforts related to the funding of acts of international terrorism, and efforts directed at the prevention, detection,

and prosecution of such funding shall be deemed necessary to prevent any money laundering in support of terrorism. United States of America Patriot Act of 2001, H.R. 3162, 107th Cong. §354 (2001). In addition, Congress has gone so far as to create a financial crimes enforcement network to battle terrorism.

The USAPA also supports taking away citizen's liberties at certain areas such as the airports. At the airport, government agencies and police departments have the right to search and seize any unusual objects or products that may cause terrorist threats or pose any clear and present danger. If anyone is seized with a high amount of cash, it tends to cause suspicion that such monies may be used for terrorism and the transportation and smuggling of cash in bulk form may now be the most common form of money laundering. The movement of large sums of cash is one of the most reliable warning signs of drug trafficking, terrorism, money laundering, racketeering, tax evasion and similar crimes. In their effort to avoid using traditional financial institutions, drug dealers and other criminals "are [now] forced to move large quantities of currency in bulk form to and through the airports, border crossings, and other ports of entry where the currency can be smuggled out of the United States and placed in a foreign financial institution or sold on the black market." United States of America Patriot Act of 2001, H.R. 3162, 107th Cong. §371(a) (1)-(3) (2001). With the amendments that were created with the USAPA, it makes the act of smuggling bulk cash itself a criminal offense; authorizing the forfeiture of any cash or instruments of the smuggling offense; and emphasizes the seriousness of the acts such as bulk cash smuggling.

The USAPA and Immigration

Under Title IV of the USAPA, it provides for Congress to take any role necessary to protect U.S. borders and when necessary, may discriminate against non-U.S. citizens. Since the September 11 attacks, the U.S. has allowed many more disabilities of the rights of citizens that used to be afforded. The U.S. must now take strategic and careful decision making when reviewing a foreign citizen's requests for domicile in the U.S. or in reviewing potential visa applications. Currently, the Department of State is now allowed to identify certain information to see any criminal history of a person applying for a visa and becoming an applicant for admission into the U.S**.** United States of America Patriot Act of 2001, H.R. 3162, 107th Cong. §403 (2001). By closing our borders, we are able to keep terrorists out of the country which deters them from committing certain acts of aggression. The problem that faces the U.S. is what procedures can be used to review any citizen that already has a current visa and get them out of the U.S.

In order to combat terrorism, immigration must be controlled. The U.S. is mainly concerned with determining who has been associated with a terrorist organization and intends to do such activity and that they will not endanger the welfare, safety, or security of the U.S. United States of America Patriot Act of 2001, H.R. 3162, 107th Cong. §411 (f) (2001). The USAPA expands judicial review powers, and the mandatory detention of suspected terrorists. In light of the terrorist attacks perpetrated against the United States on September 11, it is the idea of the Congress that the Attorney General, in consultation with the Secretary of State, "should fully implement the integrated entry and exit data system for airports, seaports, and land border ports of entry, as specified in §110 of the

Illegal Immigration Reform and Immigrant Responsibility Act of 1996 with all deliberate speed and as expeditiously as practicable." United States of America Patriot Act of 2001, H.R. 3162, 107th Cong. §414 (2001).

Other important areas that the USAPA has amended include: homeland security, the preservation of immigration benefits for victims of terrorism and humanitarian relief for certain surviving spouses and children. United States of America Patriot Act of 2001, H.R. 3162, 107th Cong. §§ 421 & 423 (2001). Furthermore, Title V of the USAPA allows for the removal of obstacles relating to the investigating of terrorist acts. It allows the "Attorney General's authority to pay rewards to combat terrorism, Secretary of State's authority to pay rewards and DNA identification of terrorists and other violent offenders. All of these new powers however, can limit the constitutional rights of non-citizens and are broad which allow for different interpretations by different federal agencies." United States of America Patriot Act of 2001, H.R. 3162, 107th Cong. §§501-503 and §507 (2001).

Conclusion

A central effort needs to be made to ensure homeland safety and security by keeping a close eye on our air and sea ports, borders, train systems, public bus and water ways. Congress has determined that all Americans are united in condemning terrorist acts and to punish those terrorists who planned and carried out the attacks against the United States on September 11, 2001, and in pursuing all those responsible for those attacks and their sponsors until they are brought to justice. Many citizens have suffered both verbal and physical assaults as a result of misguided anger toward Arab-Americans and Muslim-Americans in the wake of the September 11 terrorist attacks. Congress

declared that, in the quest to identify, locate, and bring to justice the perpetrators and sponsors of the terrorist attacks on the United States on September 11, the civil rights and civil liberties of all Americans should be protected and Congress condemned bigotry and any acts of violence or discrimination against any Americans and called upon local and Federal law enforcement authorities to work to prevent crimes against all Americans. What Congress intends does not always seep down to law enforcement and government agencies when the time comes to make an arrest or detain a citizen. In such a situation, many Americans feel that those agencies have too much power and since September 11, have more power then necessary. The issue weighed though, is we must allow law enforcement and government agencies like the FBI and CIA to power to safeguard our homeland no matter what the costs or negative factors are. By taking away a few constitutional rights of a few citizens, we protect the overall sanctity of millions of American citizens who want terrorism to end forever.