

PATRIOT ACT

*Uniting and Strengthening America by Providing
Appropriate Tools Required to Intercept and Obstruct Terrorism*

*by Lloyd W. "Tre"
Kitchens, Esquire*

On September 12, 2001, I drove my sister's car from Dallas, Texas to Lander, Wyoming, where she and her family moved, for some reason that still escapes me. Lander is a tiny town of about 3,000 people in the middle of nowhere Wyoming, which is redundant. After a two-day drive, I headed to the tiny Lander airport to catch my flight home to Little Rock, Arkansas. When I arrived at the airport, which was little more than a block building and a hangar, I found that the airport was "barricaded" with old fuel trucks and fire engines, which had been placed several hundred yards from the airport to prevent the impending terrorist attacks.

I submit that the chances of Osama bin Laden mounting further attacks against our country at the Lander airport were small at best. However, the steps taken at the Lander airport are indicative of the panic that gripped America after the attacks. This same panic resulted in the Patriot Act.

Shortly after the September 11 attacks but before the enactment of the USA Patriot Act, President Bush issued Executive Order 13224, effective on September 24, 2001, declaring a national emergency with respect to the "grave acts of terrorism ... and the continuing and immediate threat of further attacks on United States nationals or the United States." Exec. Order No. 13,224, 66 Fed.Reg. 49,079 (2001).

A paralyzing fear of terrorist attacks resulted in the

quick and easy passage of the act. The thrust of the surveillance provisions of the USA Patriot Act is to provide federal agencies with more surveillance options, and less judicial supervision. Under the Patriot Act, we have invited the Federal Government into our lives, and relinquished even more civil liberties to the Government. The 342-page bill makes changes, some large and some small, to over 15 different statutes.

If the Patriot Act were not enough, the Attorney General may now listen in on attorney-client privileged conversations, wherever "reasonable suspicion exists to believe that a particular inmate may use communications with attorneys or their agents to further or facilitate acts of terror-

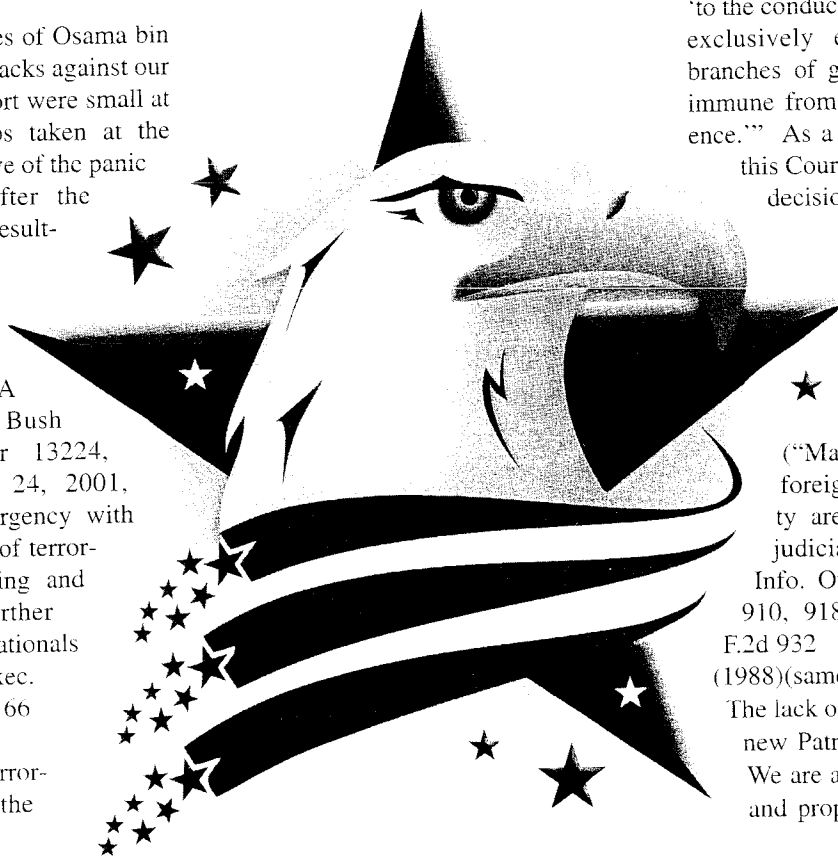
ism. Special Administrative Measure for the Prevention of Acts of Violence or Terrorism 66 Fed.Reg. 55062.

On April 9, 2002 Attorney General John Ashcroft announced the indictment of criminal defense attorney Lynne Stewart on charges that she provided material support to a foreign terrorist organization. The accusation – which Stewart unequivocally denies – was based on information gleaned by listening to conversations between the attorney and her client.

Chief Justice Rehnquist, writing for the Court in *Regan v. Wald*, 468 U.S. 222, 242, 104 S.Ct. 3026, 82 L.Ed.2d 171 (1984), reh'g denied, 469 U.S. 912, 105 S.Ct. 285, 83 L.Ed.2d 222 (1984), quoted from *Harisiades v. Shaughnessy*, 342 U.S. 580, 589, 72 S.Ct. 512, 96 L.Ed. 586 (1952), which stated that "[m]atters related to the conduct of foreign relations...are so exclusively entrusted to the political branches of government as to be largely immune from judicial inquiry or interference." As a general principle, therefore, this Court should avoid impairment of decisions made by the Congress or

the President in matters involving foreign affairs or national security. See *Haig v. Agee*, 453 U.S. 280, 292, 101 S.Ct. 2766, 69 L.Ed.2d 640 (1981) ("Matters intimately related to foreign policy and national security are rarely proper subjects for judicial intervention"); *Palestine Info. Office v. Shultz*, 674 F.Supp. 910, 918 (D.D.C. 1987), aff'd 853 F.2d 932 (1988)(same).

The lack of judicial oversight makes the new Patriot Act even more troubling. We are asked to rely on the good will and proper motives of the Executive



Branch of the Federal Government, without the benefit of public disclosure or judicial oversight.

FISA v. Title III

The Foreign Intelligence Surveillance Act of 1978 [FISA] governs surveillance of foreign persons and agents. Instead of requiring probable cause, surveillance orders are issued on a certification by the Attorney General, which is not related to probable cause in any way. On April 29, 2003, the Attorney General reported that 1,228 applications were made to the FISA Court for either electronic surveillance or physical searches during calendar year of 2002. All of these applications were ultimately approved. See Report from John Ashcroft, Attorney General, to L. Ralph Mecham, Director, Administrative Office of the United States Courts (April 29, 2003); *ACLU v. U.S. Department of Justice*, 265 F.Supp.2d 20, fn.6 (D.D.C. 2003).

The USA Patriot Act allows surveillance of U.S. citizens under standards more like FISA than Title III, and allows powers allowed under Title III to be employed even where there is no probable cause and minimal judicial involvement, as in FISA. There are four basic mechanisms for surveillance on people living in the United States: (1) interception orders authorizing the interception of communications; (2) search warrants authorizing the search of physical premises and seizure of tangible things like books or other evidence; (3) "pen register" and "trap-and-trace" device orders (pen/trap orders), which authorize the collection of telephone numbers dialed to and from a particular communications device; (4) and subpoenas compelling the production of tangible things, including records. Each of the four has its own proof standards and procedures based on the Constitution, statutes, or both.

US law provides two separate "tracks" with differing proof standards and procedures for each of these mechanisms, depending upon whether surveillance is done by domestic law enforcement or foreign intelligence. All of these have been expanded by the USAPA.

(See Patriot, page 26)

Domestic Law Enforcement

1. Intercept Orders

Title III (named after the section of the Original legislation, the Omnibus Crime Control and Safe Streets Act of 1968). Surveillance is a traditional wiretap that allows the police to bug rooms, listen to telephone conversations, or get content of electronic communications in real time.

- Obtained after law enforcement makes a showing to a court that there is "probable cause" to believe that the target of the surveillance committed one of a special list of severe crimes.
- Law enforcement must report back to the court what it discovers.
- Up to 30 days; Law enforcement must go back to court for 30-day extensions

(Courts do not treat unopened e-mail at ISPs as real-time communications).

2. Pen/Trap

Pen/Trap surveillance was based upon the physical wiring of the telephone system. It allowed law enforcement to obtain the telephone numbers of all calls to or from a specific phone.

- Allowed upon a "certification" to the court that the information is relevant to an ongoing criminal investigation.
- Court must grant if proper application made
- Does not require that the target be a suspect in that investigation and law enforcement is not required to report back to the court.

Prior to USAPA there had been debate about how this authority is to be applied in the Internet context.

Foreign Intelligence Surveillance

1. FISA Intercept Orders

- Secrete Court. No public information about what surveillance requested or what surveillance actually occurs, except for a raw annual report of number of requests made and number granted (the secret court has only refused one request)
- Previous standard was certification by Attorney General that "the purpose" of an order is a suspicion that the target is a foreign power or agent of a foreign power.
- Attorney General is not required to report to the court what it does.
- Up to 90 days, or 1 year (if foreign power)

2. FISA Pen/Trap

Previous FISA pen/trap law required not only showing of relevance but also showing that the communications device had been used to contact an "agent of a foreign power."

While this exceeds the showing under the ordinary pen/trap statute, such a showing had function of protecting US persons against FISA pen/trap surveillance.

(Chart continued on page 26)

Increased Authority to Conduct Surveillance

The increased authority provided to Law Enforcement by the USAPA to conduct surveillance spans all four areas of surveillance.

A. Law enforcement intercept orders (Wiretaps)

Wiretaps (for telephone conversations) can only be issued for certain crimes listed in 18 USC § 2516. USAPA adds to this list. This restriction has never applied to interception of electronic communications.

1. Adds Terrorism.

USAPA sec. 201 adds terrorism offenses (Note: this is probably redundant since list already included most if not all terrorist acts – e.g., murder, hijacking, kidnapping, etc.)

2. Adds Computer Fraud and Abuse Act (CFAA), 18 USC § 1030.

USAPA sec. 202 adds felony violations of the CFAA (see below for discussion of changes to CFAA)

3. Removes voicemail from Title III purview.

USAPA sec. 209 allows police to get voicemail and other stored wire communications without an intercept order; now, only search warrant needed.

4. Exempts certain interceptions from requirement of judicial authorization.

Computer trespassers, see below.

B. Law enforcement search warrants.

1. Single-jurisdiction search warrants for terrorism and for electronic evidence.

In general, search warrants must be obtained within a judicial district for searches in that district. Fed.R.Crim.Pro. 41. USAPA relaxes this rule. USAPA sec. 219 adds terrorist investigations to the list of items where single-jurisdiction search warrants may be issued. Allows issuance of any district in which activities related to

terrorism may have occurred for search of property or person within or outside the district. USAPA sec. 220. Once a judge anywhere approves a warrant for seizing unopened e-mail less than 180 days old, that order can be served on any ISP/OSP or telecommunications company nationwide, without any need that the particular service provider be identified in the warrant.

2. "Sneak-and-peek" warrants greatly expanded.

USAPA sec. 213 can delay notification for "a reasonable period" and can be "extended for good cause shown" to court for any wire or electronic communication or tangible property. This is problematic because notice to a searched person is a key component of Fourth Amendment reasonableness.

C. Law enforcement Pen/Trap orders

Pen/trap orders are issued by a court under a very low standard; USAPA does not change this standard. USAPA instead expands the reach of pen/trap orders.

1. Expressly includes Internet information, e.g., e-mail and Web browsing information.

USAPA sec. 216 modifies 18 USC §3121 (c) to expressly include routing, addressing information, thus expressly including e-mail and electronic communications. "Contents" of communications excluded, but USAPA does not define what it includes (dialing, routing, addressing, signaling information) or what it excludes (contents). This raises serious questions about treatment of Web "addresses" and other URLs that identify particular content. THIS PROVISION DOES NOT SUNSET.

The Act applies to those not named (nationwide). Previously, pen/trap orders were limited by court's jurisdiction, so they had to be installed in the judicial district. Now, the court shall enter an Ex Parte Order authorizing use anywhere within the US if the court has jurisdiction over the crime being investigated and an attorney for the US Government has certified that information "likely to be obtained" is "relevant to an ongoing criminal investigation." The order applies to any provider "whose assistance may facilitate the execution of the order," whether or not within the jurisdiction of the issuing court. But if an entity is not named, the court may require that US attorney provide

(Chart continued from page 23)

3. Physical search warrants

Judicial finding of probable cause of criminality; return on warrant. Previously, agents were required at the time of the search or soon thereafter to notify the person whose premises were required for such a search, or soon thereafter to notify person whose premises were searched that the search occurred, usually by leaving copy of warrant. USAPA makes it easier to obtain surreptitious or "sneak-and-peek" warrants under which notice can be delayed.

4. Subpoenas for stored information.

Many statutes authorize subpoenas; Grand Juries may issue subpoenas as well. The main concern here has been for stored electronic information, both e-mail communications and subscriber or transactional records held by ISPs.

Subpoenas in this area are governed by the Electronic Communications Privacy Act (ECPA).

3. FISA Physical search warrants

See FISA 50 USC §1822. USAPA extends duration of physical searches. Under previous FISA, Attorney General (without court order) could authorize physical searches for up to one year of premises used exclusively by a foreign power if unlikely that US person will be searched; minimization required. A.G. could authorize such searches up to 45 days after judicial finding of probable cause that US target is or is an agent of a foreign power; minimization required, and investigation may not be based solely on First Amendment-protected activities.

4. FISA subpoenas

Previously, FISA authorized collection of business records in very limited situations, mainly records relating to common carriers, vehicles or travel, and only via court order.

USAPA permits all "tangible things," including business records, to be obtained via a subpoena (no court order).

written or electronic certification that the order applies to the person or entity being served. THIS PROVISION DOES NOT SUNSET.

If the government uses its own technology (e.g. Carnivore), then an "audit trail" is required, e.g. 30 day report back to court.

D. Law enforcement subpoenas (and some court orders) for stored information

1. USAPA sec. 210 amends Electronic Communications Privacy Act (ECPA).

Expands records that can be sought without a court order to include: records of session times and durations, temporarily assigned network addresses; means and source of payments, including any credit card or bank account number.

Allows disclosure of customer records by the service provider on the same basis that it currently allows content.

Expands "emergency" voluntary disclosure to government of both content and customer records if reason to believe immediate danger of death or serious

injury. Also expands ECPA 2703 (d) court-ordered mandatory disclosure to government. USAPA sec. 212.

2. USAPA sec. 211 Reduction of privacy for cable records.

Previously, the Cable Act had mandated strong privacy protections for customer records of cable providers; USAPA overrides these protections for customer records related to telecommunications service. This is a major change because several courts have already held that these privacy protections don't apply for telecommunications services.

E. Information sharing between law enforcement and intelligence community.

Because foreign intelligence surveillance does not require probable cause of criminality and because of the fear that foreign intelligence surveillance aimed at foreign agents would violate the rights of US persons, the law has tried to keep foreign intelligence surveillance (including evidence gained therefrom) separate from law enforcement investigations. USAPA

greatly blurs the line of separation between the two.

1. Easier to use FISA authority for Criminal Investigations.

USAPA sec. 218, foreign intelligence gathering now only needs to be "a significant purpose" not "the purpose" (edits to 50 USC §1804(a)(7)(b), and 1823 (a)(7)(B)). FISA court only looks to see that certifications are present and are not "clearly erroneous".

The courts have said it is not the function of the courts to "second guess" the certifications. The USAPA makes it easier for the government to obtain a FISA surveillance order for the purposes of mounting a criminal prosecution. *ACLU v. U.S. Department of Justice*, 265 F.Supp.2d 20, 32 (D.D.C. 2003).

2. Now can disclose formerly secret Grand Jury information to Intelligence Services.

USAPA §203(a) amends Federal Rule of Civil Procedure 6. Grand jury information now can be disclosed to intelligence

(See Patriot, page 28)

Kinko's is Your Law Firm's Branch Office.



for all your
litigation support,

trial exhibits,
custom **charts**,
graphs, timelines,

discovery
document copying
and labeling needs,

choose **kinko's**
as your legal partner.

- ▼ Discovery document copying
- ▼ Legal documents and manuals
- ▼ Custom binding and finishing
- ▼ Exhibits with full-color copies
- ▼ Enlargements up to 24" x 36"
- ▼ Confidential handling of all materials
- ▼ Experienced graphic designer on site
- ▼ Free pick up and delivery

KINKO'S LEGAL CENTER
Open 24 hours a day, 7 days a week.
1121 South Spring Street ▼ 372-0775

kinko's
Your branch office

services when "matters involve foreign intelligence or counterintelligence" per 50 USC §401(a) or foreign intelligence information.

3. Foreign Intelligence Information.

A new category of information can be disclosed to foreign intelligence agents.

Any information, whether or not concerning a US person, that "relates" to the ability of the US to protect against actual or potential attack, sabotage or international terrorism or clandestine intelligence activities; any information, whether or not concerning a US Person, that "relates" to the national defense or security or conduct of foreign affairs. **THIS PROVISION DOES NOT SUNSET.**

4. Disclose criminal wiretap information with any Government Official, including Foreign Intelligence Services.

Section 203(b) amends 18 USC §2517. Allows disclosure of contents of wiretaps or evidence derived therefrom to any other government official, including intelligence, national defense and national security, "to the extent such contents include foreign intelligence or counterintelligence or foreign intelligence information."

5. General authority to disclose

Section 203(d). Notwithstanding other law, lawful for foreign intelligence or counterintelligence or foreign intelligence information may be disclosed to anyone to assist in performance of official duties.

USAPA sec. 504, also authorizes general coordination between law enforcement and FISA surveillance.

USAPA sec. 224 provides that several surveillance provisions of the USAPA will expire on December 31, 2005.

A. The provisions that expire include:

- Sec. 201. Authority to intercept wire, oral, and electronic communications relating to terrorism.
- Sec. 202. Authority to intercept wire, oral and electronic communications relating to computer fraud and abuse offenses.
- Sec. 203(b), (d). Authority to share criminal investigative information.
- Sec. 206. Roving surveillance authority under the foreign intelligence surveillance act of 1978.
- Sec. 207. Duration of FISA surveillance of non-United States Person who are agents of a foreign power.
- Sec. 209. Seizure of voice-mail messages pursuant to warrants.
- Sec. 212. Emergency disclosure of electronic communications to protect life and limb.
- Sec. 214. Pen register and trap and trace authority under FISA.
- Sec. 215. Access to records and other items under the Foreign Intelligence Surveillance Act.
- Sec. 217. Interception of computer trespasser communications.
- Sec. 218. Foreign intelligence Information.
- Sec. 220. Nationwide service of search warrants for electronic evidence.

- Sec. 223. Civil liability for certain unauthorized disclosures.
- B. The following provisions do not expire:
 - Sec. 203(a),(c): Grand jury sharing of information.
 - Sec. 208: Designation of Judges: increases the number of FISA judges.
 - Sec. 210: ECPA scope of subpoenas for records of electronic communications – clearly allowing e-mails routing information.
 - Sec. 211: ECPA clarification of scope: privacy provisions of Cable Act overridden for communication services offered by cable providers (but not for records relating to cable viewing)
 - Sec. 213: Sneak & Peek: delay notification of execution of a warrant.
 - Sec. 216: Modification of pen/trap authorities: (in original PARTIOT, would have sunsetted).
 - Sec. 219: Single jurisdiction search warrants for terrorism.
 - Sec. 222: Assistance to law enforcement.
 - Sec. 225: Immunity for compliance with FISA wiretap. Can continue all investigations active at the time of expiration.

Conclusion

Our civil liberties have been eroded by the involuntary nature of our "sacrifices." When a person irrationally fears crowded elevators and takes the stairs instead, only that person suffers the inconvenience of their personal response. But when everyone, fearful or not, is forced to suffer because of the fears of others, then such measures become tyrannical: we should expect rational deliberation and justifications by our leaders before accepting them. But in the aftermath of 9/11, tens of billions of dollars were immediately reallocated with little public debate. Clark R. Chapman & Alan W. Harris, "A Skeptical Look at September 11th," **Skeptical Inquirer**, September 10, 2002.

Many provisions of the Patriot Act have little to do with the attacks of September 11, 2001, such as the extensive portions of the act that deal with computer based communications (there has been no connection between e-mail or the internet). But due to our fears we acquiesce to the loss of our liberties.

An Important Message for Plaintiff Attorneys ...

It was inevitable that attorneys would be sued by their own clients for not being apprised of the benefits of a structured settlement and given the opportunity to take their payments tax-free over time, rather than as a lump sum.

Plaintiff's Attorneys Learned the Hard Way

It happened in Texas when the mother of a child injured at birth and mentally incapacitated for life sued the attorneys who had represented her daughter in a medical negligence lawsuit that settled 10 years ago because the \$2.5 million in damages was taken in cash rather than in periodic payments. She also sued the guardian ad litem, whose sole duty was to look out for the welfare of the child during that litigation. The amount recovered from the attorneys for legal malpractice was more than the damages received in 1991 in the underlying medical malpractice case.

Please call Joe McCormack or Denny Koehn today.

CORNERSTONE SETTLEMENT SERVICES, INC.

Your Structured Settlement Service Company

901-766-3249 • 800-786-1109 • (Fax) 901-766-6313
3455 Winbrook Drive • Memphis, Tennessee 38116

