

**TWENTY-FIRST CENTURY ANTITERRORIST LEGISLATION AND
TWENTIETH CENTURY CIVIL RIGHTS
AN ANALYSIS OF THE 2001 U.S.A. PATRIOTS ACT**

RUDY SANDOVAL*

*“They that can give up essential liberty to obtain a little
temporary safety deserve neither liberty nor safety.”*

-Benjamin Franklin

I. INTRODUCTION

In World War II, the attack on Pearl Harbor led to the internment of over 100,000 people, over two-thirds of whom were citizens of the United States, not because of individualized determinations in that they posed a threat to national security or the war effort, but solely for their Japanese ancestry.¹ The internment began in April 1942, and the last camp was not closed² until four years later, in March 1946.³ In the McCarthy era⁴, the United States Congress made it a crime to be a member of the Communist Party, and passed the McCarran-Walter Act,⁵ which authorized the government to keep out and

* Rudy Sandoval, Associate Professor of Business and International Law and Associate Vice President for Administration, The University of Texas at San Antonio.

¹ See Exec. Order 9066, *reprinted in* 50 U. S. C. § 104 (Feb. 19, 1942). President Roosevelt signed the Executive Order allowing the forced exclusion of all persons of Japanese ancestry from the West Coast solely on the basis of race. See also *Conscience and the Constitution* stating that “From March to August, more than 110,000 Japanese Americans are expelled from their homes and businesses and moved to temporary detention centers, most no more than horse stalls at the local racetrack. Japanese Americans lose an estimated \$6-10 billion in property and lost income” available at http://www.pbs.org/conscience/the_story/timeline/index.html (last visited Mar. 15, 2002) (hereinafter *Conscience & the Constitution*).

² See *Conscience & the Constitution*, *supra* note 1. After his re-election to a fourth term, and anticipating the Supreme Court ruling on habeas corpus, President Roosevelt ends the exclusion of Japanese Americans from the West Coast, thus allowing Japanese American to go home. On December 18, 1944 the U.S. Supreme court rules in the *Endo* case that loyal citizens cannot be detained against their will. In *Korematsu* it upholds Executive order 9066 and the army’s eviction of Japanese American.

³ *Civil Liberties and Proposed Anti-Terrorism Legislation: Hearings Before the Subcommittee on the Constitution, Federalism and Property Rights of the Senate Judiciary Committee* (Oct. 3, 2001) (testimony of Prof. David Cole), available at <http://judiciary.senate.gov/te100301sc-cole.htm> (last visited March 18, 2002 [hereinafter Cole]).

⁴ See Tobias Barrington Wolf, *Why We Are Here: A Law Professor Discusses His Difficult Return To The Classroom*, at http://writ.news.findlaw.com/commentary/20010917_wolff.html (last visited Sept. 24, 2001).

⁵ See The McCarran-Walter Bill, Pub.L. No. 82-414 (1952). Pat McCarran was the chairman of the Senate Internal Security Subcommittee that investigated the administrations headed by Franklin D. Roosevelt and

expel non-citizens who advocated Communism or other proscribed ideas, or who belonged to the Communist Party. Under the McCarran-Walter Act, the United States denied visas to, among others, writers Gabriel Garcia Marquez⁶ and Carlos Fuentes. At the time that these actions were initially taken, they all appeared reasonable in light of the threats faced by the nation.⁷ Hopefully the nation has learned from these mistakes. In 1988, Congress paid restitution to the Japanese internees⁸ and in 1990, Congress repealed the McCarran-Walter Act political exclusion and deportation provisions.

The attacks⁹ of September 11, 2001 quite properly spurred renewed consideration of the capability of the United States to forestall future attacks. The Administration proposed, and Congress passed legislation (the U.S.A. Patriot Act, 2001)¹⁰ that gives a wide range of new law enforcement powers¹¹ in an attempt to protect Americans against terrorism.¹²

The focus of this paper is to delineate the major amendments caused by the 2001 antiterrorist legislation that have impacted certain civil liberties protected under the Constitution of the United States. On October 26, 2001, the President of the United States signed the U.S.A. Patriot Act¹³ into law. The Bill is 342 pages long, amends fifteen

Harry S. Truman. In September 1950 he was the chief sponsor of the Internal Security Act. This legislation required registration with the Attorney General of the American Communist Party and affiliated organizations. In June 1952, Pat McCarran and Francis Walter instigated the passing of the McCarran-Walter Act that imposed more rigid restrictions on entry quotas to the United States. It also stiffened the existing law relating to the admission, exclusion and deportation of dangerous aliens as defined in the Internal Security Act, available at <http://www.spartacus.schoolnet.co.uk/USAmccarranA.htm> (last visited Mar. 15, 2002)

⁶ Marquez was the 1982 Nobel Laureate in Literature for his novels and short stories, in which the fantastic and the realistic are combined in a richly composed world of imagination, reflecting a continent's life and conflicts. He wrote ONE HUNDRED YEARS OF SOLITUDE, translated by Gregory Rabassa.

⁷ See Cole, *supra*, note 3.

⁸ See Commerce-Justice-State Appropriations/Japanese-American Reparations, 101st Congress, 1st Session, (Sept. 29, 1989). An excepted committee amendment to the bill amended the Civil Liberties Act of 1988--which established a \$1.3 billion Civil Liberties Public Education fund from which tax-free \$20,000 restitution payments was be made to eligible Americans of Japanese ancestry who were interned during World War II--to make such restitutions, which began on October 1, 1990, entitlements pursuant to the 1974 Budget Act.

⁹ See generally Peter Spiro, *Not War Crimes*, available at http://writ.news.findlaw.com/commentary/20010919_sprior.html (last visited Sept. 24, 2001) ((stating that "many more (civilian) Americans were killed on September 11 than in three of the nation's five declared wars -- the war of 1812, the Mexican War of 1847-48 and the Spanish --American War of 1898- as well as the Persian Gulf conflict.")).

¹⁰ H.R. 3162, 107th Cong., Title 2 (2001), Uniting and Strengthening America by Providing Appropriate Tools required to Intercept and Obstruct Terrorism Act of 2001 [hereinafter U.S.A.Patriots Act].

¹¹ See Russell Covey, *The need for Clarity in Assessing the Terrorist Act: Why the Acts May or May not Constitute War, Crimes, and War Crimes, and Why Definitions Matter*, at http://writ.news.findlaw.com/commerntary/20010925_covey.htm (last visited Sept. 24, 2001) (stating that war is a political act of an essentially forward-looking nature. Wars more typically are fought to remove threats to national or international security, and may be justified before any violent or "criminal" action occurs. Criminal justice, in contrast, is fundamentally backward looking. Punishment is imposed in proportion to the severity of the crime committed, and meted out consistent with notions of justice. An unexecuted threat cannot normally be punished. While war presumes collective responsibility, criminal justice imposes responsibility on individuals.)

¹² See Cole, *supra* note 3.

¹³ See U.S.A Patriots Act .

different statutes, and was passed by the Congress within five weeks of its introduction. The law has given sweeping new powers to both domestic law enforcement and international intelligence agencies and has short-circuited certain checks and balance that previously gave courts the opportunity to ensure that these powers were not abused.¹⁴ The analysis of this paper is limited to Title II –Enhanced Surveillance Procedures of the U.S.A. Patriots Act.

II. ENHANCED SURVEILLANCE PROCEDURE

A. AUTHORITY TO SHARE CRIMINAL INVESTIGATIVE INFORMATION

The U.S.A. Patriot Act tears down the “wall”¹⁵ that has traditionally existed between the government’s authority to conduct counter-intelligence surveillance against foreign powers and terrorist groups, and its authority to conduct criminal investigations¹⁶ of Americans.¹⁷

The Act¹⁸ allows data collected in a criminal investigation to be shared widely, without judicial review, and regardless of whether the activities serve a law enforcement or counter-intelligence purpose.¹⁹ The Act now allows for disclosure of matters occurring before the grand jury, the disclosure of which is prohibited (1) when directed by a court preliminarily to or in connection with a judicial proceeding;²⁰ (2) when permitted by a court at the request of the defendant, upon a showing that grounds may exist for a motion to dismiss the indictment because of matters occurring before the grand jury;²¹ (3) when the disclosure is made by an attorney for the government to another Federal grand jury;²² (4) when permitted by a court at the request of an attorney for the government upon a showing that such matters may disclose a violation of State criminal law to an appropriate official of a State or subdivision of a State for the purpose of enforcing such law;²³ or (5) when the matters involve foreign intelligence or counterintelligence,²⁴ or foreign intelligence information²⁵ to any Federal law enforcement, intelligence, protective,

¹⁴ See EFF Analysis Of The Provisions Of The USA Patriots Act, available at http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html (last visited Mar. 15, 2002)[hereinafter EFF Analysis].

¹⁵ See *id.*

¹⁶ See U.S. A.Patriots Act § 218, amending 50 U.S.C. §§ 1804 (a) (7) (b), 1823(a)(7)(B) (stating that foreign intelligence gathering now only needs to be “a significant purpose” not “the purpose.”).

¹⁷ See Senate Judiciary Committee, Subcommittee on Constitution, Federalism, and Property Rights on *Protecting Constitutional Freedoms in the Face of Terrorism* (Oct. 3, 2001) (testimony of Jerry Berman, Executive Director of the Center for Democracy & Technology), available at <http://judiciary.senate.gov/te1003301sc-berman.htm> (last visited Oct. 10, 2001) [hereinafter Berman].

¹⁸ See U.S.A. Patriots Act.

¹⁹ See *id.* § 212.

²⁰ *Id.* § 203 (a)(1)(C)(i)(I).

²¹ *Id.* § 203 (a)(1)(C)(i)(II).

²² *Id.* § 203 (a)(1)(C)(i)(III).

²³ *Id.* § 203 (a)(1)(C)(i)(IV).

²⁴ See National Security Act § 3, 50 U.S.C. § 401a (1947).

²⁵ See U.S.A. Patriots Act § 203 (a)(1)(C)(iv). *Foreign Intelligence information* means information whether or not concerning a United States Person, that relates to the ability of the United States to protect against

immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties.²⁶

1. HOW DISCLOSURE SHALL BE MADE

If the court orders disclosure of matters occurring before the grand jury, the disclosure shall be made in such manner, at such time, and under such conditions as the court may direct.²⁷

2. HOW THE INFORMATION IS TO BE USED

Any Federal official to whom information is disclosed concerning foreign intelligence or counterintelligence²⁸ or foreign intelligence information²⁹ may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information. Once the information is disseminated to the FBI, Justice, CIA or other Federal government official, the official may use the information as her or she deems "necessary" in carrying out duties. Within a reasonable time after such disclosure, an attorney for the government shall file under seal a notice with the court stating the fact that such information was disclosed and the departments, agencies, or entities to which the disclosure was made.³⁰ The only procedural requirement is that the government attorney has to submit a notice of disclosure to the court, but the information is sealed and the person whose information is being disclosed does not have to be informed.

(1) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (2) sabotage or international terrorism or (3) or clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of foreign power or (4) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to the national defense or the security of the United States; or the conduct of the foreign affairs of the United States.

²⁶ See *id.* § 203 (a)(1)(C)(i)(V).

²⁷ See *id.* § 203 (a)(1)(C)(ii).

²⁸ See National Security Act, §3, 50 U.S.C. §401a (1947).

²⁹ See U.S.A. Patriots Act § 203 (a)(1)(C)(iv). *Foreign Intelligence information* means information whether or not concerning a United States Person, that relates to the ability of the United States to protect against (1) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (2) sabotage or international terrorism or (3) or clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of foreign power or (4) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to the national defense or the security of the United States; or the conduct of the foreign affairs of the United States. See also *id.* § 203 (a)(1)(C)(iv)(II) Information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to-- (aa) the national defense or the security of the United States; or (bb) the conduct of the foreign affairs of the United States.

³⁰ See *id.* § 203 (a)(1)(C)(iii).

B. AUTHORITY TO SHARE ELECTRONIC, WIRE, AND ORAL INTERCEPTION INFORMATION

The U.S.A. Patriots Act³¹ allows data collected in a criminal investigation to be shared widely and used for any number of activities, without judicial review and regardless of whether those activities serve a law enforcement or counter-intelligence purpose. It states that 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 therefrom, 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 counterintelligence³² or foreign intelligence information³³ to assist the official who is to receive (visited Sept. 24, 2001) that information in the performance of his official duties. Certainly, the government's law enforcement and intelligence communities ought to be encouraged to work together, but the terms of their cooperation should be carefully defined, with standards that serve the dual purposes of national security and civil liberties.³⁴ The Act further states that any Federal official who receives information pursuant to this provision may use that information only as "necessary" in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.³⁵ Although the Federal user of the information can only use the information as "necessary," the term is not defined and therefore is open to a broad range of interpretations.

C. FOREIGN INTELLIGENCE INFORMATION

The Act provides for increased information sharing between domestic law enforcement and Federal intelligence officers. This is a partial repeal of the wall put up in the 1970's after the discovery that the FBI and CIA had been conducting investigations on over half a million Americans during the McCarthy era and afterwards.³⁶ The new amendments to the Foreign Intelligence Surveillance Act³⁷ state that it shall be *lawful* for foreign intelligence or counterintelligence³⁸ or foreign intelligence information³⁹ obtained as part of a criminal investigation to be disclosed to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official

³¹ See *id.*

³² See National Security Act § 3, 50 U.S.C. 401a (1947).

³³ See U.S.A. Patriots Act.

³⁴ See Berman, *supra* note 17.

³⁵ See U.S.A. Patriots Act § 203 (b)(1).

³⁶ See *Provisions of the USA Patriot Act That Relate to Online Activities* (Oct. 31, 2001), available at http://www.eff.org/privacy/surveillance/terrorism_militias/20011031_eff_usa_patriot_analysis.html (last visited Mar. 5, 2002) [hereinafter *Provisions*].

³⁷ 50 U.S.C. 36, Foreign Intelligence Surveillance Act (1947).

³⁸ See National Security Act *supra* note 32.

³⁹ See U.S.A. Patriots Act § 203 (b)(2)(19 for the definition of "foreign intelligence information."

duties.⁴⁰ It also 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.⁴¹ Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.⁴² Whether law enforcement and intelligence agencies will use these new powers carefully and limit their use to bona fide investigations remains to be seen since the statute does not articulate appropriate punishment to those who misuse the new powers, nor is there court supervision.⁴³

III. EXPANDED SURVEILLANCE AUTHORITY

United States law has traditionally provided four basic mechanisms for surveillance on persons living in the United States, but the U.S.A. Patriots Act has amended them. The four basic mechanisms were: (1) interception orders authorizing the interception of communications;⁴⁴ (2) search warrants authorizing the search of physical premises and seizure of tangible things like books or other evidence;⁴⁵ (3) "pen register" and "trap-and-trace" orders which authorize the collection of telephone numbers dialed to and from a particular communication device;⁴⁶ and (4) subpoenas compelling the production of tangible things, such as records.⁴⁷ Each mechanism had its own proof standards and procedures based on the U.S. Constitution, statutes or both.⁴⁸ The new act has lowered the standards for obtaining these surveillance tools.

Originally, the Foreign Intelligence Surveillance Act (FISA) was limited to electronic eavesdropping and wiretapping.⁴⁹ In 1994 it was expanded to permit covert physical entries in connection with "security" investigations.⁵⁰ In 1998, it was amended to permit pen/trap orders.⁵¹ In 2001, the U.S.A. Patriots Act expanded the power again to include "roving surveillance authority."⁵² The new "roving wiretap" authority permits the government to intercept, for example, all Internet communications coming from a public Internet terminal, no matter who is using it, if a suspected terrorist is seen using that terminal.⁵³ The standards under FISA are much lower than the standards for criminal wiretaps. Moreover, the surveillance is supposed to be focused on the collection of

⁴⁰ See *id.* § 203 (d)(1).

⁴¹ See *Provisions*, *supra* note 36.

⁴² See U.S.A. Patriots Act § 203 (d)(1).

⁴³ See *Provisions*, *supra* note 36.

⁴⁴ See U.S.A. Patriots Act § 202.

⁴⁵ See *id.* § 501, Access to records and other items under the Foreign Intelligence Surveillance Act.

⁴⁶ *Id.* § 214, Pen Register and Trap and Trace Authority under FISA.

⁴⁷ See *id.* § 210, Scope of subpoenas for records of electronic communications.

⁴⁸ See *Provisions*, *supra* note 36.

⁴⁹ See 50 U.S.C. § 1801(f).

⁵⁰ See *id.* §§ 1821-1829.

⁵¹ *Id.* §§ 1841-1846. FISA can also be used to obtain certain business records. See *id.* §§ 1861-62.

⁵² *Id.* § 1805 (c)(2)(B).

⁵³ See Berman, *supra* note 17.

intelligence, not criminal evidence. For instance, when surveillance is conducted for domestic law enforcement purposes, the probable cause standard of the Fourth Amendment applies to interception orders and search warrants. But a court order compelling an ISP to produce e-mail logs and addresses of past e-mail correspondence uses a lower standard. The lower standard is that the government must show specific and articulable facts showing reasonable grounds to believe that the records are relevant and material to an ongoing criminal investigation. On the other hand, a pen/trap order uses an even lower standard, for example, the government need only tell the court that the surveillance is relevant to a criminal investigation. The standard for subpoenas is also very low.⁵⁴

Under the U.S.A. Patriots Act, the duration of FISA surveillance of non-United States persons who are agents of a foreign power has been extended. An order of the FISC may approve electronic surveillance of an agent of a foreign power for the period specified in the application or for 120 days, whichever is less.⁵⁵ In addition, an order issued under the Foreign Intelligence Surveillance Act of 1978 may be approve for a physical search for the period necessary to achieve its purpose, or for 90 days,⁵⁶ (formerly 45 days) whichever is less. In addition, a physical search concerning a foreign power may be obtained for the period specified in the application or for 120 days, whichever is less.⁵⁷ The FISA court, which last year approved more than 1,000 surveillance requests, has denied only one request in its twenty-two year history. Furthermore, an extension of the surveillance may only be extended against an agent of a foreign power and not a United States person,⁵⁸ for the period specified in the application or for a period not to exceed one year.⁵⁹

IV. DESIGNATION OF JUDGES

FISA allows a secret court⁶⁰ to authorize United States intelligence agencies to conduct surveillance using each of the four basic mechanisms listed above.⁶¹ The courts' system has been expanded. The FISA dictates that the Chief Justice of the United States shall publicly designate seven district court judges from seven of the United States judicial circuits who shall constitute a court which shall have jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States.⁶² The U.S.A. Patriot Act changes the number of district court judges from

⁵⁴ See Provisions, *supra* note 36.

⁵⁵ See U.S.A. Terrorist Act § 207. The new legislation extended the surveillance from 90 days to 120 days.

⁵⁶ *Id.*, which changes the number of days from 45 to 90.

⁵⁷ *Id.* § 207 (1a)(2)(C).

⁵⁸ See *id.* § 207 (b)(2).

⁵⁹ See *id.* § 207(b)(1)(B)

⁶⁰ See generally, Patrick S. Poole, *Inside America's Secret Court: The Foreign Intelligence Surveillance Court*, available at <http://fly.hiwaay.net/~pspoole/fiscsort.html> (last visited Dec.20, 2001).

⁶¹ See Provisions, *supra* note 36.

⁶² See Title 50 U.S.C. § 1803(a) Designation of judges.

seven to eleven,⁶³ and requires that no fewer than three shall reside within 20 miles of the District of Columbia.⁶⁴

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, and the Attorney General must certify that “the purpose” of the surveillance is to gather foreign intelligence information. The secret court’s role here, however, is quite limited in that it is not suppose to “second-guess” the government’s certifications or representations. Hence, the court has denied only one application in its twenty-plus years existence. Furthermore, FISA does not require that status reports be submitted to the court and therefore, the court is left without supervisory powers.⁶⁵

V. SEIZURE OF VOICE-MAIL MESSAGES PURSUANT TO WARRANTS

The new Act also increases the power of government surveillance to include the seizure of voice-mail messages pursuant to warrants⁶⁶ by giving extended power to a governmental entity that may require disclosure from a provider of electronic communications service with respect to the content of “wire” or electronic communication.⁶⁷

VI. SCOPE OF SUBPOENAS FOR RECORDS OF ELECTRONIC COMMUNICATIONS

Under the old statute, a provider of electronic communications service or remote computing service had to disclose to a governmental entity, with proper jurisdiction and authority the (1) name, (2) address, and (3) local and long distance telephone toll billing records, (4) telephone number or other subscriber number or identity, (5) length of service of a subscriber to or customer of such service, and (6) the types of services the subscriber or customer utilized.⁶⁸ The U.S.A. Patriot Act expands the content of information sought to include (1) local and log distance telephone connection records,⁶⁹ or records of session times and duration, (2) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address,⁷⁰ (3) means and source of payment for such service (including any credit card or bank account

⁶³ See U.S.A. Patriot Act § 208 (1), modifying § 103(a) of the Foreign Intelligence Surveillance Act of 1978 50 U.S.C. 1803(a).

⁶⁴ See *id.*

⁶⁵ See *Provisions, supra* note 61.

⁶⁶ See U.S.A. Patriots Act § 209, amending title 18 U.S.C, §§ 2510 (1), (14).

⁶⁷ *Id.* § 2703, Requirements for governmental access.

⁶⁸ See 18 U.S.C. Part I Chap. 121 § 2703(c), Requirements for governmental access.

⁶⁹ See U.S.A .Patriots Act § 210 (1) (C), Scope of subpoenas for records of electronic communications.

⁷⁰ See U.S.A. Patriots Act § 210 (1)(E).

number) of a subscriber⁷¹ and (4) the types of services the subscriber or customer utilized.⁷²

VII. DISCLOSURE OF ELECTRONIC COMMUNICATIONS

A. VOLUNTARY DISCLOSURE OF CUSTOMER COMMUNICATIONS OR RECORDS

Under the laws of criminal procedure, a person or entity providing a electronic communication service⁷³ or one providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service.⁷⁴ The new statute adds a third status, namely that a provider of remote computing service or electronic communication service to the public shall not knowingly divulge the content of the communication to any governmental entity except the contents of the communications.⁷⁵ Furthermore, under the original statute, a governmental entity may require a provider of remote computing service to disclose the contents of a wire or electronic communication⁷⁶ without required notice to the subscriber or customer, if the governmental entity obtains a warrant, or alternatively with an administrative subpoena or a court order if prior notice is given by the governmental entity to the subscriber or customer.⁷⁷ The new Act allows a service provider to divulge a customer's communication to a governmental entity if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay.⁷⁸ Similarly, a provider may also divulge a record or other information pertaining to a subscriber to or customer of such service under the same circumstances.⁷⁹

B. REQUIRED DISCLOSURE OF CUSTOMER COMMUNICATIONS OR RECORDS

The U.S.A. Patriots Act changes the caption of Section 2703 of Title 18 of the United States Code from "Requirements For Governmental Access" to "Required Disclosure of Customer Communications or Records."⁸⁰ Previously, records concerning electronic communication service or remote computing service could only be disclosed to a

⁷¹ *Id.* § 210 (1) (F).

⁷² *See id.* § 210 (2), Scope of subpoenas for records of electronic communication, amending 18 U.S.C. § 2703(c) (2).

⁷³ *See* 18 U.S.C. § 2702(a)(1)

⁷⁴ *See id.* § 2702(a)(2) Crimes and Criminal Procedure.

⁷⁵ *See* U.S.A. Patriots Act § 212(a)(1)(B)(iii).

⁷⁶ *See* 18 U.S.C. § 2703 (b)(1).

⁷⁷ *Id.* § 2703(b)(2)(B).

⁷⁸ *See* U.S.A. Patriots Act § 212(a)(D)(3).

⁷⁹ *Id.* a§ 212(a)(E).

⁸⁰ *See id.* § 212(b)(1)(A,) amending 16 U.S.C. § 2703.

subscriber or customer of such service but not to a governmental entity.⁸¹ The new Act states that a governmental entity may require a provider of electronic communication service or remote computing service⁸² to disclose records or other information pertaining to a subscriber to or customer of such service.⁸³

VIII. DELAYING NOTICE OF EXECUTION OF A WARRANT

Section 3103a of Title 18 of the United States Code provides additional grounds for issuing a warrant. A warrant may be issued to search for and seize any property that constitutes evidence of a criminal offense in violation of the laws of the United States.⁸⁴ Under this section a notice can be delayed for a court order or an administrative subpoena for a period not to exceed ninety days if there is reason to believe that notification of the existence of the court order or subpoena may have an adverse result.⁸⁵ The new Act amends Section 3103a by adding that the issuance of the warrant or a court order to search for and seize any property or material that constitutes evidence of a criminal offense in violation of the laws of the United States may be delayed if (1) the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result,⁸⁶ (2) the warrant prohibits the seizure of any tangible property, any wire⁸⁷ or electronic communication⁸⁸ or, except as expressly provided in chapter 121, any stored wire or electronic information, except where the court finds reasonable necessity for the seizure; and (3) the warrant provides for the giving of such notice within a reasonable period of its execution, which period may thereafter be extended by the court for good cause shown.⁸⁹ The consequence is that notice may be deferred either temporarily or indefinitely with respect to the issuance of a warrant.

⁸¹ See 18 U.S.C. § 2703(c).

⁸² See U.S.A. Patriots Act § 212(b)(1)(C)(i), amending 16 U.S.C. § 2703.

⁸³ See 18 U.S.C. § 2703(c).

⁸⁴ *Id.* § 3103a, Additional Grounds for Issuing Warrant.

⁸⁵ *Id.* § 2705(a)(A), (B).

⁸⁶ See U.S.A. Patriots Act, § 213(2) amending 18 U.S.C. § 3103a. Adverse Results means (A) endangering the life or physical safety of an individual;(B) flight from prosecution;(C) destruction of or tampering with evidence; (D) intimidation of potential witnesses; or (E) otherwise serious jeopardizing an investigation or unduly delaying a trial. See, 18 U.S.C. § 2705(a)(2).

⁸⁷ See 18 U.S.C. § 2510 (stating that “wire communication” means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including switching devices)).

⁸⁸ See U.S.A. Patriots Act § 213(2), amending 18 U.S.C. § 3103a. See also 18 U.S.C. § 2510, stating that “Electronic Communication” means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system that affects interstate or foreign commerce.

⁸⁹ See *id.* § 213(2).

IX. PEN REGISTER AND TRAP AND TRACE AUTHORITY

Under the old Act, the Attorney General could make an application for an order or an extension of an order authorizing or approving the installation and use of a pen register⁹⁰ or trap and trace device for any investigation to gather foreign intelligence information⁹¹ or information concerning international terrorism being conducted by the FBI under the supervision of the Attorney General.⁹² The new Act, on the one hand, ensure that foreign intelligence information obtained under this section does not concern a United States person,⁹³ but on the other hand, it adds that the government may obtain information on clandestine intelligence activities on a United States person so long as the investigation is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution.⁹⁴ In other words, investigations on United States persons are now allowed so long as their First Amendment rights are not violated.

With respect to pen registers and trap and trace devices for foreign intelligence and international terrorism investigations, the original statute required that each application for an order be approved by the Attorney General and certified by the applicant that the information likely to be obtained is relevant to the ongoing foreign intelligence or international terrorism investigation.⁹⁵ The new law requires that the information be relevant to an ongoing investigation to protect against international terrorism, and it adds clandestine intelligence activities.⁹⁶ In addition, the investigation may also be against a United States person so long as the investigation is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.⁹⁷ Furthermore, the information likely to be obtained does not have to be relevant to the ongoing investigation so long as the information is foreign intelligence information and does not concern a United States person.⁹⁸

Furthermore, under the original statute each application required the approval of the Attorney General and included information which demonstrates that there is reason to believe that the telephone line to which the pen register or trap and trace device is to be attached, or the communication instrument or device to be covered by the pen register or trap and trace device, has been or is about to be used in communication⁹⁹ with an individual who is engaging or has engaged in international terrorism or clandestine

⁹⁰ *Id.* at § 216 (c) (2) means dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communications.

⁹¹ *See* 50 U.S.C. § 1842(a)(1).

⁹² *See id.*

⁹³ *See* U.S.A. Patriots Act § 214(a).

⁹⁴ *Id.* § 214(a), amending the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1842.

⁹⁵ *See* 50 U.S.C. § 1842(c)(2).

⁹⁶ *See* U.S.A. Patriots Act § 214(a)(2).

⁹⁷ *Id.*

⁹⁸ *Id.* §214.

⁹⁹ *See* 50 U.S.C. § 1842(c)(3).

intelligence activities or foreign power or agent of a foreign power.¹⁰⁰ The new Act simply removes these requirements for obtaining an application under these conditions.¹⁰¹

The Government has also obtained, under the U.S.A. Patriots Act, the authority for the court to enter an Exparte Order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States so long as it is certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.¹⁰² Similarly, the Act authorizes nationwide service of search warrants for electronic evidence by expanding the definition of court of competent jurisdiction to include any Federal court without geographic limitation.¹⁰³

A. INVESTIGATION OF UNITED STATES PERSONS IS INCLUDED

Under the Foreign Intelligence Surveillance Act, upon an application, a judge could enter an ex parte order as requested, approving the installation and use of a pen register or trap and trace device if certain requirements were satisfied.¹⁰⁴ These requirements included (1) the identity of the person, if known, who is the subject of the foreign intelligence or international terrorism investigation¹⁰⁵ and (2) in the case of an application for the installation and use of a pen register or trap and trace device with respect to a telephone line.¹⁰⁶ The U.S.A. Patriots Act eliminates the requirement that the person be the subject of foreign intelligence or international terrorism and simply requires that the identity of the person, if known, who is the subject of the investigation,¹⁰⁷ be given, therefore broadening the classifications of persons for whom an order can be obtained. The new act classifies three types of persons that must be identified, if known: (1) the person to whom the equipment is leased; (2) the person whose name is listed in the telephone line; or (3) other facility to which the pen register or trap and trace device is to be attached or applied.¹⁰⁸

¹⁰⁰ See *id.* §§ 1842C(c) (A), (B).

¹⁰¹ See U.S.A. Patriots Act § 214(a)(3).

¹⁰² *Id.* § 216(b)(1)(a)(1), stating that the order shall apply to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order.

¹⁰³ See *id.* § 220(a) (3), Nationwide Service of Search Warrants for Electronic Evidence.

¹⁰⁴ See 50 U.S.C. § 1842 (d).

¹⁰⁵ *Id.* § 1842 (d)(2)(A)(i)

¹⁰⁶ *Id.* § 1842 (d)(2)(A)(ii)

¹⁰⁷ See U.S.A. Patriots Act § 214(a)(4)(i), amending 50 U.S.C. § 1842(d)(2)(A).

¹⁰⁸ *Id.* § 214 (a)(4)(ii). The new Act also requires that the application specify “the attributes of the communications to which the order applies, such as the number or other identifier, and if known, the location of the telephone line or other facility to which the pen register or trap and traces devices is to be attached or applied and, in the case of a trap and trace device, the geographic limits of the trap and traces order.” *Id.* § 214 (a)(4)(iii).

B. AUTHORIZATION DURING EMERGENCIES

Under the Foreign Intelligence Surveillance Act¹⁰⁹ the Attorney General could grant authorization for the installation and use of a pen register or trap and trace device on an emergency basis to gather foreign intelligence information or information concerning international terrorism.¹¹⁰ The new Act broadens the power of the Attorney General by amending the Foreign Intelligence Surveillance Act by striking out “foreign intelligence information or information concerning international terrorism,” and allows the collection of information to protect against international terrorism in addition to 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 to the Constitution.¹¹¹ In other words, under the new Act, information against Americans may be investigated if they are involved in clandestine intelligence activities, and provided their First Amendment rights are not violated.

X ACCESS TO CERTAIN BUSINESS RECORDS

The former Foreign Intelligence Surveillance Act¹¹² stated that with respect to having access to certain business records for foreign intelligence and international terrorism investigation, the Director of the Federal Bureau of Investigation or a designee “may make an application for an order authorizing a common carrier, public accommodations facilities, physical storage facility, or vehicle rental facilities to release records in its possession for an investigation to gather foreign intelligence information or an investigation concerning international terrorism.¹¹³ The U.S.A. Patriots Act¹¹⁴ defines the type of business records to be obtained and further states that an order may be obtained requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism.¹¹⁵ The new Act also expands the reason for the investigation to include 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 to the Constitution.¹¹⁶ This means that the United States person can now be placed under surveillance under the Foreign Intelligence Surveillance Act (FISA).

¹⁰⁹ See 50 U.S.C., Chap. 36 Foreign Intelligence Surveillance Act, Subchap. III, Pen Registers and Trap and Trace Devices.

¹¹⁰ See *id.* at § 1843(a).

¹¹¹ See U.S.A. Patriots Act § 214 (b)(1).

¹¹² See 50 U.S.C. at Subchap. IV Access to Certain Business Records for Foreign Intelligence Purposes.

¹¹³ See 50 U.S.C. § 1862(a), Access to Certain Business Records.

¹¹⁴ See U.S.A. Patriots Act § 215, Access to Certain Business Records for Foreign Intelligence and International Terrorism investigations.

¹¹⁵ *Id.* § 215 (a)(1), amending Title V of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1861.

¹¹⁶ See *id.* § 215 (a)(1), amending Title V of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1861.

Moreover, FISA required that the application for the order articulate specific facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power.¹¹⁷ The U.S. Patriots Act reduces the standard to obtain the order, and the Attorney General is only required to specify that the records concerned are sought for an authorized investigation to obtain foreign intelligence information to protect against international terrorism or clandestine intelligence activities.¹¹⁸

In other words, under the new Act, the standard for obtaining the order is lower, and the order is no longer restricted to foreign agents or foreign powers only. Furthermore, FISA states that no person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section.¹¹⁹ In addition, FISA provides protection for the person who in good faith produces tangible things under an order pursuant to this section, and will not be held liable to any other person for producing the evidence.¹²⁰

XI. CONGRESSIONAL OVERSIGHT

Twice a year, the Attorney General is required to fully 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.¹²¹ The statute does not require the Attorney General to provide information about the investigation with any specificity except to inform the committees about the requests that were made to the court to obtain an order. In addition, twice a year, the Attorney General has to provide to the Committees on the Judiciary of the House of Representatives and the Senate a report setting forth with respect to the preceding six-months¹²²: (1) the total number of applications made for orders approving requests for the production of tangible things,¹²³ and (2) the total number of such orders either granted, modified, or denied.¹²⁴ No further information is required. In other words, there is little or no supervision concerning surveillance activities conducted by the Attorney General.

¹¹⁷ See The Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1862 (b)(2)(B).

¹¹⁸ See U.S.A. Patriots Act § 215 (b)(2), amending Title V of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1862 (b)(2)(B).

¹¹⁹ See U. S. Patriots Act § 215 (d).

¹²⁰ *Id.* § 215 (e).

¹²¹ *Id.* § 502 (a).

¹²² See *id.* § 502(b).

¹²³ *Id.* at § 502(b)(1).

¹²⁴ See *id.* § 502 (b)(2).

XII. SUNSET PROVISIONS

With some exceptions, the U.S.A. Patriots Act contains a sunset clause that takes effect on December 31, 2005, at which time it will become ineffective.¹²⁵ The exceptions to the sunset clause include (1) authority to share grand jury information;¹²⁶ (2) making it lawful for foreign intelligence or counter intelligence or foreign intelligence information obtained as part of a criminal investigation to be disclosed to any federal law enforcement officer;¹²⁷ (3) the employment of translators by the Federal Bureau of Investigation;¹²⁸ (4) the expansion of the Foreign Intelligence Surveillance Courts from seven to eleven;¹²⁹ (5) the expansion of the subpoena power for records of electronic communication;¹³⁰ (6) authority for delaying notice of the execution of a warrant;¹³¹ (7) access to business records for foreign intelligence and international terrorism investigations,¹³² and (8) allowing for multiple-jurisdiction search warrants for terrorism.¹³³

XIII. CONCLUSION

On September 11, 2001, thousands of people from all over the world lost their lives in New York as a result of a brutal assault on the United States of America and its form of government.¹³⁴ We have a right to expect that the United States will bring those accountable to justice and the Federal government should have the tools to accomplish this objective.¹³⁵ The people comprise the government of the United States and are, therefore, a partner in ensuring that its will is carried out. Hence, all Americans have an obligation to examine carefully the steps our country may now take to reduce the risk of future terrorist attacks.¹³⁶ We need to consider proposals calmly and deliberately with a determination not to erode the liberties¹³⁷ and

¹²⁵ See *id.* § 224. stating that the sunset clause will not apply to §§ 203(a), 203(c), 205, 208, 210, 211, 213, 216, 219, 221, 222.

¹²⁶ See *id.* § 203(a)(1).

¹²⁷ *Id.* § 203 (c).

¹²⁸ *Id.* § 205.

¹²⁹ See *id.* § 208(1).

¹³⁰ See *id.* §§ 210, 211.

¹³¹ *Id.* § 213.

¹³² See *id.* § 215.

¹³³ *Id.* § 219.

¹³⁴ See Senate Judiciary Committee Subcommittee on the Constitution, Federalism, and Property Rights, 107th Congress (Oct. 3, 2001) (testimony of Gorver Norquist) (hereinafter Norquist).

¹³⁵ See Testimony before the Senate Committee on Governmental Affairs, Homeland Security, A Framework or addressing the Nation's Efforts) (testimony of David M. Walker), available at <http://news.findlaw.com/cnn/docs/gao/homelandsec92101.pdf> (last visited Sept. 21, 2001). See also, generally Reuters, Congress Wrestles with Anti-Terrorism Bill, FindLaw Legal News and Commentary, Sept. 26, 2001), at <http://news.findlaw.com/news/s/20010926/attackcongresssecuritydc.html> (last visited Sept. 26, 2001)

¹³⁶ See Norquist *supra* note 134.

¹³⁷ See Julie Hilden, *The Civil Liberties we need to Keep: Evaluating the Governments Proposals*, at <http://writ.news.findlaw.com/hilden/20010920.html> (last visited Sept. 24, 2001).

freedoms that are at the core of the American way of life.¹³⁸ It is therefore imperative to ensure that actions by the government uphold the principles of a democratic society, that government officials are accountable, and that all decisions are taken in a manner consistent with the Constitution.¹³⁹ The goal should be, as it has been in the past, in times of war and of peace, to reconcile the requirements of security with the demands of liberty. Finally we must have faith in our democratic system and our constitution, and in our ability to protect at the same time, both, the freedom and the security of all Americans.¹⁴⁰

¹³⁸ See Norquist, *supra* note 134. See also Testimony of Gorver Norquist, available at <http://judiciary.senate.gov/te100301sc-norquist.htm> (last visited Mar. 18, 2002)

¹³⁹ *Id.* See also, generally Marci Hamilton, *When Extremists Test the Constitutional Order: Reflections on the Recent Terrorist Act*, at <http://writ.news.findlaw.com/hamilton/20010913.html> (last visited Sept. 24, 2001).

¹⁴⁰ See Norquist, *supra* note 134.