

## The USA Patriot Act Law Enforcement Perspective

Richard Ma, Ron Richardson, Ray Skoog

### Introduction

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (The USA Patriot Act) was signed into law on October 26, 2001 by President George Bush. The motivation for the rapid (some would say *too* rapid) acceptance of the Patriot Act was that the escalating acts of terrorism around the world finally found their way inside the borders of the United States of America, in the form of 9/11. The provisions of the Patriot Act amend over 15 federal statutes concerning laws pertaining to computer fraud and abuse, wiretapping, immigration, and foreign intelligence as well as laws pertaining to the privacy of Americans at large. The goal of the Patriot Act, or at least what got it passed, is to strengthen America's defense against a highly motivated, seemingly inhuman enemy, which is apparently willing to resort to any means necessary to attack the nation. However the Patriot Act does not limit itself to the pursuit of terrorists, and in fact most of its provisions can be applied to more mundane criminals. In the hands of law enforcement officers (LEOs), the powers provided by the Act will probably end up nailing the ordinary criminals most often. This broadness will make the Act truly useful to LEOs all over America.

Although receiving much criticism for the potential encroachment into the privacy and confidentiality of the American way of life, the Patriot Act provides LEOs with a new toolbox to combat the bad guys, and most Americans seem to be OK with the new balance. The Act updates many existing laws to cope with the rapid and expansive growth of electronic communications and the advent of the Internet. Paramount to concerns about the Patriot Act is the lessening of judicial review for various procedures, however, streamlining law enforcement efforts is mandatory to meet unprecedented illegal encroachments on American society specifically and the world in general during the "age of information." The Patriot Act attempts to furnish LEOs with tools sufficient to the task of combating a deadly and cunning modern enemy.

Many details of The USA Patriot Act are available in the papers preceding and following this one. This paper discusses the Patriot Act from the perspective of law enforcement. We skip over large areas of the Patriot Act, and further, we assume that the provisions of the Act will be held constitutional (they are little use to LEOs if struck down in court).

To familiarize the reader, a general overview of major provisions follows:

- \* Greater authority for federal officials to track and intercept communications, for both law enforcement and foreign intelligence gathering purposes. The act expands powers relating to wiretaps, search warrants, pen/trap orders and subpoenas.
- \* New powers for the Secretary of Treasury to combat the use of U.S. financial institutions for money laundering.
- \* Attempts to close borders to terrorists, and attempts to detain and remove those that are within U.S. borders.
- \* New crimes have been defined and new penalties have been created. These new crimes tend not to cover new ground so much as they tend to fill in gaps and make penalties more severe.

- \* New procedural efficiencies are allowed for use against terrorists. The changes include increased rewards for tip-offs, new search warrants (“sneak and peak”), and the lengthening of the statute of limitations for terrorist crimes.

## Wiretap

A wiretap is originally defined as an act or instance of attaching a mechanical or electronic device to a telephone or telegraph line to get information. The Patriot Act modernizes FISA (Foreign Intelligence Surveillance Act) to apply to the diverse nature of electronic communications and expedite the collection of intelligence. Law enforcement is additionally granted access to information pertaining to computer use and Internet activities such as email and Web surfing. All forms of electronic communication are considered for intelligence under the activity of wiretapping.

The codification of FISA authority supersedes current criminal law requiring LEOs to ascertain that the device to be tapped is actually being used by the target of a wiretap. The requirement for separate court orders for each communication carrier is eliminated. The expansion of Multi-Point (roving wiretap) Authority allows a single wiretap to legally “roam” from device to device. Intelligence efforts are expedited by tapping the person rather than itemized communication media.

## Pen Register and Trap and Trace

Laws were originally written for Pen Register and Trap and Trace (PR/TT) devices to monitor outgoing and incoming phone numbers. The Patriot Act authorizes the installation of recording devices to collect the data transferred in computer dialing, routing, addressing, and signaling information. Although the content of the data transmission is still subject to 4<sup>th</sup> Amendment protections, other associated information eases the identification and location of target users.

Jurisdictional Expansion is added to the use of PR/TT. Authorization applies to anywhere in the United States if granted to the government. State-granted court orders are limited to the jurisdiction of the state court granting the order. The statutory requirement that the surveillance target is a foreign agent is eliminated for the issuance of a PR/TT monitoring order. The codification of the Patriot Act in relation to wiretaps and PR/TT broadens the application communications monitoring practices. Petition for court orders need only affirm that an investigation is taking place, reducing the burden of providing *probable cause* to initiate surveillance. Delayed notice to the target of a information collection procedure is authorized if it can be demonstrated that the notice would produce an *adverse result* to the collection of information. Delays are stipulated as being a *reasonable* amount of time and can be extended up to one year. Monitoring activities can proceed and be extended even if current efforts have not produced evidence of illegal activity.

## Search Warrants – Single Jurisdiction

The Fourth Amendment to the Constitution requires that before the government conducts an invasive search to find evidence of crime, it must prove to a judicial officer that it has probable cause of crime. This requirement helps ensure that search warrants are applied only to those likely to be involved in criminal activity, and not to others. [2]

Section 218 turns this concept upside down. It permits the FBI to conduct a secret search for the purpose of investigating crime even though the FBI does not have probable cause of crime. The section authorizes unconstitutional activity – searches in non-emergency circumstances- for criminal activity with no showing of probable cause of crime. [2]

### Search Warrants – Sneak and Peak

Previously, agents were required at the time of the search or soon thereafter to notify person whose premises were searched that search occurred, usually by leaving copy of warrant which is a key component of Fourth Amendment.

USAPA makes it easier to obtain surreptitious or “sneak-and-peek” warrants under which notice can be delayed. [1]

### Subpoenas – Amendment to ECPA

The Electronic Communications Privacy Act (ECPA) 1986 sets out the provisions for access, use, disclosure, interception and privacy protections of electronic communications which 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. The law was enacted in 1986 and covers various forms of wire and electronic communications. The law prevents government entities from requiring disclosure of electronic communications from a provider without proper procedure. [3]

USAPA 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. USAPA allows disclosure of customer records by the service provider on the same basis that it currently allows content. [1]

### Subpoenas – Reduction of Privacy for Cable Records

Previously, the Cable Act 1992 had mandated strong privacy protection for customer records of cable providers.

USAPA overrides these protections for customer records related to telecommunications services. This is a major change because several courts have already held that these privacy protections don't apply for telecommunications services. [1]

### Money

Money laundering is a process whereby the origin of funds generated by illegal means is concealed, sort of washing of dirty money, so that the money can be put into circulation without LEOs noticing. The Patriot Act expands the anti-money laundering provisions in the Bank Secrecy Act, which was designed to make it easier to detect and prosecute money laundering and the financing of terrorism through it. While it is quite possible that terrorist operatives could get into the country and pay their way to do their deeds rather than relying on laundered money, this is more difficult, it limits the possible scope of the operation, it requires a more talented goon (one that can get and hold a job), and requires that the attention of the operatives be diverted somewhat from the objective. Tracking money is not a foolproof way to find terrorists, but it does raise the bar somewhat, and in any case, it doesn't do any harm to the LEO cause. Further, the Patriot Act is not limited to assisting the pursuit of terrorists; in fact most parts of it are not targeted at any single group, and this includes the new money laundering rules. LEOs will certainly appreciate their enhanced ability to detect the flow of dirty money, possibly connected to things such as drugs and political payoffs.

With the general benefit of careful watch of money established, let's look at what the Act does. The Act requires certain things of “financial institutions”, including the following:

- a) Increased reporting for transactions involving more than \$10k in cash, coins (etc).
- b) Maintenance of records that identify the owners of all accounts. Regulations may be put in place requiring foreign nationals to obtain an ID number before opening accounts at financial institutions.
- c) Prompt and secret reporting of any suspicious transactions.
- d) Development of internal policies, procedures and controls appropriate to the level of risk of money laundering.
- e) Designation of a “compliance officer” with appropriate training and access to senior management, whose task it is to oversee compliance with the Patriot Act.
- f) Perform ongoing employee training appropriate to role of employees in company to address knowledge gaps opened by employee turnover and movement within the organization.

Financial institutions in the above use are defined as foreign, merchant, commercial and private banks, credit unions, thrift institutions, securities brokers and dealers, and investment companies. More surprisingly, the definition also includes investment bankers; futures commission merchants, commodity trading advisors, and commodity pool operators; currency exchanges; issuers, redeemers, or cashiers of traveler’s checks, checks, money orders, or similar instruments; operators of credit card systems; insurance companies; dealers in precious metals, stones or jewels; pawnbrokers; loan of finance companies; travel agencies; licenced senders of money or anyone else who engages as a business in the transmission of funds, including in informal money transfer systems outside of the conventional financial institutions system; telegraph companies; businesses engaged in vehicle sales, including automobile, airplane and boat sales; persons involved in real estate closings and settlements; casinos or gaming establishments; and pretty much anything else that the Secretary of the Treasury decides is like any of the above, or is transferring money in such a way that it is deemed interesting for criminal, tax, or regulatory matters.

What this decidedly meaty list doesn’t cover explicitly it covers with the weasel words at the end, and essentially it will operate as a huge data gathering engine for all sorts of criminal activity, terrorist-related or not. Plainly this is good for the LEO cause because it will have the potential to raise lots of flags and probably generate trustworthy evidence for prosecution, since the organizations involved are presumably honest and the records are presumably rather accurate. The government is obviously serious about getting useful data out of this since they require people be appointed to oversee it and since they require ongoing employee training.

### Immigrants

Although aliens are overall a small percent of the American public, all 19 of the 9/11 hijackers were aliens that entered the country legally. Based on this it seems like it would be an excellent idea to pay a large amount of attention to aliens, including those trying to enter legally, and the Patriot Act does just this. The Act:

- a) Allows imprisonment of immigrants without charge, potentially for an indefinite time.
- b) Establishes a program to monitor certain foreign students (various types of schools).
- c) Provides certain information to the INS from the criminal history records of visa applicants and applicants for admission.
- d) Calls for enhanced passports that are harder to duplicate, also calls for an integrated entry and exit data system.
- e) Prevents consulate shopping.
- f) Triples the number of customs and INS personnel at the northern border.

Point (a) above is going to be quite handy for LEOs because now if the Attorney General “certifies” an alien, that alien can be held without charge for seven days, presumably while LEOs work to find something to keep him or her in jail longer. Prior to the Patriot Act it was not legal to

hold aliens without charge, so this is a significant change and has caused considerable outcry from civil rights defenders. At the end of the 7 day stay, if the immigrant is eligible for deportation but cannot be deported in the foreseeable future (for example if their home country refuses to except them), they can be held indefinitely in 6-month allotments. All that is needed is that the Attorney General (or the Deputy Attorney General) finds that there are reasonable grounds to believe that the individual threatens national security, or the safety of the community or any person. Since this requirement is so easy to meet and since it doesn't require any actual proof, LEOs have a very strong hand in keeping certain people off of the street.

Point (b) above could obviously generate leads or otherwise intimidate terrorists that intend to follow in the footsteps of the 9/11 crew, however it is of little use against most criminals. The other provisions of the Act are less dramatic and will serve mostly to make it more difficult for questionable immigrants to get into the country. This might have a positive effect on the crime rate.

### Conclusion

In conclusion, today we've outlined some of the new powers given to LEOs by the Patriot Act, and generally they are powers that allow or require more data collection. It is important to note that data is not evidence, and unless the LEOs of this country can convert data to evidence, or at least to a lead to work from, then the Patriot Act will be a failure.

### References, Sources

- 1) EFF Analysis of The Provisions of The USA PATRIOT Act. Web page. <[http://www.eff.org/Privacy/Surveillance/Terrorism\\_militias](http://www.eff.org/Privacy/Surveillance/Terrorism_militias)>, October 2001.
- 2) How the USA-Patriot Act Enables Law Enforcement to Use Intelligence Authorities to Circumvent The Privacy Protections Afforded in Criminal Cases. Web page. <<http://www.aclu.org/Redirect.cfm?pg=%2Fcongress%2F1102301i%2Ehtml>>
- 3) Electronic Communications Privacy Act. Web page. <<http://legal.web.aol.com/resources/legislation/ecpa.html>>
- 4) Hunton & Williams. Client Alert: Prepare Now for New Regulatory Requirements Under the USA Patriot Act of 2001. PDF format. <[www.hunton.com](http://www.hunton.com)>, June 2002.
- 5) Doyle, Charles. CRC Report for Congress: The USA Patriot Act: A Sketch. PDF format. The Library of Congress, April 2002.
- 6) Patriot Act Summary. Web page. <<http://members.tripod.com/~warrior69/id144.htm>>
- 7) Kenny, John J, Joseph M. McLaughlin and Valerie Caproni. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism ("USA PATRIOT Act") Act of 2001. Web page. <<http://www.stblaw.com/FSL5CS/memos/memos1025.asp>>, November 2001
- 8) American Library Association: office for Intellectual Freedom. The USA Patriot Act in the Library. April 2002. Accessed 22 Mar 2003. <<http://www.ala.org.alaorg/oif/usapatriotlibrary.html>>.
- 9) CNN: LAW. Explaining the U.S.A Patriot Act. 8 August 2002. CNN.com. Accessed 22 March 2003. <<http://cnn.com/2002/LAW/o8/23/patriot.act.explainer>>.

- 10) Doyle, Charles. *The USA Patriot Act: A legal Analysis*. The Library of Congress: Congressional Research Service. 15 April 2002. Accessed 25 March 2003. <[www.aallnet.org/chapter/call/publications/usapatriotact.htm](http://www.aallnet.org/chapter/call/publications/usapatriotact.htm)>.
- 11) Electronic Privacy Information Center. *The USA Patriot Act*. Last update: 19 March 2003. Accessed 22 March 2003. <<http://www.epic.org/privacy/terrorism/usapatriot/>>.
- 12) Podesta, John. *USA Patriot Act: The Good, the Bad, and the Sunset*. ABA Network. Winter, 2002. Accessed 25 March 2003. <<http://www.abanet.org/irr/hr/winter02/podesta.html>>.
- 13) Stanford Education. *The USA Patriot Act: A critical Tool for Law Enforcement*. Accessed 25 March 2003. <[http://www.Stanford.edu/~jimkr/digital\\_dilemmas/patriot\\_act/for.html](http://www.Stanford.edu/~jimkr/digital_dilemmas/patriot_act/for.html)>.