Federalist Society
for Law and Public Policy Studies
Criminal Law and Procedure Practice Group

White Paper
on Anti-Terrorism Legislation:
Surveillance &Wiretap Laws
Developing Necessary and Constitutional Tools for Law Enforcement

Prepared by:

Tom Gede, Chair, Criminal Law & Procedure Practice Group
Montgomery N. Kosma, Gibson Dunn & Crutcher, Washington, D.C.
Arun Chandra, Morgan & Finnegan, New York, NY

November 2001

I. Introduction:

On October 26, 2001, President George W. Bush signed into law the USA-PATRIOT Act of 2001, giving the nation's law enforcement and intelligence services critical new powers to detect, investigate and pursue terrorism and terrorist threats faced by the citizens of the United States. Reflecting on the horrific terrorist attacks of September 11, 2001, the President said the new law would protect constitutional rights while "preventing more atrocities in the hands of the evil ones."[1]

As the President noted at the signing ceremony:

> … [the] legislation gives law enforcement officials better tools to put an end to financial counterfeiting, smuggling and money laundering. Secondly, it gives intelligence operations and criminal operations the chance to operate not on separate tracks, but to share vital information so necessary to disrupt a terrorist attack before it occurs.…
>
> [The] new law … will allow surveillance of all communications used by terrorists, including e-mails, the Internet, and cell phones.… Under this new law, warrants are valid across all districts and across all states. And, finally, the new legislation greatly enhances the penalties that will fall on terrorists or anyone who helps them…. [The earlier] statutes deal more severely with drug-traffickers than with terrorists.
>
> …
>
> This legislation is essential not only to pursuing and punishing terrorists, but also preventing more atrocities in the hands of the evil ones.[2]

In a nutshell, this comprehensive package of laws includes dramatic new approaches and tools for federal law enforcement designed to *prevent* terrorist acts. These new tools include most notably streamlined and enhanced surveillance powers, tools that allow law enforcement to target, observe, listen and read the communications of suspected terrorists. At the same time, they present new challenges for all Americans - from the most pro-law-

[1] *See Bush Comments on Signing New Antiterrorism Law*, at http://usinfo.state.gov/topical/pol/terror/01102600.htm (last visited November 13, 2001).

[2] *Id.*

enforcement to those working to protect civil liberties.

It is now axiomatic that since the shocking attacks of September 11, 2001, the "world has changed." The metamorphosis continues in the weeks and months since "9/11," as new acts of terrorism abruptly thrust themselves into our daily consciousness. Americans, it is said, are profoundly unwitting and naive about their own security, derived in no small measure from their trusting nature, generosity and sense of community. One wonders whether the changes brought about by terrorism on American soil will lead to fundamental and basic changes to our everyday liberties. Will greater surveillance powers for law enforcement agencies threaten these liberties or are they merely the long-needed basic tools for equipping our police officers, detectives and special agents to fight a shadowy, mostly hidden terrorist menace?

Urging passage of new antiterrorist powers, Attorney General John Ashcroft testified before the House Judiciary Committee on September 24, calling for specific tools needed "to identify, dismantle, disrupt and punish terrorist organizations before they strike again."[3] The fight against terrorism has become the highest priority of the Department of Justice. At the same time, General Ashcroft reassured the panel that he was committed to the preservation of basic constitutional liberties. He pledged to "meet the challenge of terrorism within our borders and targeted at our friends and neighbors with the same careful regard for the constitutional rights of Americans and respect for all human beings. ... This Justice Department will never waver in its defense of the Constitution, or relent in our defense of civil rights. The American spirit that rose from the rubble in New York knows no prejudice, and defies division by race, ethnicity or religion."[4]

The Attorney General argued "the deficiencies in our current laws on terrorism reflect two facts. First, our laws fail to make defeating terrorism a national priority. Indeed, we have tougher laws against organized crime and drug trafficking than terrorism. Second, technology has dramatically outpaced our statutes. Law enforcement tools created decades ago were crafted for rotary telephone -- not email, the Internet, mobile communications and voice mail. Every day that passes without dated statutes and the old rules of engagement -- each day that so passes is a day that terrorists have a competitive advantage. ... we are today sending our troops into the modern field of battle with antique weapons. It is not a prescription for victory."[5]

Reflecting a consensus within the law enforcement community, the Attorney

---

[3] *See Attorney General John Ashcroft Testimony Before the House Committee on the Judiciary on September 24, 2001*, at http://www.usdoj.gov/ag/agcrisisremarks9_24.htm (last visited November 13, 2001).

[4] *Id.*

[5] *Id.*

General proposed some long-sought changes in the surveillance tools used by law enforcement for detecting and investigating crimes. He pointed out that "[t]errorists are trained to change cell phones frequently, to route email through different Internet computers in order to defeat surveillance."[6] Thus, he suggested that his "proposal creates a more efficient technology neutral standard for intelligence-gathering, ensuring that law enforcement's ability to trace the communications of terrorists over cell phones, computer networks and the new technologies that may be developed in the years ahead."[7] In response, the Congress listened, acted and passed an anti-terrorism bill that largely included most of the Attorney General's suggestions.[8]

The bill passed by Congress merged provisions of a comprehensive House bill, H.R. 2975, entitled the PATRIOT Act of 2001 (Provide Appropriate Tools Required to Intercept and Obstruct Terrorism),[9] with a Senate bill, S. 1510, entitled the USA Act of 2001 (United and Strengthening America).[10] Eventually labeled the USA-PATRIOT Act of 2001 (hereinafter referred as the Act), the principal surveillance features of the passed legislation include:

- Allows federal officials to obtain a wiretapping order that would follow a suspect to any phone the person uses;

- Allows federal officials to obtain nationwide search warrants for terrorism investigations, including for both electronic mails (e-mail) and physical searches;

- Authorizes nationwide search warrants for computer information in terrorism investigations, including billing records;

- Allows federal officials to seize voice mail records if a judge issues a warrant;

- Requires judicial monitoring of the FBI's use of its Carnivore e-mail tracking system;

---

[6] *Id.*

[7] *Id.*

[8] *See* 115 Stat. 272.

[9] H.R. 2975 was introduced by House Judiciary Chair James F. Sensenbrenner, Jr., on October 2, 2001. While reflecting the Administration's proposed bill, it limited various provisions and passed out of the Judiciary Committee as modified, including various sunset provisions. The House Judiciary bill was subsequently amended roughly to match the Senate bill, and as amended, H.R. 2975 passed the House of Representatives on October 12, 2001, by a vote of 337 to 79.

[10] S.1510 reflected the Administration's proposal, the Anti-Terrorism Act of 2001 ("ATA"), and was introduced, as modified, by Majority Leader Senator Thomas A. Daschle on October 4, 2001. With certain amendments limiting wiretap and computer intercepts, the bill passed the Senate on October 11, 2001, by a vote of 96 to 1.

- Authorizes individuals to sue if the government leaks information gained through the new wiretapping and surveillance powers;

- Adds a Dec. 31, 2005, expiration date or "sunset" for most of the new wiretapping and surveillance powers.

During the congressional debate, the American Civil Liberties Union (ACLU), the Electronic Frontier Foundation (EFF), Electronic Privacy Information Center (EPIC), the Center for Democracy and Technology (CDT) and may other organizations took strong exception to many provisions in the legislation, arguing that they implicate both the principles of the Fourth Amendment and a number of specific federal statutes. This paper examines many of the concerns raised by these organizations and suggests that the surveillance provisions in the final legislation are by and large reasonable and measured, granting the appropriate legal powers to law enforcement investigators in a modern, digital age. As discussed herein, the surveillance provisions, with one notable exception, are subject to a sunset provision, and thus, to some measure of congressional review. Of particular concern to civil libertarians and computer privacy advocates is one section governing a wider pen register and trap and trace authority, including its application to the Internet, discussed more fully below. Section II of this paper provides the principal background statutes that were amended by the USA-PATRIOT Act of 2001. Section III analyzes the principal surveillance-related provisions as to their function, legal impact and constitutionality, where appropriate. Section IV provides recommendations and a conclusion.

II. Background: Governing statutes.

1. The federal wiretap statute.[11] Originating from a 1968 law, the law allows a contemporaneous interception of a wire, oral or electronic communication only upon a showing of "probable cause" and the issuance of a Section 2518 wiretap order or warrant from a federal court, called a "Title III" wiretap order.

2. The pen register and trap and trace statute.[12] This statute permits law enforcement to install and use devices that record phone numbers called by a suspect (pen register) as well as received (trap and trace) upon an ex parte showing to a court that the information likely to be obtained is "relevant to an ongoing criminal investigation." An *ex parte* order under Section 3123 generally is limited to a sixty-day period.

[11] 18 U.S.C. 2510-2522.

[12] 18 U.S.C. 3121-3127.

3. The Electronic Communications Privacy Act of 1986 ("ECPA").[13] This law, at Section 2703(c), allows the government to use an administrative subpoena to compel communication providers to disclose certain transactional records that pertain to electronic communications, such as a customer's name, address and length of service. More revealing electronic records or information may require a court order not unlike that required for a pen register and trap and trace.

4. The Foreign Intelligence Surveillance Act of 1978 ("FISA").[14] Generally, this law allows wiretapping a foreign power or terrorist in the United States on a probable cause showing and is limited to "foreign intelligence." Under Section 1802(a)(1), the Attorney General may authorize immediate surveillance without a court order when he certifies in writing and under oath that (among other conditions) the government will comply in statutory "minimization procedures" (relating to the unnecessary dissemination of nonpublic information), and that there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a "United States person" is a party. In all other circumstances, the government may only conduct electronic surveillance pursuant to an advance procedure for judicial review. A special court of district court judges is established as a FISA court for these purposes. FISA thus provides a heightened standard of review for "United States persons," which include, in general terms, citizens and permanent resident aliens. FISA expressly provides that United States persons shall not be subject to FISA surveillance solely on the basis of their constitutionally protected First Amendment rights.[15]

III. Analysis of USA-PATRIOT Act of 2001: Anti-Terrorism Surveillance Provisions.

Numerous provisions of the USA-PATRIOT Act of 2001 provide for enhanced law enforcement authority to conduct surveillance of suspected terrorist target, mostly found in the Act in TITLE II - ENHANCED SURVEILLANCE PROCEDURES. This analysis focuses on the principal provisions relating to surveillance and information gathered by surveillance in the context of their constitutionality and value for fighting terrorist activity. Sections relating to both surveillance generally and surveillance under the Foreign Intelligence Surveillance Act (FISA) are examined in Parts A and B, respectively.

[13] 18 U.S.C. 2701-2711.

[14] 50 U.S.C. 1801-1811.

[15] 50 U.S.C. § 1805(a)(3)(A) (a "United States person" may not be determined to be an agent of a foreign power "solely upon the basis of activities protected by the first amendment to the Constitution of the United States.").

Part A: Provisions Relating to General Surveillance Authority

1. Nationwide and Internet application of pen registers and trap and trace devices.

Section 216 of the Act authorizes courts to grant pen register and trap and trace ("PR/TT") orders that are valid anywhere in the nation and to facilities other than telephone lines (e.g., the Internet). It amends 18 U.S.C. § 3123(a) by allowing courts to grant orders that are valid "anywhere within the United States" authorizing PR/TT if the court has jurisdiction over the crime being investigated and the government certifies that the information "likely to be obtained" is "relevant to an ongoing criminal investigation," which was the existing standard for the PR/TT application in Section 3122. The additional grant of authority to capture "routing" and "addressing" information for Internet users does not authorize the interception of the content of any such communications. The government is required to use the latest available technology to insure that a pen register or trap and trace device does not intercept content. Additionally, the section requires complete recording and *ex parte* reporting to the court on the details of the use of any "Carnivore"-like devices on packet-switched data networks. Information that must be reported includes which officer or officers installed the device, the date and time the device was installed, operated and uninstalled, and the information collected by the device.

Analysis: This provision is one of the most controversial in the new anti-terrorism law, presenting difficult issues of electronic privacy and law enforcement authority. Law enforcement has long sought the nationwide application of pen register and trap and trace authority, independent of the Internet considerations. Pen registers and trap and trace devices generally do not present the same Fourth Amendment considerations as a Title III wiretap of a wire communication. In *Smith v. Maryland*,[16] the Supreme Court upheld the use of these devices, noting the person using a telephone or communications device "voluntarily exposes" the dialing information to the communications service company, and therefore, there is no legitimate expectation of privacy with respect to that information under *Katz v. United States*.[17] The *Smith* Court further held the devices do not reveal content of the communications.[18]

The new section simply allows courts to grant orders that are valid "anywhere within the United States." That serves as a tool for those investigating terrorism, as it allows investigators to get the source of a wire or electronic communication. Thus, the government will be able to obtain one pen register and trap and trace order that could be

[16] 442 U.S. 735 (1979).

[17] 389 U.S. 347 (1967); *see also United States v. Miller*, 425 U.S. 435 (1976)

[18] 442 U.S. at 741; s*ee also United States v. New York Telephone Co.*, 434 U.S. 159, 166-167 (1977).

applied to any communications provider in the chain of providers carrying the suspect's communications. This provision increases tracing efficiency by eliminating the current need to apply for new orders each time the investigation leads to another jurisdiction. During the congressional debate, the ACLU complained that these provisions marginalize the role of the judiciary and gives a "blank warrant," allowing law enforcement to fill in the "place to be searched," contrary to Fourth Amendment law. Of course, in *Katz*, the Court makes clear that the Fourth Amendment "protects people, not places."[19] Further , it is important to remember that pen registers and trap and trace devices are not directed at the content of the communications, but instead a pen trap device records only the numbers of incoming and outgoing telephone numbers,[20] and their use has been upheld by the Court in *Smith*. Thus, nationwide application does not threaten any legitimate constitutional concern. Additionally, ACLU's view fails to recognize that today's digital technology allows a terrorist, saboteur or anyone misusing electronic communications to reside and move about without regard to "place." Even in investigating the most standard telephonic communications, the requirement to continually re-apply for the authority in venues across a nation that is now thoroughly and digitally interconnected significantly impedes the ability of law enforcement to efficiently follow the chain of communications.

The extension of this authority to the Internet does appear to pose significant privacy issues, however.[21] The original House bill did not include a restriction on "content," but it was added to conform to the Senate bill. Electronic privacy organizations and others[22] continue to express concern that this law allows law enforcement to expand PR/TT orders to "Web surfing," if law enforcement believes it is "relevant to an ongoing criminal investigation." For example, the EFF and the ACLU make the argument that Internet addresses themselves contain "content" - specifically, the URL's a person visits on the Web, a "rich and revealing" form of content. Along with information about the information being accessed by the target, some URL's include content information sent by

[19] 389 U.S. at 361.

[20] The Supreme Court has stressed that the information collected by pen registers is limited. *United States v. New York Tel. Co.*, 434 U.S. 159, 167 (1977) ("Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers."). Recent court decisions have reemphasized that such devices' "only capability is to intercept" the telephone numbers a person calls. *Brown v. Waddell*, 50 F.3d 285, 292 (4th Cir. 1995).

[21] The latest case that comes closest to addressing these concerns is *United States Telecom Association, v. FCC.* 227 F.3d 450 (D.C. Cir. 2000). The court rejected the regulatory standard that would have permitted the incidental receipt of content information in connection with the implementation of the pen register and trap and trace forwarding.

[22] *See generally EFF Analysis Of The Provisions Of The USA PATRIOT Act (*Oct 31, 2001), at http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html (providing analysis of the USA-PATRIOT Act of 2001 by Electronic Frontier Foundation (EFF)); *see also ACLU Legislative Documents*, at http://www.aclu.org/congress/archives.html (last visited November 12, 2001) (containing ACLU's posted press releases on the Anti-terrorism bills).

the user. For example, the results displayed by an Internet search engine usually include the list of search terms typed in by the sender.[23] Such information is not strictly *transactional* information, and yet, under the law, it could be accessible under the lower PR/TT standard for obtain a PR/TT court order. The Electronic Privacy Information Center (EPIC) noted the following concerning the original Administration proposal ("Anti-Terrorism Act," or "ATA") on this matter:

> …The proposed ATA does not take into account the unique nature of such information, which contains data far more revealing than phone numbers, such as URLs generated while using the Web which often contain a great deal of information that cannot in any way be analogized to a telephone number. Although the FBI has compared telephone calls to Internet communications to justify invocation of the existing pen register statute to authorize the use of its controversial Carnivore system, whether current law in fact grants such authority remains an open and debatable question. The proposed amendment would codify the FBI's questionable interpretation of the pen register statute, thereby closing the door to fully informed and deliberate consideration of this complex issue.[24]

It appears that the law's reach into what may be considered "content" in areas of Internet communications may well be the subject of further study or litigation. This amendment is not subject to the "sunset" provisions of the new law, and thus, does not have the built-in remedy of an automatic congressional review.

2. Nationwide scope of subpoenas for records of electronic communications.

In Section 210, the Act amended the ECPA[25] to broaden the types of records that law enforcement may subpoena from electronic communications service providers by requiring providers to disclose the means and source of payment. Previously, the government could only subpoena communications providers for a more limited class of records, such as the customer's name, address, and length of service.

---

[23] *See CDT's Analysis of S. 2092: Amending the Pen Register and Trap and Trace Statute in Response to Recent Internet Denial of Service Attacks and to Establish Meaningful Privacy Protections* (April 4, 2000), at http://www.cdt.org/security/000404amending.shtml.

[24] *Analysis of Provisions of the Proposed Anti-Terrorism Act of 2001* Affecting the Privacy of Communications and Personal Information (September 24, 2001), at http://www.epic.org/privacy/terrorism/ata_analysis.html.

[25] 18 U.S.C. section 2703(c)(1)(C).

Analysis: Obtaining information on certain payments made, including the bank account or credit card numbers, is a long-sought tool for law enforcement facing the exigencies of tracking and monitoring potential terrorist attacks. During congressional debate, the ACLU complained that the Act would cause judges to be bypassed where they should review or supervise these types of record searches. However, in fast-moving investigations, like terrorist bombings cases, Internet communications can be a critical method of identifying conspirators to determine the source of the attacks. Delay encountered in court orders can often undermine the efficacy of a fast-moving investigation. Obtaining billing and other information can identify not only the perpetrator but also give valuable information about the financial accounts of those responsible and their co-conspirators.

3. Seizure of voice mail messages pursuant to warrants.

In Section 209, the Act authorizes government access to voice mails with a court order supported by probable cause in the manner in which e-mails may currently be accessed, and authorizes nationwide service with a single search warrant for voice mails. Previously, the definition of a "wire communication" in 18 U.S.C. § 2510(1) included "any electronic storage of such communication." Consequently, the government was required to apply for a Title III wiretap order before it could obtain unopened voice mail messages held by a service provider. This section amends the definition of "wire communication" to no longer include stored communications. It also amends 18 U.S.C. § 2703 to specify that the government may use a search warrant (instead of a wiretap order) to compel the production of unopened voice mail, thus harmonizing the rules applicable to stored voice and non-voice (e.g., e-mail) communications.

Analysis: This provision eliminates the anomaly inherent in treating voice mail with more regard than other forms of communications that may not subject to a full Title III wiretap order requirement, such as e-mail. It provides an important tool for law enforcement that streamlines and harmonizes the rules for warrants for this kind of surveillance. This provision still calls for the type of court-ordered warrant required for other stored communications under the Electronic Communications Privacy Act (ECPA), not significantly different than what is required for any written document. Given the reasonableness requirement for the court order in Section 2703(d), it does not seem to implicate the Fourth Amendment. In *United States v. Smith*,[26] the court held that third party interception of voice mail falls into a *statutory* category requiring a wiretap order. The court did not, however, find that the Fourth Amendment compels that voice mail must be treated the same as other wire communications. Under this rationale, Congress is empowered to effect the statutory change. This provision of the Act now makes clear that the voice mail in *Smith* is not subject to a Title III wiretap order.

[26] 155 F.3d 1051 (9th Cir. 1998).

During debate, the ACLU position on this provision was that it "extends the same inadequate standards that currently govern e-mail to voice mail, which is content and should be subject to the same standard as a wiretap." Congress has already made a judgment, however, that seizing e-mail (and now voice mail) is not an "intercept" of a contemporaneously acquired communication.[27] And while there may be content involved, again, the material is not significantly different than other stored communications or similar physical evidence seized with a warrant. The courts have deferred to the Congress in cases involving such communications.

4. Adding terrorism, computer fraud to wiretap authority.

Section 201 of the Act, entitled AUTHORITY TO INTERCEPT WIRE, ORAL, AND ELECTRONIC COMMUNICATIONS RELATING TO TERRORISM, adds chemical weapons and terrorism as offenses that are subject to the wiretap probable cause showing in 18 U.S.C. Section 2516 (in Chapter 119 of Title 18), notably Sections 229 (chemical weapons), 2332 (violent crimes against U. S. nationals outside the U. S.), 2332a (use of weapons of mass destruction) 2332b (terrorism transcending national boundaries), 2332d (financial transactions with countries designated as supporting terrorism), 2339A (providing material support to terrorists), and 2339B (providing material support to terrorist organizations). Section 202 of the Act adds computer fraud and abuse to Section 2516's intercept authority. These provisions presented no significant controversy during the congressional debate and nor do any constitutional impediments appear to exist.

5. Providing authority to share wiretap and grand jury criminal investigative information.

Section 203 of the Act, entitled AUTHORITY TO SHARE CRIMINAL INVESTIGATIVE INFORMATION, provides for certain limited sharing of criminal investigative information not heretofore permitted by statute. Section 203(a) amends grand jury procedures under Rule 6(e) of the Federal Rules of Criminal Procedures to authorize disclosure of "foreign intelligence information,"[28] obtained by a grand jury to any Federal law enforcement,

---

[27] *See United States v. Turk*, 526 F.2d 654, 658-659 (5th Cir. 1976) (dealing with contemporaneousness of interception); *Smith*, supra, 155 F.3d at 1056 (dealing with anomalies in treatment of voice mail as stored communication).

[28] The Act allows disclosure of foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a) or "foreign intelligence information." The latter is defined in the USA-PATRIOT ACT generally as: (a) information, "whether or not concerning a United States person," that relates to the ability of the United States to protect against actual or potential attacks of a foreign power; sabotage or international terrorism; or clandestine foreign intelligence activity; and (b) information, "whether or not concerning a United States person," with respect to a foreign power that relates to the national defense or security of the United States or the conduct of the foreign affairs of the United States. This differs from the definition in 50 U.S.C. section 1801(e), which conditions the information as following: "information that relates to, and if concerning a United States person is necessary to ...."

intelligence, protective, immigration, national defense, or national security official to assist the official receiving that information in the performance of his official duties. It also requires that, within a reasonable time after disclosure of any grand jury information, an attorney for the government notify the court of the disclosure and the departments, agencies or entities to which disclosure was made.

Section 203(b) allows the disclosure of foreign intelligence information obtained from the interception of communications pursuant to a court-ordered wiretap to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official. Section 203(c) requires the Attorney General to establish procedures for disclosure of information that identifies a "United States person," roughly defined as a citizen or permanent resident alien, such as the current procedures established under Executive Order 12333 for the intelligence community. Section 203(d) authorizes disclosure of foreign intelligence information obtained as part of a criminal investigation notwithstanding any other law. Recipients may use information only as necessary for their official duties, and use of the information outside those limits remains subject to applicable penalties, such as penalties for unauthorized disclosure under chapter 119, contempt penalties under Rule 6(e) and the Privacy Act.

Analysis: This information-sharing provision was highly controversial and drew considerable criticism and debate in the Congress, and was the principal subject of a statement by Senator Patrick Leahy, Chairman of the Senate Judiciary Committee, on October 25, 2001.[29] Senator Leahy and others warned of potential political abuse of the dissemination of intelligence from domestic investigations.

Clearly, this Act authorizes the expanded sharing with intelligence agencies of information collected as part of a criminal investigation and the expanded use of foreign intelligence surveillance information in criminal investigations. As such, it should facilitate the coordination of efforts by both criminal and foreign intelligence agencies where foreign-sponsored terrorism is the target of an investigation. However, Senator Leahy reminded his audience of "our nation's unfortunate experience with domestic surveillance and intelligence abuses that came to light in the mid-1970s," referring to a time when, until Watergate and the Vietnam war, the Executive branch had a "free hand in using the FBI, the CIA, and other intelligence agencies to conduct domestic surveillance in the name of national security." Senator Leahy pointed to the risks of misusing such information, which was once studied by the Senate Select Committee to Study Governmental Affairs with Respect to Intelligence Communities, chaired by Senator Frank Church. The Church Committee conducted a major investigation and concluded that the FBI's internal security and domestic intelligence programs were used to compile intelligence on activities of U.S. citizens that was protected by the First Amendment. As a result, national intelligence

[29] 147 Cong. Rec. S.10990 (daily ed. Oct. 25, 2001) (statement of Senator Leahy) (discussing information sharing).

agencies and the FBI shared their collected intelligence on certain critics of governmental policy and antiwar protesters. While Congress did not implement all the recommendations of the Church Committee, it did pass FISA, limiting surveillance to foreign powers and agents of foreign powers; it also added the statutory probable cause standard for targeting any American as an "agent of a foreign power" required a showing of clandestine intelligence activities, sabotage, or international terrorist activities on behalf of a foreign power.[30]

In the context of this Act, Senator Leahy expressed concern that highly sensitive personal, political and business information acquired for law enforcement purposes, including information from domestic law enforcement wiretaps, could get disclosed to intelligence, defense, and national security agencies, if it fit the broad definitions of "foreign intelligence" and "foreign intelligence information." He expressed concern that the net not be so wide that it included information about lawful activities, business transactions, political relationships, or personal opinions, and noted that criminal investigations could involve information on persons who are investigated and later cleared, or never prosecuted or for whom immunity is granted.

Nonetheless, Senator Leahy acknowledged that in the current crisis, "there is justification for expanding authority specifically for counterintelligence to detect and prevent international terrorism." He noted that "... none of the changes in FISA would authorize investigations of Americans for the broader, more ambiguous purpose of collecting "foreign intelligence" generally. In that respect, the bill adheres to the basic principles recommended by the Church Committee." Indeed, the Church Committee had suggested the FBI should be permitted to disseminate personally identifiable information about Americans to intelligence, military and other national security agencies in two areas – "preventive criminal investigations of terrorist activities" and "preventive intelligence investigations of hostile foreign intelligence activities."[31]

The Act does provide certain critical safeguards from the abuses suggested by Senator Leahy. As noted, the Act mandates judicial oversight of the dissemination of grand jury information, requiring a government attorney to file with the court a notice under seal that informs the court of the disclosure and of the departments, agencies, or entities to which the disclosure was made. With respect to disclosure of information from wiretaps and other criminal investigative methods, although judicial review is not required, Section 203(c) provides that the Attorney General shall establish procedures for the disclosure of any information obtained by a wiretap or communications intercept that identifies a United States person. And in addition to the various civil and criminal

[30] *See generally* 50 U.S.C. §§ 1801 - 1811.

[31] 147 Cong. Rec. S.10990 (daily ed. Oct. 25, 2001) (statement of Senator Leahy) (discussing information sharing).

sanctions that already exist under Title 18 and FISA, this Act, in Section 223, provides for government liability and administrative discipline against government employees for improper disclosure of information. Finally, the more controversial parts of these provisions are subject to a sunsetting in four years.[32] Congressional oversight should be - and given the Senators' concerns, likely will be - exercised at the time of the sunsetting to determine the utility and risks presented by these provisions.

It should be noted that terrorists of the type who committed the tragic acts against the World Trade Center and the Pentagon on September 11, 2001, may well fall within the definition of "United States persons," which includes within its scope non-citizens, such as resident aliens. The amendments in the Act thus appear warranted and balanced by important safeguards, allowing appropriate sharing of surveillance information on a "United States person" if that information is lawfully obtained under other provisions of this Act. Courts have generally permitted such a limited sharing of lawfully obtained information from surveillance activities, where it is narrowly tied to "foreign intelligence" or "foreign intelligence information."

6. Nationwide service of search warrants for electronic evidence.

Section 220 of the Act provides for nationwide service of search warrants for certain electronic evidence. Prior to passage of the Act, the government was required to use a search warrant under ECPA to compel an Internet service provider (ISP) or similar provider to disclose unopened e-mail.[33] However, under Federal Rule of Criminal Procedure 41, the evidence had to be obtained "within the district" of the issuing court. The Act authorizes a court with jurisdiction "over the offense" to issue search warrants for electronic communications in electronic storage anywhere in the United States, without requiring the intervention of its counterparts in districts where the Internet service providers are located. The term "court of competent jurisdiction" includes any Federal court within that definition, "without geographic limitation." Congress amended the original Administration proposal by requiring the court to be one with jurisdiction "over the offense."

Analysis: This provision is widely regarded as a vital tool in the investigation of terrorism and crime. By way of example, under the law prior to the passage of the Act, an investigator in an Eastern United States city seeking electronic e-mail in the Yahoo! account of a suspected terrorist would have needed to coordinate with agents, prosecutors, and judges in the Northern District of California (i.e., the location of Yahoo! offices), none of whom may have had any other involvement in the investigation. As is apparent, such electronic communications information can be critical in establishing relationships,

[32] *See* Section 224. It should be noted that Sections 203(a) and 203(c) are not subject to the sunset provision.

[33] *See* 18 U.S.C. § 2703(a).

motives, means, and plans of terrorists. Additionally, it may be equally relevant to cyber-incidents in which a terrorist motive has not (but may well be) identified, or in cases that require the quickest response (e.g., kidnapping, threats, or other dangers to public safety or the economy). This new provision minimizes the intervention of other agencies and courts where the major Internet service providers are located. Like the nationwide pen register and trap and trace authority in Section 216, no constitutional bar appears to a nationwide service of search warrants issued by a court with jurisdiction over the offense.

Part B: Provisions Relating to the Foreign Intelligence Surveillance Act of 1978 (FISA)

1. "Roving" Surveillance Authority under the Foreign Intelligence Surveillance Act of 1978.

Section 206 of the USA-PATRIOT Act modifies the Foreign Intelligence Surveillance Act to allow surveillance to "follow" a person who uses multiple communications devices or locations. This conforms FISA to parallel criminal procedures for electronic surveillance in 18 U.S.C. sec. 2518(11)(b).[34] The court order need not specify the person whose assistance in the surveillance is required (such as a particular communications common carrier), where the court finds that the actions of the target may have the effect of thwarting the identification of a specified person, i.e., the common carrier.

Referred to as the "multi-point authority" provision, it expands the obligations of third parties to furnish assistance to the government under FISA. Before the Act, under FISA, a common carrier was required by the court order to furnish the government with information and technical assistance necessary to accomplish electronic surveillance in a manner that will protect its secrecy and produce a minimum of interference with the services that the carrier is providing the target of electronic surveillance. However, international terrorists and agents are trained to thwart surveillance by rapidly changing hotel accommodations, cell phones, Internet accounts, etc., just prior to important meetings or communications. In such situations, the government has to return to the FISA Court for an order that specifies each new carrier, landlord, etc., before effecting surveillance. Under the Act's new provisions, the FBI could simply present the newly discovered carrier, landlord, custodian, or other person with a more generic order issued by the Court and effect FISA coverage as soon as technically feasible. Clearly, this would facilitate a dramatic improvement in the ability to investigate and pursue terrorists "on the move" who are plotting criminal activities.

[34] 18 U.S.C. § 2518(11)(b)(ii), in the section governing procedures for wiretaps, provides that the requirements relating to the specification of the facilities from which a communication is to be intercepted do not apply if the government shows "there is probable cause to believe that the [target's] actions could have the effect of thwarting interception from a specified facility; ..."

The ACLU has criticized this provision, noting that an intercept "is not limited to the target and will lead to interception of many innocent conversations not involving the target."[35] It is precisely for that reason, however, that Congress placed in Title III and FISA strict certification and minimization requirements. Moreover, this provision simply conforms FISA to an existing provision in the basic wiretap law and does not seem to present additional constitutional concerns. A number of courts have held the "roving bug" under Title III does not violate the particularity requirement of the Fourth Amendment,[36] particularly given the narrow circumstances and limitations for its use.

2. Duration of FISA surveillance of non-United States persons who are agents of foreign power.

Section 207 of the Act increases the initial period of a FISA order for surveillance search targeted against an agent of a foreign power from 90 to 120 days, and changes the period for extensions from 90 days to one year. While this provision is narrower than the Administration proposal, which sought to eliminate the initial 90-day limitation and authorize surveillance for up to one year from the outset, the additional time is viewed as useful to government investigators targeting potential terrorist activity. The Administration proposal appeared in the bill passed by the House Judiciary Committee. However, the full House followed the Senate bill model, which provided for initial electronic surveillance orders to expire in 120 days, with extensions up to a year. The change has no effect on electronic surveillance of U.S. citizens.

Analysis: There does not appear to be constitutional or other legal impediments to the congressional direction here. During the debate, the ACLU position was that the extensions "severely" limit the FISA Court's power to ensure that surveillance is continued only when productive. As enacted, however, the surveillance period was not extended to a full year, and by providing for a court-reviewed extension, the FISA Court has an opportunity to review productivity of the surveillance.

3. Pen register and trap and trace authority under FISA.

In Section 214, the Act modified FISA provisions governing pen registers and trap and trace devices to eliminate the requirement of showing to the court that the target is in communication with an "agent of a foreign power." Instead, the pen register or trap and trace must be shown to be "relevant" to an investigation to protect against international

---

[35] *Surveillance Powers: A Chart* (posted on Oct. 10, 2001), at http://aclu.org/congress/patriot_chart.html. *See also EFF Analysis Of The Provisions Of The USA PATRIOT Act (*Oct 31, 2001), at http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html (providing analysis of the USA-PATRIOT Act of 2001 by EFF)..

[36] *See e.g., United States v. Bianco*, 998 F.2d 1112 (2nd Cir. 1993); *United States v. Gaytan*, 74 F.3d 545 (5th Cir. 1996).

terrorism or clandestine intelligence activities or to obtain foreign intelligence information not concerning United States persons. The original Administration proposal would have removed the "agent of a foreign power" requirement only; Congress added the additional relevancy determination requirement.

Analysis: The original Administration proposal was criticized by the ACLU as leading to a potential for increased spying on Americans by intelligence agencies. The addition of the relevancy certification should resolve those concerns. If an investigation does touch upon a United States person (where the investigation is to protect against international terrorism or clandestine intelligence activities), the law adds the following additional proviso: "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.'' As for Fourth Amendment concerns, PR/TT authority does not require the same heightened standards as Title III wiretap authority, as discussed above, because it does not invade comparable expectations of privacy. Accordingly, the provision here should present no legal or constitutional problems under the First or Fourth Amendments.

4. Access to records under FISA.

Section 215 of the Act removes the "agent of a foreign power" standard for court-ordered access to certain business records, papers, documents and other tangible items under FISA. The FBI may make an application to the FISA court or a designated judge whenever needed to protect against international terrorism or clandestine intelligence activities or to obtain foreign intelligence information not concerning United States persons. If it involves a United States person, the access may not be based solely on activities protected by the First Amendment. The original Administration proposal was to grant such authority with an administrative subpoena, but the Congress settled on the requirement for a court order. No constitutional impediment appears to be present here.

5. Broader "purposes" in application for foreign intelligence surveillance order.

Section 218 of the Act amends FISA's certification requirement when an order is sought for electronic surveillance for foreign intelligence information.[37] Under 50 U.S.C. § 1802, the President, through the Attorney General, may authorize electronic surveillance without a court order, generally when there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party.[38] Strict certification and minimization requirements must be followed when the

[37] 50 U.S.C. § 1804(a)(7)(B).

[38] The President's authority (exercise through the Attorney General) under this provision is to acquire foreign intelligence information for periods of up to one year "if the Attorney General certifies in writing under oath that - (A) the electronic surveillance is solely directed at - (i) the acquisition of the contents of communications transmitted by

Attorney General does not seek an order under FISA.[39] Similarly, when a federal officer goes to the FISA court or designated judge for an order for electronic surveillance under the FISA which may involve communications of a United States person, the application requires not only the approval of the Attorney General, based upon his finding that it satisfies strict criteria and requirements, including minimization requirements, but it has required a certification by the Assistant to the President for National Security Affairs or a designated senior executive branch official that, among other things, "the purpose" of the surveillance is to obtain foreign intelligence information.[40] This Act changes the certification requirement to state that "a significant purpose" rather than "the purpose" of the surveillance under FISA is to obtain foreign intelligence information. The Administration proposed the language "a purpose," but Congress opted for a slightly tougher "significant purpose."

Analysis: This single, seemingly small change in FISA language is highly significant in the debate over the reach of FISA surveillance. The effect of the language that required "the purpose" of the surveillance to be the gathering of foreign intelligence information was essentially to require that the "primary" or only purpose of the surveillance be for foreign intelligence information, even if other criminal evidence was to be revealed. Now, under this Act, as long as one of the certified purposes of the FISA surveillance is foreign intelligence information, the court-ordered FISA surveillance should not be stymied by the primary purpose requirement. Critics, such as the ACLU, have stated that this law will bypass "probable cause standards by extending weaker intelligence-gathering wiretap standards to criminal searches. Even [the] 'significant

---

means of communications used exclusively between or among foreign powers [as defined]; or (ii) the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power [as defined]; (B) there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party; and (C) the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures ..." 50 U.S.C. section 1802(a).

[39] The Attorney General must adopt "minimization procedures" that, inter alia, are "reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information; (2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance." 50 U.S.C. section 1801(h).

[40] The requirements of the certification of the national security official include: "(A) the information sought [is] foreign intelligence information; (B) that the purpose of the surveillance is to obtain foreign intelligence information [discussed above]; (C) that such information cannot reasonably be obtained by normal investigative techniques; (D) that designates the type of foreign intelligence information being sought according to the categories described in section 1801(e) of this title; and (E) including a statement of the basis for the certification that - (i) the information sought is the type of foreign intelligence information designated; and (ii) such information cannot reasonably be obtained by normal investigative techniques." 50 U.S.C. 1804(a)(7).

purpose' language will encourage use of FISA rather than more privacy-protective domestic surveillance law."[41]

It should be remembered, however, that FISA, as enacted, provided a statutory scheme that went beyond Fourth Amendment strictures. While the Supreme Court has not specifically addressed the President's authority to authorize a warrantless wiretap for national security purposes, that authority seems sound. For example, in *United States v. United States District Court*,[42] a pre-FISA case, the Court expressed no opinion about the use of warrantless surveillance for national security purposes and limited the opinion solely to its facts. Following *Keith*, lower courts have found that the President has the inherent authority to conduct warrantless surveillance for national security purposes, including for foreign intelligence surveillance.[43] Thus, the procedures set forth in FISA that enable federal law enforcement to conduct electronic surveillance are not mandated by Constitutional concerns. Congress may alter them as appropriate.

In a profile on Department of Justice criminal chief, Assistant Attorney General Michael Chertoff, author Jeffrey Toobin in the November 5, 2001 The New Yorker, wondered whether the built-in reluctance of the FBI to allow criminal evidence that is revealed in FISA surveillance may have prevented early vetting of information about Zacarias Moussaoui, a French Moroccan. Agents asked for authority to conduct FISA surveillance after learning Moussaoui had requested flight school training in how to steer a jetliner, but not how to take off or land; that he had connections to "radical Islamic extremists;" and that he had recently traveled to Pakistan and Afghanistan. The FBI denied the request apparently fearing that potential multiple purposes in the surveillance could undercut any criminal evidence gathered on Moussaoui. Assistant Attorney General Chertoff told Toobin: "The [primary purpose] language [in FISA] has given rise to a mind-set where people feel forced to choose between one kind of investigation and the other. But we can't make that choice anymore."

In testimony on October 3, 2001 before the Senate Judiciary's Subcommittee on the Constitution, Federalism and Property Rights, Cardozo School of Law Professor John O. McGinnis addressed this key provision:

> This change is constitutional. First, . . . it is not at all clear that FISA procedures are required at all when the President or the Attorney General certifies that such

[41] *See ACLU Legislative Documents*, at http://www.aclu.org/congress/archives.html (last visited November 12, 2001) (containing ACLU's posted press releases on the Anti-terrorism bills).

[42] 407 U.S. 297, 321-22 (1972) (This case is commonly known as *Keith* case).

[43] *See, e.g., United States v. Truong Dinh Hung*, 629 F.2d 908, 912 (4th Cir. 1980).

> collection is reasonable given national security considerations. If one of the bona fide purposes of the collection of information is to promote national security, the collection is by definition reasonable in the national security context. [¶] Even more fundamentally, so long as collection has a bona fide national security purpose (and FISA judges are available to make sure that it does) its law enforcement benefits do not undermine its national security justification. To claim otherwise would be to suggest that action which is justified to protect our national security somehow becomes illegitimate if it has other non-illicit, and possibly beneficial, consequences. Moreover, without an expansion of the FISA definition some national security objectives would go unaddressed, because some national security collections may also have substantial law enforcement benefits. Indeed, terrorist acts are simultaneously crimes and profound threats to our national security and thus it would be often difficult for the Attorney General or even a court to determine whether the primary purpose of a collection is national security or terrorism.[44]

Given the President's extraordinary authority in national security matters and the otherwise extraordinarily tight and thorough certification and minimization requirements for FISA surveillance, it seems unlikely that this change in the Act implicates constitutional concerns. At the same October 3, 2001 hearing where Professor McGinnis testified, Catholic University Law School Dean Douglas Kmiec stated:

> Gathering intelligence without meeting the stringent probable cause and notice elements of a traditional Title III criminal investigation are essential to tracking down terrorist activity. The real distinction should not be between intelligence and criminal purposes, but whether the surveillance or search is being effectively directed at terrorist activity, especially that from a foreign source, without having to decide whether at any given time one purpose or the other predominates. . . . [¶]

All proposed Section 153 does is eliminate the statutory basis for judicial challenge to acquired evidence in a subsequent Article III trial of a terrorist suspect.

[44] *Testimony of John O. McGinnis* (October 3, 2001), at http://www.senate.gov/~judiciary/te100301sc-mcginnis.htm.

Without the statutory impediment that the Attorney General seeks to eliminate, to find unconstitutionality under the Fourth Amendment, the Supreme Court would have to both disregard the longstanding claims of inherent presidential authority to protect the national security interests of the United States and, in a circumstance like the present national security emergency, the fact of that emergency. Warrant requirements need not be followed where there is special government need. Searches without warrants or probable cause are generally constitutional "when special needs, beyond the normal need for law enforcement" make these elements unworkable.[45] The Constitutional standard for all searches or surveillance is "reasonableness."[46]

C. Sunsetting Provisions.

The surveillance provisions of the Act are subject to certain sunset limitations. There is a 4-year sunset for most of the provisions discussed above, except for Section 216 of the Act, governing the nationwide and Internet application of pen register and trap and trace authority. Under Section 224 of the Act, the sunsetted provisions will "cease to have effect on December 31, 2005."

IV. RECOMMENDATIONS AND CONCLUSION

The Act presents significant questions for the future of law enforcement in the nation as it faces unparalleled threats from within and without. Attorney General Ashcroft has recently announced he has decided to shift the primary focus of the Department of Justice from investigating and prosecuting past crimes to identifying threats if future terrorist acts, preventing them from happening, and punishing would-be perpetrators for their plans of terror.[47] As he said on October 24, "We cannot wait for terrorists to strike to begin investigations and to take action. The death tolls are too high, the consequences too great. We must prevent first -- we must prosecute second."[48] The tools provided to in the USA-PATRIOT Act are clearly and appropriately directed to meet the challenges posed by the Attorney General.

Probably, the single most difficult issues presented by the new law are those relating

[45] *Veronia School District 47J v. Acton,* 515 U.S. 646 (1995).

[46] *Testimony of Douglas W. Kmiec* (October 3, 2001), at http://www.senate.gov/~judiciary/te100301sc-kmiec.htm.

[47] *U.S. Dept. of Justice press release*, Nov. 8, 2001, "Prevention of Acts Threatening Public Safety and National Security."

[48] *See Attorney General John Ashcroft Testimony Before the House Committee on the Judiciary on September 24, 2001*, at http://www.usdoj.gov/ag/agcrisisremarks9_24.htm (last visited November 13, 2001).

to the provisions governing the nationwide and Internet application of pen register and trap and trace authority, found in Section 216 of the Act. These provisions face criticism by civil libertarians, political libertarians and those interested in protecting privacy on the Internet. As pen register and trap and trace authority have been expanded to allow Internet and e-mail "routing" and "addressing," and as such authority is less than what is required for a Title III wiretap, the law might facilitate a potential acquisition of "content." It is not clear whether there is any deterrent to acquiring or using such information; indeed, inappropriate acquisition may take place for some time before it is discovered and enjoined. Further, as it is not subject to the sunset provisions of the Act, there is no automatic trigger for congressional review. This paper suggests that Congress exercise ongoing oversight in this particular area, which remains of concern to many of the supporters of the enacted USA-PATRIOT Act. This oversight may involve calling upon the Attorney General to report to the Congress on the details of the Department's use of the pen register and trap and trace authority, particularly when following "routing" and "addressing" in electronic communications. While the provision was not sunset in this Act, Congress could amend the provision in future legislation to require renewal of the provision.

Without commenting on the sunsetting provisions in general, this analysis finds that the anti-terrorism tools provided in the USA-PATRIOT Act of 2001 are strong, vital and necessary tools, provided in an extraordinary time of need. The Executive Branch should work closely with the Congress in the next four years to demonstrate the efficacy, necessity and, where necessary, the need for adjustments in this package of key law enforcement powers to fight terrorism.

Finally, this paper also suggests that the Executive Branch can be expected to exercise restraint in the execution of powers granted it by the Congress, certainly during this extraordinary time of heightened demands, unknown threats and increased apprehension affecting the public. While we rely on checks and balances to protect our freedoms, in times like these, we also place a great deal of trust in our law enforcement protectors.

# # #