Congressional Research Service
Informing the legislative debate since 1914

# The USA PATRIOT Act: A Sketch

April 18, 2002

**Congressional Research Service**
https://crsreports.congress.gov
RS21203

**CRS REPORT**
Prepared for Members and
Committees of Congress

# The USA PATRIOT Act: A Sketch

Charles Doyle
Senior Specialist
American Law Division

## Summary

Congress passed the USA PATRIOT Act (the Act) in response to the terrorists' attacks of September 11, 2001. The Act gives federal officials greater authority to track and intercept communications, both for law enforcement and foreign intelligence gathering purposes. It vests the Secretary of the Treasury with regulatory powers to combat corruption of U.S. financial institutions for foreign money laundering purposes. It seeks to further close our borders to foreign terrorists and to detain and remove those within our borders. It creates new crimes, new penalties, and new procedural efficiencies for use against domestic and international terrorists. Although it is not without safeguards, critics contend some of its provisions go too far. Although it grants many of the enhancements sought by the Department of Justice, others are concerned that it does not go far enough.

The Act originated as H.R.2975 (the PATRIOT Act) in the House and S.1510 in the Senate (the USA Act). S.1510 passed the Senate on October 11, 2001, 147 *Cong. Rec.* S10604 (daily ed.). The House Judiciary Committee reported out an amended version of H.R. 2975 on the same day, H.R.Rep.No. 107-236. The House passed H.R. 2975 the following day after substituting the text of H.R. 3108, 147 *Cong.Rec.* H6775-776 (daily ed. Oct. 12, 2001). The House version incorporated most of the money laundering provisions found in an earlier House bill, H.R. 3004, many of which had counterparts in S.1510 as approved by the Senate. The House subsequently passed a clean bill, H.R. 3162 ( under suspension of the rules), which resolved the differences between H.R. 2975 and S.1510, 147 *Cong.Rec.* H7224 (daily ed. Oct. 24, 2001). The Senate agreed to the changes, 147 *Cong.Rec.* S10969 (daily ed. Oct. 24, 2001), and H.R. 3162 was sent to the President who signed it on October 26, 2001.

This is an abbreviated versions of *The USA PATRIOT Act: A Legal Analysis*, CRS Report RL31377, stripped of its citations and footnotes.

## Criminal Investigations: Tracking and Gathering Communications

Federal communications privacy law features a three tiered system, erected for the dual purpose of protecting the confidentiality of private telephone, face-to-face, and computer communications while enabling authorities to identify and intercept criminal communications. Title III of the Omnibus Crime Control and Safe Streets Act of 1968 supplies the first level. It prohibits electronic eavesdropping on telephone conversations, face-to-face conversations, or computer and other forms of electronic communications in most instances. It does, however, give authorities a narrowly defined process for electronic surveillance to be used as a last resort in serious criminal cases. When approved by senior Justice Department officials, law enforcement officers may seek a court order authorizing them to secretly capture conversations concerning any of a statutory list of offenses (predicate offenses). Title III court orders come replete with instructions describing the permissible duration and scope of the surveillance as well as the conversations which may be seized and the efforts to be taken to minimize the seizure of innocent conversations. The court notifies the parties to any conversations seized under the order after the order expires.

Below Title III, the next tier of privacy protection covers telephone records, e-mail held in third party storage, and the like, 18 U.S.C. 2701-2709 (Chapter 121). Here, the law permits law enforcement access, ordinarily pursuant to a warrant or court order or under a subpoena in some cases, but in connection with *any* criminal investigation and without the extraordinary levels of approval or constraint that mark a Title III interception.

Least demanding and perhaps least intrusive of all is the procedure that governs court orders approving the government's use of trap and trace devices and pen registers, a kind of secret "caller id.", which identify the source and destination of calls made to and from a particular telephone, 18 U.S.C. 3121-3127 (Chapter 206). The orders are available based on the government's certification, rather than a finding of a court, that use of the device is likely to produce information relevant to the investigation of a crime, any crime. The devices record no more than identity of the participants in a telephone conversation, but neither the orders nor the results they produce need ever be revealed to the participants.

The Act modifies the procedures at each of the three levels. It:

- permits pen register and trap and trace orders for electronic communications (*e.g.*, e-mail);
- authorizes nationwide execution of court orders for pen registers, trap and trace devices, and access to stored e-mail or communication records;
- treats stored voice mail like stored e-mail (rather than like telephone conversations);
- permits authorities to intercept communications to and from a trespasser within a computer system (with the permission of the system's owner);
- adds terrorist and computer crimes to Title III's predicate offense list;
- reenforces protection for those who help execute Title III, ch. 121, and ch. 206 orders;

- encourages cooperation between law enforcement and foreign intelligence investigators;
- establishes a claim against the U.S. for certain communications privacy violations by government personnel; and
- terminates the authority found in many of these provisions and several of the foreign intelligence amendments with a sunset provision (Dec. 31, 2005).

## Foreign Intelligence Investigations

The Act eases some of the restrictions on foreign intelligence gathering within the United States, and affords the U.S. intelligence community greater access to information unearthed during a criminal investigation, but it also establishes and expands safeguards against official abuse. More specifically, it:

- permits "roving" surveillance (court orders omitting the identification of the particular instrument, facilities, or place where the surveillance is to occur when the court finds the target is likely to thwart identification with particularity);
- increases the number of judges on the Foreign Intelligence Surveillance Act (FISA) court from 7 to 11;
- allows application for a FISA surveillance or search order when gathering foreign intelligence is *a significant* reason for the application rather than *the* reason;
- authorizes pen register and trap & trace device orders for e-mail as well as telephone conversations;
- sanctions court ordered access to any tangible item rather than only business records held by lodging, car rental, and locker rental businesses;
- carries a sunset provision;
- establishes a claim against the U.S. for certain communications privacy violations by government personnel; and
- expands the prohibition against FISA orders based solely on an American's exercise of his or her First Amendment rights.

## Money Laundering

In federal law, money laundering is the flow of cash or other valuables derived from, or intended to facilitate, the commission of a criminal offense. It is the movement of the fruits and instruments of crime. Federal authorities attack money laundering through regulations, criminal sanctions, and forfeiture. The Act bolsters federal efforts in each area.

**Regulation**: The Act expands the authority of the Secretary of the Treasury to regulate the activities of U.S. financial institutions, particularly their relations with foreign individuals and entities. He is to promulgate regulations:

- under which securities brokers and dealers as well as commodity merchants, advisors and pool operators must file suspicious activity reports (SARs);

- requiring businesses, which were only to report cash transactions involving more than $10,000 to the IRS, to file SARs as well;
- imposing additional "special measures" and "due diligence" requirements to combat foreign money laundering;
- prohibiting U.S. financial institutions from maintaining correspondent accounts for foreign shell banks;
- preventing financial institutions from allowing their customers to conceal their financial activities by taking advantage of the institutions' concentration account practices;
- establishing minimum new customer identification standards and record-keeping and recommending an effective means to verify the identity of foreign customers;
- encouraging financial institutions and law enforcement agencies to share information concerning suspected money laundering and terrorist activities; and
- requiring financial institutions to maintain anti-money laundering programs which must include at least a compliance officer; an employee training program; the development of internal policies, procedures and controls; and an independent audit feature.

**Crimes**: The Act contains a number of new money laundering crimes, as well as amendments and increased penalties for earlier crimes. It:

- outlaws laundering (in the U.S.) any of the proceeds from foreign crimes of violence or political corruption;
- prohibits laundering the proceeds from cybercrime or supporting a terrorist organization;
- increases the penalties for counterfeiting;
- seeks to overcome a Supreme Court decision finding that the confiscation of over $300,000 (for attempt to leave the country without reporting it to customs) constituted an unconstitutionally excessive fine;
- provides explicit authority to prosecute overseas fraud involving American credit cards; and
- endeavors to permit prosecution of money laundering in the place where the predicate offense occurs.

**Forfeiture**: The Act creates two types of forfeitures and modifies several confiscation-related procedures. It allows confiscation of all of the property of any individual or entity that participates in or plans an act of domestic or international terrorism; it also permits confiscation of any property derived from or used to facilitate domestic or international terrorism. The Constitution's due process, double jeopardy, and ex post facto clauses may limit the anticipated breath of these provisions. Procedurally, the Act:

- establishes a mechanism to acquire long arm jurisdiction, for purposes of forfeiture proceedings, over individuals and entities;
- allows confiscation of property located in this country for a wider range of crimes committed in violation of foreign law;
- permits U.S. enforcement of foreign forfeiture orders;

- calls for the seizure of correspondent accounts held in U.S. financial institutions for foreign banks who are in turn holding forfeitable assets overseas; and
- denies corporate entities the right to contest a confiscation if their principal shareholder is a fugitive.

## Alien Terrorists and Victims

The Act contains a number of provisions designed to prevent alien terrorists from entering the United States, particularly from Canada; to enable authorities to detain and deport alien terrorists and those who support them; and to provide humanitarian immigration relief for foreign victims of the attacks on September 11.

## Other Crimes, Penalties, & Procedures

**New crimes**: The Act creates new federal crimes for terrorist attacks on mass transportation facilities, for biological weapons offenses, for harboring terrorists, for affording terrorists material support, for misconduct associated with money laundering already mentioned, for conducting the affairs of an enterprise which affects interstate or foreign commerce through the patterned commission of terrorist offenses, and for fraudulent charitable solicitation. Although strictly speaking these are new federal crimes, they generally supplement existing law by filling gaps and increasing penalties.

**New Penalties**: The Act increases the penalties for acts of terrorism and for crimes which terrorists might commit. More specifically it establishes an alternative maximum penalty for acts of terrorism, raises the penalties for conspiracy to commit certain terrorist offenses, envisions sentencing some terrorists to life-long parole, and increases the penalties for counterfeiting, cybercrime, and charity fraud.

**Other Procedural Adjustments**: In other procedural adjustments designed to facilitate criminal investigations, the Act:

- increases the rewards for information in terrorism cases;
- expands the Posse Comitatus Act exceptions;
- authorizes "sneak and peek" search warrants;
- permits nationwide and perhaps worldwide execution of warrants in terrorism cases;
- eases government access to confidential information;
- allows the Attorney General to collect DNA samples from prisoners convicted of any federal crime of violence or terrorism;
- lengthens the statute of limitations applicable to crimes of terrorism;
- clarifies the application of federal criminal law on American installations and in residences of U.S. government personnel overseas; and
- adjust federal victims' compensation and assistance programs.

A section, found in the Senate bill but ultimately dropped, would have changed the provision of federal law which requires Justice Department prosecutors to adhere to the ethical standards of the legal profession where they conduct their activities (the McDade-Murtha Amendment), 28 U.S.C. 530B.

## Author Information

Charles Doyle
Senior Specialist in American Public Law

## Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.