



WIKIPEDIA  
The Free Encyclopedia

- [Main page](#)
- [Contents](#)
- [Featured content](#)
- [Current events](#)
- [Random article](#)
- [Donate to Wikipedia](#)
- [Wikipedia store](#)

Interaction

- [Help](#)
- [About Wikipedia](#)
- [Community portal](#)
- [Recent changes](#)
- [Contact page](#)

Tools

- [What links here](#)
- [Related changes](#)
- [Upload file](#)
- [Special pages](#)

Article [Talk](#)

Read [Edit](#) [View history](#)

# Patriot Act



From Wikipedia, the free encyclopedia

The **USA PATRIOT Act** is an [Act of Congress](#) that was signed into law by [President George W. Bush](#) on October 26, 2001.<sup>[1]</sup> With its ten-letter abbreviation (USA PATRIOT) expanded, the full title is "**Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001**".<sup>[2]</sup>

On May 26, 2011, President [Barack Obama](#) signed the PATRIOT Sunsets Extension Act of 2011, a four-year extension of three key provisions in the Act:<sup>[3]</sup> [oving wiretaps](#), [searches of business records](#), and conducting surveillance of "lone wolves"—individuals suspected of terrorist-related activities not

## Patriot Act



<b>Other short titles</b>	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001
<b>Long title</b>	An Act to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes.
<b>Acronyms (colloquial)</b>	USA PATRIOT Act
<b>Nicknames</b>	Patriot Act
<b>Enacted by</b>	the <a href="#">107th United States Congress</a>

Permanent link  
Page information  
Wikidata item  
Cite this page

Print/export

Create a book  
Download as PDF  
Printable version

In other projects

Wikimedia Commons

Languages

العربية  
Български  
Čeština  
Dansk  
Deutsch  
Eesti  
Español  
Esperanto  
فارسی  
Français  
Galego  
한국어  
Bahasa Indonesia  
Íslenska  
Italiano  
עברית

linked to terrorist groups.<sup>[4]</sup>


Following a lack of Congressional approval, parts of the Patriot Act expired on June 1, 2015.<sup>[5]</sup> With the passage of the [USA Freedom Act](#) on June 2, 2015, the expired parts were restored and renewed through 2019.<sup>[6]</sup> However, Section 215 of the law was amended to stop the [National Security Agency](#) (NSA) from continuing its mass phone data collection program.<sup>[6]</sup> Instead, phone companies will retain the data and the NSA can obtain information about targeted individuals with permission from a federal court.<sup>[6]</sup>

From broad concern felt among Americans from both the [September 11 attacks](#) and the [2001 anthrax attacks](#), Congress rushed to pass legislation to strengthen security controls. On October 23, 2001, Republican Rep. [Jim Sensenbrenner](#) introduced H.R. 3162 incorporating provisions from a previously sponsored House bill and a Senate bill also introduced earlier in the month.<sup>[7]</sup>

**Effective** October 26, 2001

### Citations

**Public law** [107-56](#) 

**Statutes at Large** [115 Stat. 272](#)  (2001)

### Codification

**Acts amended** [Electronic Communications Privacy Act](#)  
[Computer Fraud and Abuse Act](#)  
[Foreign Intelligence Surveillance Act](#)  
[Family Educational Rights and Privacy Act](#)  
[Money Laundering Control Act](#)  
[Bank Secrecy Act](#)  
[Right to Financial Privacy Act](#)  
[Fair Credit Reporting Act](#)  
[Immigration and Nationality Act of 1952](#)  
[Victims of Crime Act of 1984](#)  
[Telemarketing and Consumer Fraud and Abuse Prevention Act](#)

**Titles amended** [8](#), [12](#), [15](#), [18](#), [20](#), [31](#), [42](#), [47](#), [49](#), [50](#)

**U.S.C. sections created** [18 USC §2712](#), [31 USC §5318A](#), [15 USC §1681v](#), [8 USC §1226A](#), [18 USC §1993](#), [18 USC §2339](#), [18 USC §175b](#), [50 USC §403-5b](#), [51 USC §5103a](#)

**U.S.C. sections amended** [8 USC §1105](#), [8 USC §1182g](#), [8 USC §1189](#), [8 USC §1202](#), [12 USC §1828](#), [12 USC §3414](#), [15 USC §1681a](#), [15 USC §6102](#), [15 USC §6106](#), [18 USC §7](#), [18 USC §81](#), [18 USC §175](#), [18 USC §470](#), [18 USC §471](#), [18 USC §472](#), [18 USC §473](#), [18 USC §474](#), [18 USC §476](#), [18 USC §477](#), [18 USC §478](#), [18 USC §479](#), [18 USC §480](#),

- Magyar
- Bahasa Melayu
- Nederlands
- 日本語
- Norsk bokmål
- Polski
- Português
- Русский
- Simple English
- Српски / srpski
- Suomi
- Svenska
- ӀӀӀ
- Українська
- اردو
- 中文

 Edit links

The next day, the Act passed the [House](#) 357 to 66,<sup>[8]</sup> with Democrats comprising the overwhelming portion of dissent. The three Republicans voting 'no' were [Robert Ney](#) of [Ohio](#), [Butch Otter](#) of [Idaho](#) and [Ron Paul](#) of [Texas](#). On October 25, the Act passed the [Senate](#) by 98 to 1, the only dissident being Russ Feingold of Wisconsin.<sup>[9]</sup>

Opponents of the law have criticized its authorization of [indefinite detentions](#) of immigrants; the permission given law enforcement officers to search a home or business without the owner's or the occupant's consent or knowledge; the expanded use of [National Security Letters](#), which allows the [Federal Bureau of Investigation](#) (FBI) to search telephone, e-mail, and financial records without a court order; and the expanded access of law enforcement agencies to business records, including library and financial records. Since its passage, several legal challenges have been brought against the act, and federal courts have ruled that

18 USC §481, 18 USC §484, 18 USC §493, 18 USC §917, 18 USC §930, 18 USC §981, 18 USC §1029, 18 USC §1030, 18 USC §1362, 18 USC §1363, 18 USC §1366, 18 USC §1956, 18 USC §1960, 18 USC §1961, 18 USC §1992, 18 USC §2155, 18 USC §2325, 18 USC §2331, 18 USC §2332e, 18 USC §2339A, 18 USC §2339B, 18 USC §2340A, 18 USC §2510, 18 USC §2511, 18 USC §2516, 18 USC §2517, 18 USC §2520, 18 USC §2702, 18 USC §2703, 18 USC §2707, 18 USC §2709, 18 USC §2711, 18 USC §3056, 18 USC §3077, 18 USC §3103, 18 USC §3121, 18 USC §3123, 18 USC §3124, 18 USC §3127, 18 USC §3286, 18 USC §3583, 20 USC §1232g, 20 USC §9007, 31 USC §310 (redesignated), 31 USC §5311, 31 USC §5312, 31 USC §5317, 31 USC §5318, 31 USC §5319, 31 USC §5321, 31 USC §5322, 31 USC §5324, 31 USC §5330, 31 USC §5331, 31 USC §5332, 31 USC §5341, 42 USC §2284, 42 USC §2284, 42 USC §3796, 42 USC §3796h, 42 USC §10601, 42 USC §10602, 42 USC §10603, 42 USC §10603b, 42 USC §14601, 42 USC §14135A, 47 USC §551, 49 USC §31305, 49 USC §46504, 49 USC §46505, 49 USC §60123. 50 USC §403-3c.

a number of provisions are unconstitutional.

Many provisions of the act were to [sunset](#) beginning December 31, 2005, approximately four years after its passage. In the months preceding the sunset date, supporters of the act pushed to make its sun-setting provisions permanent, while critics sought to revise various sections to enhance civil liberty protections. In July 2005, the U.S. Senate passed a reauthorization bill with substantial changes to several sections of the act, while the House reauthorization bill kept most of the act's original language. The two bills were then reconciled in a conference committee that was criticized by Senators from both the Republican and Democratic parties for ignoring civil liberty concerns.<sup>[10]</sup>

The bill, which removed most of the changes from the Senate version, passed Congress on March 2, 2006, and was signed into law by President George W. Bush on March 9 and 10, 2006.

50 USC §401a, 50 USC §1702,  
50 USC §1801, 50 USC §1803,  
50 USC §1804, 50 USC §1805,  
50 USC §1806, 50 USC §1823,  
50 USC §1824, 50 USC §1842,  
50 USC §1861, 50 USC §1862,  
50 USC §1863

#### Legislative history

- **Introduced in the House of Representatives as H.R. 3162** by Frank J. Sensenbrenner, Jr. (R-WI) on October 23, 2001
- **Committee consideration by** [United States House Committee on the Judiciary](#); [Permanent Select Committee on Intelligence](#); [Committee on Financial Services](#); [Committee on International Relations](#); [Committee on Energy and Commerce](#) (Subcommittee on Telecommunications and the Internet); [Committee on Education and the Workforce](#); [Committee on Transportation and Infrastructure](#); [Committee on Armed Services](#)
- **Passed the House on** October 24, 2001 (Yeas: 357; Nays: 66)
- **Passed the Senate on** October 25, 2001 (Yeas: 98; Nays: 1)
- **Signed into law by President George W. Bush on** October 26, 2001<sup>[1]</sup>

#### Major amendments

[USA Freedom Act](#)

## Contents

### 1 Titles

1.1 Title I: Enhancing domestic security against terrorism

1.2 Title II: Surveillance procedures

1.3 Title III: Anti-money-laundering to prevent terrorism

1.4 Title IV: Border security

1.5 Title V: Removing obstacles to investigating terrorism

1.6 Title VI: Victims and families of victims of terrorism

1.7 Title VII: Increased information sharing for critical infrastructure protection

1.8 Title VIII: Terrorism criminal law

1.9 Title IX: Improved intelligence

1.10 Title X: Miscellaneous

### 2 Section expirations

### 3 Controversy

### 4 Reauthorizations

### 5 See also

### 6 References

### 7 Further reading

7.1 Law review articles

7.2 Books

### 8 External links

8.1 Supportive views

8.2 Critical views

8.3 Other

## Titles [[edit](#)]

## **Title I: Enhancing domestic security against terrorism** [\[edit\]](#)

*Main article: [Patriot Act, Title I](#)*

Title I authorizes measures to enhance the ability of domestic security services to prevent terrorism. The title established a fund for counter-terrorist activities and increased funding for the Terrorist Screening Center which is administered by the FBI. The military was authorized to provide assistance in some situations that involve weapons of mass destruction when so requested by the [Attorney General](#). The National Electronic Crime Task Force was expanded, along with the [President's](#) authority and abilities in cases of terrorism. The title also condemned the discrimination against Arab and Muslim Americans that happened soon after the September 11 terrorist attacks. The impetus for many of the provisions came from earlier bills, for instance the condemnation of discrimination was originally proposed by Senator [Tom Harkin \(D-IA\)](#) in an amendment to the *Combatting Terrorism Act of 2001*, though in a different form. It originally included "the prayer of [Cardinal Theodore McCarrick](#), the [Archbishop of Washington](#) in a [Mass](#) on September 12, 2001 for our Nation and the victims in the immediate aftermath of the terrorist hijackings and attacks in New York City, [Washington, D.C.](#), and [Pennsylvania](#) reminds all Americans that 'We must seek the guilty and not strike out against the innocent or we become like them who are without moral guidance or proper direction.'"<sup>[11]</sup> Further condemnation of racial vilification and violence is also spelled out in Title X, where there was condemnation of such activities against [Sikh](#) Americans, who were mistaken for Muslims after the September 11th terrorist attack.<sup>[12]</sup>

## **Title II: Surveillance procedures** [\[edit\]](#)

*Main article: [Patriot Act, Title II](#)*

Title II is titled "Enhanced Surveillance Procedures", and covers all aspects of the surveillance of suspected terrorists, those suspected of engaging in computer fraud or abuse, and agents of a foreign power who are engaged in clandestine activities. It primarily made amendments to FISA,

and the ECPA, and many of the most controversial aspects of the USA PATRIOT Act reside in this title. In particular, the title allows government agencies to gather "foreign intelligence information" from both U.S. and non-U.S. citizens, and changed FISA to make gaining foreign intelligence information the significant purpose of FISA-based surveillance, where previously it had been the primary purpose.<sup>[13]</sup> The change in definition was meant to remove a legal "wall" between criminal investigations and surveillance for the purposes of gathering foreign intelligence, which hampered investigations when criminal and foreign surveillance overlapped.<sup>[14]</sup> However, that this wall even existed was found by the Federal Surveillance Court of Review to have actually been a long-held misinterpretation by government agencies. Also removed was the statutory requirement that the government prove a surveillance target under FISA is a non-U.S. citizen and agent of a foreign power, though it did require that any investigations must not be undertaken on citizens who are carrying out activities protected by the First Amendment.<sup>[15]</sup> The title also expanded the duration of FISA physical search and surveillance orders,<sup>[16]</sup> and gave authorities the ability to share information gathered before a federal grand jury with other agencies.<sup>[17]</sup>

The scope and availability of wiretapping and surveillance orders were expanded under Title II. Wiretaps were expanded to include addressing and routing information to allow surveillance of [packet switched networks](#)<sup>[18]</sup>—the [Electronic Privacy Information Center](#) (EPIC) objected to this, arguing that it does not take into account email or web addresses, which often contain content in the address information.<sup>[19]</sup> The Act allowed any district court judge in the United States to issue such surveillance orders<sup>[18]</sup> and search warrants for terrorism investigations.<sup>[20]</sup> Search warrants were also expanded, with the Act amending Title III of the *Stored Communications Access Act* to allow the FBI to gain access to stored voicemail through a search warrant, rather than through the more stringent wiretap laws.<sup>[21]</sup>

Various provisions allowed for the disclosure of electronic communications to law enforcement agencies. Those who operate or own a "protected computer" can give permission for authorities to

intercept communications carried out on the machine, thus bypassing the requirements of the Wiretap statute.<sup>[22]</sup> The definition of a "protected computer" is defined in [18 U.S.C. § 1030\(e\)\(2\)](#) and broadly encompasses those computers used in interstate or foreign commerce or communication, including ones located outside the United States. The law governing obligatory and voluntary disclosure of customer communications by [cable](#) companies was altered to allow agencies to demand such communications under U.S.C. Title 18 provisions relating to the disclosure of electronic communications (chapter 119), [pen registers](#) and [trap and trace devices](#) (chapter 206) and stored communications (121), though it excluded the disclosure of cable subscriber viewing habits.<sup>[23]</sup> [Subpoenas](#) issued to [Internet Service Providers](#) were expanded to include not only "the name, address, local and long distance telephone toll billing records, telephone number or other subscriber number or identity, and length of service of a subscriber" but also session times and durations, types of services used, communication device address information (e.g. [IP addresses](#)), payment method and bank account and credit card numbers.<sup>[24]</sup> Communication providers are also allowed to disclose customer records or communications if they suspect there is a danger to "life and limb".<sup>[25]</sup>

Title II established three very controversial provisions: "[sneak and peek](#)" warrants, [roving wiretaps](#) and the ability of the FBI to gain access to documents that reveal the patterns of U.S. citizens. The so-called "sneak and peek" law allowed for delayed notification of the execution of search warrants. The period before which the FBI must notify the recipients of the order was unspecified in the Act—the FBI field manual says that it is a "flexible standard"<sup>[26]</sup>—and it may be extended at the court's discretion.<sup>[27]</sup> These sneak and peek provisions were struck down by judge [Ann Aiken](#) on September 26, 2007 after a [Portland](#) attorney, [Brandon Mayfield](#), was wrongly jailed because of the searches. The court found the searches to violate the provision that prohibits unreasonable searches in the Fourth Amendment to the U.S. Constitution.<sup>[28][29]</sup>

Roving wiretaps are wiretap orders that do not need to specify all common carriers and third



parties in a surveillance court order. These are seen as important by the Department of Justice because they believe that terrorists can exploit wiretap orders by rapidly changing locations and communication devices such as cell phones,<sup>[30]</sup> while opponents see it as violating the particularity clause of the [Fourth Amendment](#).<sup>[31][32]</sup> Another highly controversial provision is one that allows the FBI to make an order "requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution."<sup>[33]</sup> Though it was not targeted directly at libraries, the [American Library Association](#) (ALA), in particular, opposed this provision.<sup>[34]</sup> In a resolution passed on June 29, 2005, they stated that "Section 215 of the USA PATRIOT Act allows the government to secretly request and obtain library records for large numbers of individuals without any reason to believe they are involved in illegal activity."<sup>[35]</sup> However, the ALA's stance did not go without criticism. One prominent critic of the ALA's stance was the [Manhattan Institute's Heather Mac Donald](#), who argued in an article for the [New York City Journal](#) that "[t]he furor over section 215 is a case study in Patriot Act fear-mongering."<sup>[36]</sup>

The title also covers a number of other miscellaneous provisions, including the expansion of the number of FISC judges from seven to eleven (three of which must reside within 20 miles (32 km) of the [District of Columbia](#)),<sup>[37]</sup> trade [Sanctions against North Korea](#) and [Taliban-controlled Afghanistan](#)<sup>[38]</sup> and the employment of [translators](#) by the FBI.<sup>[39]</sup>

At the insistence of Republican Representative [Richard Arme](#)y,<sup>[40]</sup> the Act had a number of [sunset provisions](#) built in, which were originally set to expire on December 31, 2005. The sunset provision of the Act also took into account any ongoing foreign intelligence investigations and allowed them to continue once the sections had expired.<sup>[41]</sup> The provisions that were to expire are below.

## Title III: Anti-money-laundering to prevent terrorism [\[edit\]](#)

*Main article: [Patriot Act, Title III](#)*

Title III of the Act, titled "International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001," is intended to facilitate the prevention, detection and prosecution of international [money laundering](#) and the financing of [terrorism](#). It primarily amends portions of the [Money Laundering Control Act of 1986](#) (MLCA) and the [Bank Secrecy Act of 1970](#) (BSA). It was divided into three subtitles, with the first dealing primarily with strengthening banking rules against money laundering, especially on the international stage. The second attempts to improve communication between law enforcement agencies and financial institutions, as well as expanding record keeping and reporting requirements. The third subtitle deals with currency smuggling and counterfeiting, including quadrupling the maximum penalty for counterfeiting foreign currency.

The first subtitle tightened the record keeping requirements for financial institutions, making them record the aggregate amounts of transactions processed from areas of the world where money laundering is a concern to the U.S. government. It also made institutions put into place reasonable steps to identify [beneficial owners](#) of bank accounts and those who are authorized to use or route funds through [payable-through accounts](#).<sup>[42]</sup> The U.S. Treasury was charged with formulating regulations intended to foster information sharing between financial institutions to prevent money-laundering.<sup>[43]</sup> Along with expanding record keeping requirements it put new regulations into place to make it easier for authorities to identify money laundering activities and to make it harder for money launderers to mask their identities.<sup>[44]</sup> If money laundering was uncovered, the subtitle legislated for the [forfeiture of assets](#) of those suspected of doing the money laundering.<sup>[45]</sup> In an effort to encourage institutions to take steps that would reduce money laundering, the Treasury was given authority to block mergers of [bank holding companies](#) and [banks](#) with other banks and bank holding companies that had a bad history of preventing money laundering. Similarly, mergers between insured depository institutions and non-insured depository institutions that have a bad

track record in combating money-laundering could be blocked.<sup>[46]</sup>

Restrictions were placed on accounts and foreign banks. It prohibited [shell banks](#) that are not an affiliate of a bank that has a physical presence in the U.S. or that are not subject to supervision by a banking authority in a non-U.S. country. It also prohibits or restricts the use of certain accounts held at financial institutions.<sup>[47]</sup> Financial institutions must now undertake steps to identify the owners of any privately owned bank outside the U.S. who have a [correspondent account](#) with them, along with the interests of each of the owners in the bank. It is expected that additional scrutiny will be applied by the U.S. institution to such banks to make sure they are not engaging in money laundering. Banks must identify all the nominal and beneficial owners of any private bank account opened and maintained in the U.S. by non-U.S. citizens. There is also an expectation that they must undertake enhanced scrutiny of the account if it is owned by, or is being maintained on behalf of, any senior [political figure](#) where there is reasonable suspicion of [corruption](#).<sup>[48]</sup> Any deposits made from within the U.S. into foreign banks are now deemed to have been deposited into any [interbank account](#) the foreign bank may have in the U.S. Thus any [restraining order](#), seizure warrant or [arrest warrant](#) may be made against the funds in the interbank account held at a U.S. financial institution, up to the amount deposited in the account at the foreign bank.<sup>[49]</sup>

Restrictions were placed on the use of internal bank [concentration accounts](#) because such accounts do not provide an effective [audit trail](#) for transactions, and this may be used to facilitate money laundering. Financial institutions are prohibited from allowing clients to specifically direct them to move funds into, out of, or through a concentration account, and they are also prohibited from informing their clients about the existence of such accounts. Financial institutions are not allowed to provide any information to clients that may identify such internal accounts.<sup>[50]</sup> Financial institutions are required to document and follow methods of identifying where the funds are for each customer in a concentration account that co-mingles funds belonging to one or more customers.

The definition of money laundering was expanded to include making a financial transaction in the U.S. in order to commit a violent crime;<sup>[51]</sup> the bribery of public officials and fraudulent dealing with public funds; the smuggling or illegal export of controlled munition<sup>[52]</sup> and the importation or bringing in of any firearm or ammunition not authorized by the U.S. Attorney General<sup>[53]</sup> and the smuggling of any item controlled under the Export Administration Regulations.<sup>[54][55]</sup> It also includes any offense where the U.S. would be obligated under a [mutual treaty](#) with a foreign nation to [extradite](#) a person, or where the U.S. would need to submit a case against a person for prosecution because of the treaty; the import of falsely classified goods;<sup>[56]</sup> [computer crime](#);<sup>[57]</sup> and any [felony](#) violation of the *Foreign Agents Registration Act of 1938*.<sup>[55]</sup> It also allows the forfeiture of any property within the jurisdiction of the United States that was gained as the result of an offense against a foreign nation that involves the manufacture, importation, sale, or distribution of a controlled substance.<sup>[58]</sup> Foreign nations may now seek to have a forfeiture or judgment notification enforced by a district court of the United States.<sup>[59]</sup> This is done through new legislation that specifies how the U.S. government may apply for a restraining order<sup>[60]</sup> to preserve the availability of property which is subject to a foreign forfeiture or confiscation judgement.<sup>[61]</sup> In taking into consideration such an application, emphasis is placed on the ability of a foreign court to follow [due process](#).<sup>[59]</sup> The Act also requires the Secretary of Treasury to take all reasonable steps to encourage foreign governments make it a requirement to include the name of the originator in [wire transfer](#) instructions sent to the United States and other countries, with the information to remain with the transfer from its origination until the point of disbursement.<sup>[62]</sup> The Secretary was also ordered to encourage international cooperation in investigations of money laundering, [financial crimes](#), and the finances of terrorist groups.<sup>[63]</sup>

The Act also introduced criminal penalties for corrupt officialdom. An official or employee of the government who acts corruptly—as well as the person who induces the corrupt act—in the carrying out of their official duties will be fined by an amount that is not more than three times the

monetary equivalent of the bribe in question. Alternatively they may be imprisoned for not more than 15 years, or they may be fined and imprisoned. Penalties apply to financial institutions who do not comply with an order to terminate any corresponding accounts within 10 days of being so ordered by the Attorney General or the Secretary of Treasury. The financial institution can be fined [\\$US10,000](#) for each day the account remains open after the 10-day limit has expired.<sup>[49]</sup>

The second annotation made a number of modifications to the BSA in an attempt to make it harder for money launderers to operate and easier for law enforcement and regulatory agencies to police money laundering operations. One amendment made to the BSA was to allow the designated officer or agency who receives [suspicious activity reports](#) to notify U.S. intelligence agencies.<sup>[64]</sup> A number of amendments were made to address issues related to record keeping and financial reporting. One measure was a new requirement that anyone who does business file a report for any coin and foreign currency receipts that are over US\$10,000 and made it illegal to structure transactions in a manner that evades the BSA's reporting requirements.<sup>[65]</sup> To make it easier for authorities to regulate and investigate anti-money laundering operations Money Services Businesses (MSBs)—those who operate [informal value transfer systems](#) outside of the mainstream financial system—were included in the definition of a financial institution.<sup>[66]</sup> The BSA was amended to make it mandatory to report suspicious transactions and an attempt was made to make such reporting easier for financial institutions.<sup>[67]</sup> [FinCEN](#) was made a [bureau](#) of the [United States Department of Treasury](#)<sup>[68]</sup> and the creation of a secure [network](#) to be used by financial institutions to report suspicious transactions and to provide alerts of relevant suspicious activities was ordered.<sup>[69]</sup> Along with these reporting requirements, a considerable number of provisions relate to the prevention and prosecution of money-laundering.<sup>[70]</sup> Financial institutions were ordered to establish anti-money laundering programs and the BSA was amended to better define anti-money laundering strategy.<sup>[71]</sup> Also increased were civil and criminal penalties for money laundering and the introduction of penalties for violations of [geographic targeting orders](#) and

certain record-keeping requirements.<sup>[72]</sup> A number of other amendments to the BSA were made through subtitle B, including granting the [Board of Governors of the Federal Reserve System](#) power to authorize personnel to act as law enforcement officers to protect the premises, grounds, property and personnel of any U.S. National reserve bank and allowing the Board to delegate this authority to U.S. Federal reserve bank.<sup>[73]</sup> Another measure instructed United States Executive Directors of international financial institutions to use their voice and vote to support any country that has taken action to support the U.S.'s War on Terrorism. Executive Directors are now required to provide ongoing auditing of disbursements made from their institutions to ensure that no funds are paid to persons who commit, threaten to commit, or support terrorism.<sup>[74]</sup>

The third subtitle deals with currency crimes. Largely because of the effectiveness of the BSA, money launders had been avoiding traditional financial institutions to launder money and were using cash-based businesses to avoid them. A new effort was made to stop the laundering of money through bulk currency movements, mainly focusing on the confiscation of criminal proceeds and the increase in penalties for money laundering. Congress found that a criminal offense of merely evading the reporting of money transfers was insufficient and decided that it would be better if the smuggling of the bulk currency itself was the offense. Therefore, the BSA was amended to make it a criminal offense to evade currency reporting by concealing more than US\$10,000 on any person or through any luggage, merchandise or other container that moves into or out of the U.S. The penalty for such an offense is up to 5 years imprisonment and the forfeiture of any property up to the amount that was being smuggled.<sup>[75]</sup> It also made the civil and criminal penalty violations of currency reporting cases<sup>[76]</sup> be the forfeiture of all a defendant's property that was involved in the offense, and any property traceable to the defendant.<sup>[77]</sup> The Act prohibits and penalizes those who run unlicensed money transmitting businesses.<sup>[78]</sup> In 2005, this provision of the USA PATRIOT Act was used to prosecute Yehuda Abraham for helping to arrange money transfers for British arms dealer Hermant Lakhani, who was arrested in August 2003 after

being caught in a government sting. Lakhani had tried to sell a missile to an FBI agent posing as a [Somali](#) militant.<sup>[79]</sup> The definition of counterfeiting was expanded to encompass analog, digital or electronic image reproductions, and it was made an offense to own such a reproduction device. Penalties were increased to 20 years imprisonment.<sup>[80]</sup> Money laundering "unlawful activities" was expanded to include the [provision of material support or resources to designated foreign terrorist organizations](#).<sup>[81]</sup> The Act specifies that anyone who commits or conspires to undertake a fraudulent activity [outside the jurisdiction](#) of the United States, and which would be an offense in the U.S., will be prosecuted under [18 U.S.C. § 1029](#), which deals with fraud and related activity in connection with access devices.<sup>[82]</sup>

## **Title IV: Border security** [\[edit\]](#)

*Main article: [Patriot Act, Title IV](#)*

Title IV amends the [Immigration and Nationality Act of 1952](#) to give more law enforcement and investigative power to the United States Attorney General and to the [Immigration and Naturalization Service](#) (INS). The Attorney General was authorized to waive any cap on the number of full-time [employees](#) (FTEs) assigned to the INS on the [Northern border](#) of the United States.<sup>[83]</sup> Enough funds were set aside to triple the maximum number of [Border Patrol](#) personnel, Customs Service personnel and INS inspectors along with an additional US\$50,000,000 funding for the INS and the [U.S. Customs Service](#) to improve technology for monitoring the Northern Border and acquiring additional equipment at the Canadian northern border.<sup>[84]</sup> The INS was also given the authority to authorize overtime payments of up to an extra US\$30,000 a year to INS employees.<sup>[85]</sup> Access was given to the [Department of State](#) and the INS to criminal background information contained in the [National Crime Information Center's Interstate Identification Index](#) (NCIC-III), [Wanted Persons File](#) and any other files maintained by the [National Crime Information Center](#) to determine whether [visa](#) applicants and applicants could be admitted to the U.S.<sup>[86]</sup> The [Department of State](#) was required

to form final regulations governing the procedures for taking fingerprints and the conditions with which the department was allowed to use this information.<sup>[87]</sup> Additionally, the [National Institute of Standards and Technology](#) (NIST) was ordered to develop a technology standard to verify the identity of persons applying for a United States visa.<sup>[87]</sup> The reason was to make the standard the technology basis for a cross-agency, cross-platform electronic system used for conducting [background checks](#), confirming identities and ensuring that people have not received visas under different names.<sup>[88]</sup> This report was released on November 13, 2002,<sup>[89]</sup> however, according to NIST, this was later "determined that the fingerprint system used was not as accurate as current state-of-the-art fingerprint systems and is approximately equivalent to commercial fingerprint systems available in 1998."<sup>[90]</sup> This report was later superseded by section 303(a) of the [Enhanced Border Security and Visa Entry Reform Act of 2002](#).

Under subtitle C, various definitions relating to terrorism were altered and expanded. The INA was [retroactively](#) amended to disallow aliens who are part of or representatives of a foreign organization or any group who endorses acts of terrorism from entering the U.S. This restriction also included the family of such aliens.<sup>[91]</sup> The definition of "terrorist activity" was strengthened to include actions involving the use of any dangerous device (and not just explosives and firearms).<sup>[91]</sup> To "engage in terrorist activity" is defined as committing, inciting to commit or planning and preparing to undertake an act of terrorism. Included in this definition is the gathering of intelligence information on potential terrorist targets, the solicitation of funds for a terrorist organization or the solicitation of others to undertake acts of terrorism. Those who provide knowing assistance to a person who is planning to perform such activities are defined as undertaking terrorist activities. Such assistance includes affording material support, including a [safe house](#), transportation, communications, funds, transfer of funds or other material financial benefit, false documentation or identification, weapons (including [chemical](#), [biological](#), or [radiological weapons](#)), explosives, or training to perform the terrorist act.<sup>[91]</sup> The INA criteria for making a decision to




designate an organization as a terrorist organization was amended to include the definition of a terrorist act.<sup>[92]</sup> Though the amendments to these definitions are retroactive, it does not mean that it can be applied to members who joined an organization, but since left, before it was designated to be a terrorist organization under [8 U.S.C. § 1189](#) by the Secretary of State.<sup>[91]</sup>

The Act amended the INA to add new provisions enforcing mandatory detention laws. These apply to any alien who is engaged in terrorism, or who is engaged in an activity that endangers U.S. national security. It also applies to those who are inadmissible or who must be deported because it is certified they are attempting to enter to undertake illegal [espionage](#); are exporting goods, technology, or sensitive information illegally; or are attempting to control or overthrow the government; or have, or will have, engaged in terrorist activities.<sup>[93]</sup> The Attorney General or the Attorney General's deputy may maintain custody of such aliens until they are removed from the U.S., unless it is no longer deemed they should be removed, in which case they are released. The alien can be detained for up to 90 days but can be held up to six months after it is deemed that they are a national security threat. However, the alien must be charged with a crime or removal proceedings start no longer than seven days after the alien's detention, otherwise the alien will be released. However, such detentions must be reviewed every six months by the Attorney General, who can then decide to revoke it, unless prevented from doing so by law. Every six months the alien may apply, in writing, for the certification to be reconsidered.<sup>[93]</sup> [Judicial review](#) of any action or decision relating to this section, including judicial review of the merits of a certification, can be held under [habeas corpus](#) proceedings. Such proceedings can be initiated by an application filed with the [United States Supreme Court](#), by any justice of the Supreme Court, by any [circuit judge](#) of the [United States Court of Appeals](#) for the [District of Columbia Circuit](#), or by any [district court](#) otherwise having jurisdiction to entertain the application. The final order is subject to [appeal](#) to the [United States Court of Appeals](#) for the District of Columbia Circuit.<sup>[93]</sup> Provisions were also made for a report to be required every six months of such decisions from the U.S. Attorney General to

the [Committee on the Judiciary of the House of Representatives](#) and the [Committee on the Judiciary of the Senate](#).<sup>[93]</sup>

A sense of Congress was given that the U.S. Secretary of State should expedite the full implementation of the integrated entry and exit data system for airports, seaports, and land border ports of entry specified in the *Illegal Immigration Reform and Immigrant Responsibility Act of 1996* (IIRIRA). They also found that the U.S. Attorney General should immediately start the Integrated Entry and Exit Data System Task Force specified in section 3 of the *Immigration and Naturalization Service Data Management Improvement Act of 2000*. Congress wanted the primary focus of development of the entry-exit data system was to be on the utilization of biometric technology and the development of tamper-resistant documents readable at ports of entry. They also wanted the system to be able to interface with existing law enforcement databases.<sup>[94]</sup> The Attorney General was ordered to implement and expand the foreign student monitoring program that was established under section 641(a) of the IIRIRA.<sup>[95]</sup> which records the date and port of entry of each foreign student. The program was expanded to include other approved educational institutions, including air flight schools, language training schools or vocational schools that are approved by the Attorney General, in consultation with the [Secretary of Education](#) and the Secretary of State. US\$36,800,000 was appropriated for the [Department of Justice](#) to spend on implementing the program.<sup>[96]</sup>

The Secretary of State was ordered to audit and report back to Congress on the Visa waiver program specified under [8 U.S.C. § 1187](#)  for each fiscal year until September 30, 2007. The Secretary was also ordered to check for the implementation of precautionary measures to prevent the counterfeiting and theft of passports as well as ascertain that countries designated under the visa waiver program have established a program to develop tamper-resistant passports.<sup>[97]</sup> The Secretary was also ordered to report back to Congress on whether [consulate shopping](#) was a problem.<sup>[98]</sup>

The last subtitle, which was introduced by Senators John Conyers and Patrick Leahy, allows for the preservation of immigration benefits for victims of terrorism, and the families of victims of terrorism.<sup>[99]</sup> They recognized that some families, through no fault of their own, would either be ineligible for permanent residence in the United States because of being unable to make important deadlines because of the September 11 terrorist attacks, or had become ineligible to apply for special immigration status because their loved one died in the attacks.<sup>[100]</sup>

## **Title V: Removing obstacles to investigating terrorism** [\[edit\]](#)

*Main article: [Patriot Act, Title V](#)*

It allows the U.S. Attorney General to pay rewards pursuant of advertisements for assistance to the Department of Justice to combat terrorism and prevent terrorist acts, though amounts over \$US250,000 may not be made or offered without the personal approval of the Attorney General or President, and once the award is approved the Attorney General must give written notice to the Chairman and ranking minority members of the Committee on Appropriations and the Judiciary of the Senate and of the House of Representatives.<sup>[101]</sup> The *State Department Basic Authorities Act of 1956* was amended to allow the Department of State to offer rewards, in consultation with the Attorney General, for the full or significant dismantling of any terrorist organization<sup>[102]</sup> and to identify any key leaders of terrorist organizations.<sup>[103]</sup> The Secretary of State was given authority to pay greater than \$US5 million if he so determines it would prevent terrorist actions against the United States and Canada.<sup>[104]</sup> The *DNA Analysis Backlog Elimination Act* was amended to include terrorism or crimes of violence in the list of qualifying Federal offenses.<sup>[105]</sup> Another perceived obstacle was to allow federal agencies to share information with federal law enforcement agencies. Thus, the act now allows federal officers who acquire information through electronic surveillance or physical searches to consult with federal law enforcement officers to coordinate efforts to investigate or protect against potential or actual attacks, sabotage or international terrorism or

clandestine intelligence activities by an intelligence service or network of a foreign power.<sup>[106]</sup>

[Secret Service](#) jurisdiction was extended to investigate computer fraud, access device frauds, false identification documents or devices, or any fraudulent activities against U.S. financial institutions.<sup>[107]</sup> The *General Education Provisions Act* was amended to allow the U.S. Attorney General or Assistant Attorney General to collect and retain educational records relevant to an authorized investigation or prosecution of an offense that is defined as a Federal crime of terrorism and which an educational agency or institution possesses. The Attorney General or Assistant Attorney General must "certify that there are specific and articulable facts giving reason to believe that the education records are likely to contain information [that a Federal crime of terrorism may be being committed]." An education institution that produces education records in response to such a request is given legal immunity from any liability that rises from such a production of records.<sup>[108]</sup>

One of the most controversial aspects of the USA PATRIOT Act is in title V, and relates to [National Security Letters](#) (NSLs). An NSL is a form of [administrative subpoena](#) used by the FBI, and reportedly by other U.S. government agencies including the CIA and the [Department of Defense](#) (DoD). It is a demand letter issued to a particular entity or organization to turn over various records and data pertaining to individuals. They require no probable cause or judicial oversight and also contain a [gag order](#), preventing the recipient of the letter from disclosing that the letter was ever issued. Title V allowed the use of NSLs to be made by a Special Agent in charge of a Bureau field office, where previously only the Director or the Deputy Assistant Director of the FBI were able to certify such requests.<sup>[109]</sup> This provision of the Act was challenged by the ACLU on behalf of an unknown party against the U.S. government on the grounds that NSLs violate the First and Fourth Amendments of the U.S. Constitution because there is no way to legally oppose an NSL subpoena in court, and that it was unconstitutional not to allow a client to inform their Attorney as to the order because of the gag provision of the letters. The court's judgement found in favour of the ACLU's

case, and they declared the law unconstitutional.<sup>[110]</sup> Later, the USA PATRIOT Act was reauthorized and amendments were made to specify a process of judicial review of NSLs and to allow the recipient of an NSL to disclose receipt of the letter to an attorney or others necessary to comply with or challenge the order.<sup>[111]</sup> However, in 2007 the U.S. District Court struck down even the reauthorized NSLs because the gag power was unconstitutional as courts could still not engage in meaningful judicial review of these gags. On August 28, 2015, Judge Victor Marrero of the federal district court in Manhattan ruled the gag order of [Nicholas Merrill](#) was unjustified. In his decision, Judge Marrero described the FBI's position as, "extreme and overly broad," affirming that "courts consistent with the First Amendment, simple accept the Government's assertions that disclosure would implicate and create a risk." He also found that the FBI's gag order on Mr. Merrill "implicates serious issues, both with respect to the First Amendment and accountability of the government to the people."<sup>[112]</sup> Initially, the ruling was released in [redaction](#) by Judge Marrero. The FBI was given 90 days to pursue any other alternative course of action, but elected not to do so. Upon release of the unredacted ruling on November 30, 2015, it was revealed for the first time the extent to which the FBI's NSL accompanied by a gag order sought to collect information. Through the court documents, it was revealed for the first time that through an NSL, the FBI believes it can legally obtain information including an individual's complete [web browsing history](#), the [IP addresses](#) of everyone a person has corresponded with, and all the records of all online purchases within the last 180 days. The FBI also claims via the extension of a NSL, it can obtain [cell site](#) location information. In the landmark case of Nicholas Merrill the FBI in specific sought to seek the following information on an account: DSL account information, radius log, subscriber name and related subscriber information, account number, date the account opened or closed, addresses associated with the account, subscriber day/evening telephone numbers, screen names or other on-line names associated with the account, order forms, records relating to merchandise orders/shipping information for the last 180 days, all billing related to the account, [internet service provider](#) (ISP), all email addresses associated with the account, internet protocol

address assigned to the account, all website information registered to the account, uniform resource locator address assigned to the account, any other information which you consider to be an electronic communication transactional record. This was the first time it was revealed the extent to which an NSL under the Patriot Act could request communication information.<sup>[113][114]</sup>

## **Title VI: Victims and families of victims of terrorism** [\[edit\]](#)

*Main article: [Patriot Act, Title VI](#)*

Title VI amended the *Victims of Crime Act of 1984* (VOCA) to change how the U.S. Victims of Crime Fund was managed and funded, improving the speedy provision of aid to families of public safety officers by expedited payments to officers or the families of officers injured or killed in the line of duty. Payments must be made no later than 30 days later.<sup>[115]</sup> The Assistant Attorney General was given expanded authority under Section 614 of the U.S.A. P.A.T.R.I.O.T. Act to make grants to any organization that administers any [Office of Justice Programs](#), which includes the Public Safety Officers Benefits Program.<sup>[116]</sup> Further changes to the Victims of Crime Fund increased the amount of money in the Fund and changed the way that funds were distributed.<sup>[117]</sup> The amount available for grants made through the Crime Victim Fund to eligible crime victim compensation programs were increased from 40 percent to 60 percent of the total in the Fund. A program can provide compensation to U.S. citizens who were adversely affected overseas. [Means testing](#) was also waived for those who apply for compensation.<sup>[118]</sup> Under VOCA, the Director may make an annual grant from the Crime Victims Fund to support crime victim assistance programs. An amendment was made to VOCA to include offers of assistance to crime victims in the [District of Columbia](#), the [Commonwealth of Puerto Rico](#), the [United States Virgin Islands](#), and any other U.S. territory.<sup>[119]</sup> VOCA also provides for compensation and assistance to victims of terrorism or mass violence.<sup>[120]</sup> This was amended to allow the Director to make supplemental grants to States for eligible crime victim compensation and assistance programs, and to victim service organizations,

public agencies (including Federal, State, or local governments) and non-governmental organizations that provide assistance to victims of crime. The funds could be used to provide emergency relief, including crisis response efforts, assistance, compensation, training and technical assistance for investigations and prosecutions of terrorism.<sup>[121]</sup>

## **Title VII: Increased information sharing for critical infrastructure protection**

[\[edit\]](#)

*Main article: [Patriot Act, Title VII](#)*

Title VII has one section. The purpose of this title is to increase the ability of U.S. law enforcement to counter terrorist activity that crosses jurisdictional boundaries. It does this by amending the [Omnibus Crime Control and Safe Streets Act of 1968](#) to include terrorism as a criminal activity.

## **Title VIII: Terrorism criminal law** [\[edit\]](#)

*Main article: [Patriot Act, Title VIII](#)*

Title VIII alters the definitions of terrorism, and establishes or re-defines rules with which to deal with it. It redefined the term "domestic terrorism" to broadly include mass destruction as well as assassination or kidnapping as a terrorist activity. The definition also encompasses activities that are "dangerous to human life that are a violation of the criminal laws of the United States or of any State" and are intended to "intimidate or coerce a civilian population," "influence the policy of a government by intimidation or coercion," or are undertaken "to affect the conduct of a government by mass destruction, assassination, or kidnapping" while in the jurisdiction of the United States.<sup>[122]</sup> Terrorism is also included in the definition of [racketeering](#).<sup>[123]</sup> Terms relating to [cyber-terrorism](#) are also redefined, including the term "protected computer," "damage," "conviction," "person," and "loss."<sup>[124]</sup>

New penalties were created to convict those who attack [mass transportation systems](#). If the

offender committed such an attack while no passenger was on board, they are fined and imprisoned for a maximum of 20 years. However, if the activity was undertaken while the mass transportation vehicle or ferry was carrying a passenger at the time of the offense, or the offense resulted in the [death](#) of any person, then the punishment is a fine and life imprisonment.<sup>[125]</sup> The title amends the biological weapons statute to define the use of a biological agent, toxin, or delivery system as a weapon, other than when it is used for "[prophylactic](#), protective, [bona fide](#) research, or other peaceful purposes." Penalties for anyone who cannot prove reasonably that they are using a biological agent, toxin or delivery system for these purposes are 10 years imprisonment, a fine or both.<sup>[126]</sup>

A number of measures were introduced in an attempt to prevent and penalize activities that are deemed to support terrorism. It was made a crime to harbor or conceal terrorists, and those who do are subject to a fine or imprisonment of up to 10 years, or both.<sup>[127]</sup> U.S. [forfeiture](#) law was also amended to allow authorities to seize all foreign and domestic assets from any group or individual that is caught planning to commit acts of terrorism against the U.S. or U.S. citizens. Assets may also be seized if they have been acquired or maintained by an individual or organization for the purposes of further terrorist activities.<sup>[128]</sup> One section of the Act (section 805) prohibited "material support" for terrorists, and in particular included "expert advice or assistance."<sup>[129]</sup> In 2004, after the [Humanitarian Law Project](#) filed a civil action against the U.S. government, a Federal District Court struck this down as unconstitutionally vague;<sup>[130]</sup> but in 2010 the Supreme Court upheld it.<sup>[131]</sup> Congress later improved the law by defining the definitions of the "material support or resources," "training," and "expert advise or resources."<sup>[132]</sup>

Cyberterrorism was dealt with in various ways. Penalties apply to those who either damage or gain unauthorized access to a protected computer and then commit a number of offenses. These offenses include causing a person to lose an aggregate amount greater than US\$5,000, as well as adversely affecting someone's medical examination, diagnosis or treatment. It also encompasses



actions that cause a person to be injured, a threat to public health or safety, or damage to a governmental computer that is used as a tool to administer justice, national defense or national security. Also prohibited was extortion undertaken via a protected computer. The penalty for attempting to damage protected computers through the use of viruses or other software mechanism was set to imprisonment for up to 10 years, while the penalty for unauthorized access and subsequent damage to a protected computer was increased to more than five years imprisonment. However, should the offense occur a second time, the penalty increases up to 20 years imprisonment.<sup>[133]</sup> The act also specified the development and support of cybersecurity forensic capabilities. It directs the Attorney General to establish regional computer forensic laboratories that have the capability of performing forensic examinations of intercepted computer evidence relating to criminal activity and cyberterrorism, and that have the capability of training and educating Federal, State, and local law enforcement personnel and prosecutors in computer crime, and to "facilitate and promote the sharing of Federal law enforcement expertise and information about the investigation, analysis, and prosecution of computer-related crime with State and local law enforcement personnel and prosecutors, including the use of multijurisdictional task forces." The sum of \$50,000,000 was authorized for establishing such labs.<sup>[134]</sup>

## **Title IX: Improved intelligence** [\[edit\]](#)

*Main article: [Patriot Act, Title IX](#)*

Title IX amends the *National Security Act of 1947* to require the [Director of Central Intelligence](#) (DCI) to establish requirements and priorities for foreign intelligence collected under FISA and to provide assistance to the United States Attorney General to ensure that information derived from electronic surveillance or physical searches is disseminated for efficient and effective foreign intelligence purposes.<sup>[135]</sup> With the exception of information that might jeopardize an ongoing law enforcement investigation, it was made a requirement that the Attorney General, or the head of

any other department or agency of the Federal Government with law enforcement responsibilities, disclose to the Director any foreign intelligence acquired by the U.S. Department of Justice. The Attorney General and Director of Central Intelligence were directed to develop procedures for the Attorney General to follow in order to inform the Director, in a timely manner, of any intention of investigating criminal activity of a foreign intelligence source or potential foreign intelligence source based on the intelligence tip-off of a member of the intelligence community. The Attorney General was also directed to develop procedures on how to best administer these matters.<sup>[136]</sup> International terrorist activities were made to fall within the scope of foreign intelligence under the *National Security Act*.<sup>[137]</sup>

A number of reports were commissioned relating to various intelligence-related government centers. One was commissioned into the best way of setting up the [National Virtual Translation Center](#), with the goal of developing automated translation facilities to assist with the timely and accurate translation of foreign intelligence information for elements of the U.S. intelligence community.<sup>[138]</sup> The USA PATRIOT Act required this to be provided on February 1, 2002, however the report, entitled "Director of Central Intelligence Report on the National Virtual Translation Center: A Concept Plan to Enhance the Intelligence Community's Foreign Language Capabilities, April 29, 2002" was received more than two months late, which the [Senate Select Committee on Intelligence](#) reported was "a delay which, in addition to contravening the explicit words of the statute, deprived the Committee of timely and valuable input into its efforts to craft this legislation."<sup>[139]</sup> Another report was commissioned on the feasibility and desirability of reconfiguring the Foreign Terrorist Asset Tracking Center and the [Office of Foreign Assets Control](#) of the [Department of the Treasury](#).<sup>[140]</sup> It was due by February 1, 2002 however, it was never written. The Senate Select Committee on Intelligence later complained that "[t]he Director of Central Intelligence and the Secretary of the Treasury failed to provide a report, this time in direct contravention of a section of the USA PATRIOT Act" and they further directed "that the statutorily-

directed report be completed immediately, and that it should include a section describing the circumstances which led to the Director's failure to comply with lawful reporting requirements."<sup>[141]</sup>

Other measures allowed certain reports on intelligence and intelligence-related matters to be deferred until either February 1, 2002 or a date after February 1, 2002 if the official involved certified that preparation and submission on February 1, 2002, would impede the work of officers or employees engaged in counterterrorism activities. Any such deferral required congressional notification before it was authorized.<sup>[142]</sup> The Attorney General was charged with training officials in identifying and utilizing foreign intelligence information properly in the course of their duties. The government officials include those in the Federal Government who do not normally encounter or disseminate foreign intelligence in the performance of their duties, and State and local government officials who encounter, or potentially may encounter in the course of a terrorist event, foreign intelligence in the performance of their duties.<sup>[143]</sup> A sense of Congress was expressed that officers and employees of the intelligence community should be encouraged to make every effort to establish and maintain intelligence relationships with any person, entity, or group while they conduct lawful intelligence activities.<sup>[137]</sup>

## **Title X: Miscellaneous** [\[edit\]](#)

*Main article: [Patriot Act, Title X](#)*


Title X created or altered a number of miscellaneous laws that did not really fit into the any other section of the USA PATRIOT Act. [Hazmat](#) licenses were limited to drivers who pass background checks and who can demonstrate they can handle the materials.<sup>[144]</sup> The [Inspector General of the Department of Justice](#) was directed to appoint an official to monitor, review and report back to Congress all allegations of civil rights abuses against the DoJ.<sup>[145]</sup> It amended the definition of "electronic surveillance" to exclude the interception of communications done through or from a protected computer where the owner allows the interception, or is lawfully involved in an

investigation.<sup>[146]</sup> Money laundering cases may now be brought in the district the money laundering was committed or where a money laundering transfer started from.<sup>[147]</sup> Aliens who committed money laundering were also prohibited from entering the U.S.<sup>[148]</sup> Grants were provided to [first responders](#) to assist them with responding to and preventing terrorism.<sup>[149]</sup> US\$5,000,000 was authorized to be provided to the [Drug Enforcement Administration](#) (DEA) to train police in [South](#) and [East Asia](#).<sup>[150]</sup> The Attorney General was directed to commission a study on the feasibility of using [biometric](#) identifiers to identify people as they attempt to enter the United States, and which would be connected to the FBI's database to flag suspected criminals.<sup>[151]</sup> Another study was also commissioned to determine the feasibility of providing [airlines](#) names of suspected terrorists before they boarded flights.<sup>[152]</sup> The Department of Defense was given temporary authority to use their funding for private contracts for security purposes.<sup>[153]</sup> The last title also created a new Act called the *Crimes Against Charitable Americans Act*<sup>[154]</sup> which amended the *Telemarketing and Consumer Fraud and Abuse Prevention Act* to require [telemarketers](#) who call on behalf of [charities](#) to disclose the purpose and other information, including the name and mailing address of the charity the telemarketer is representing.<sup>[155]</sup> It also increased the penalties from one year imprisonment to five years imprisonment for those committing fraud by impersonating a [Red Cross](#) member.<sup>[156]</sup>

## Section expirations [\[edit\]](#)

Status	Section	Title	Expiration date
✓	<a href="#">PA 201</a>	Authority to intercept wire, oral, and electronic communications relating to terrorism	<del>2006-03-10</del>
✓	<a href="#">PA 202</a>	Authority to intercept wire, oral, and electronic	<del>2006-03-</del>

		communications relating to computer fraud and abuse offenses	<del>10</del>
✓	<a href="#">PA 203(b)</a>	Authority to share electronic, wire and oral interception information	<del>2006-03-10</del>
✓	<a href="#">PA 204</a>	Clarification of intelligence exceptions from limitations on interception and disclosure of wire, oral, and electronic communications	<del>2006-03-10</del>
✓	<a href="#">PA 206</a> <a href="#">50 USC 1805(c)(2)(B)</a> 	Roving surveillance authority under the Foreign Intelligence Surveillance Act of 1978.	2019-12-15
✓	<a href="#">PA 207</a>	Duration of FISA surveillance of non-United States persons who are agents of a foreign power	<del>2006-03-10</del>
✓	<a href="#">PA 209</a>	Seizure of <a href="#">voice-mail</a> messages pursuant to warrants	<del>2006-03-10</del>
✓	<a href="#">PA 212</a>	Emergency disclosure of electronic communications to protect life and limb	<del>2006-03-10</del>
✓	<a href="#">PA 214</a>	Pen register and trap and trace authority under FISA	<del>2006-03-10</del>
	<a href="#">PA 215</a> <a href="#">50 USC 1861</a> 	Access to records and other items under the Foreign Intelligence Surveillance Act.	<del>2015-06-01</del>
✓	<a href="#">PA 217</a>	Interception of computer trespasser communications	<del>2006-03-10</del>
✓	<a href="#">PA 218</a>	Foreign intelligence information	<del>2006-03-</del>

			<del>10</del>
✓	<a href="#">PA 220</a>	Nationwide service of search warrants for electronic evidence	<del>2006-03-10</del>
✓	<a href="#">PA 223</a>	Civil liability for certain unauthorized disclosures	<del>2006-03-10</del>
✓	<a href="#">PA 225</a>	Immunity for compliance with FISA wiretap	<del>2006-03-10</del>
✓	<a href="#">IRTPA 6001</a> <a href="#">50 USC</a> <a href="#">1801(b)(1)(C)</a> 	"Lone wolf" provision	2019-12-15

## Controversy [\[edit\]](#)

See also: *[Controversial invocations of the Patriot Act](#)*

The USA PATRIOT Act has generated a great deal of controversy since its enactment.

Opponents of the Act have been quite vocal in asserting that it was passed opportunistically after the [September 11 attacks](#), believing that there would have been little debate. They view the Act as one that was hurried through the Senate with little change before it was passed. (Senators [Patrick Leahy](#) and [Russ Feingold](#) proposed amendments to modify the final revision.)<sup>[157][158][159]</sup>

The sheer magnitude of the Act itself was noted by [Michael Moore](#) in his controversial film *[Fahrenheit 9/11](#)*. In one of the scenes of the movie, he records Congressman [Jim McDermott](#) alleging that no Senator had read the bill<sup>[160]</sup> and John Conyers, Jr. as saying, "We don't read most of the bills. Do you really know what that would entail if we read every bill that we passed?" Congressman Conyers then answers his own rhetorical question, asserting that if they did it would

"slow down the legislative process".<sup>[161]</sup> As a [dramatic device](#), Moore then hired an [ice-cream van](#) and drove around Washington, D.C. with a loud speaker, reading out the Act to puzzled passers-by, which included a few Senators.<sup>[162]</sup>

However, Moore was not the only commentator to notice that not many people had read the Act. When [Dahlia Lithwick](#) and Julia Turne for [Slate](#) asked, "How bad is PATRIOT, anyway?", they decided that it was "hard to tell" and stated:

The [ACLU](#), in a new fact sheet challenging the [DOJ](#) Web site, wants you to believe that the act threatens our most basic civil liberties. Ashcroft and his roadies call the changes in law "modest and incremental." Since almost nobody has read the legislation, much of what we think we know about it comes third-hand and spun. Both advocates and opponents are guilty of fear-mongering and distortion in some instances.<sup>[163]</sup>

One prime example of a controversy of the Patriot Act is shown in the case of [Susan Lindauer](#).

Another is the recent court case [United States v. Antoine Jones](#). A nightclub owner was linked to a drug trafficking stash house via a law enforcement GPS tracking device attached to his car. It was placed there without a warrant, which caused a serious conviction obstacle for federal prosecutors in court. Through the years the case rose all the way to the United States Supreme Court where the conviction was overturned in favor of the defendant. The court found that increased monitoring of suspects caused by such legislation like the Patriot Act directly put the suspects' Constitutional rights in jeopardy.

The [Electronic Privacy Information Center](#) (EPIC) has criticized the law as unconstitutional, especially when "the private communications of law-abiding American citizens might be intercepted incidentally",<sup>[164]</sup> while the [Electronic Frontier Foundation](#) held that the lower standard applied to

wiretaps "gives the [FBI](#) a 'blank check' to violate the communications privacy of countless innocent Americans".<sup>[32]</sup> Others do not find the roving wiretap legislation to be as concerning. Professor [David D. Cole](#) of the [Georgetown University Law Center](#), a critic of many of the provisions of the Act, found that though they come at a cost to privacy are a sensible measure<sup>[165]</sup> while Paul Rosenzweig, a Senior Legal Research Fellow in the Center for Legal and Judicial Studies at [The Heritage Foundation](#), argues that roving wiretaps are just a response to rapidly changing communication technology that is not necessarily fixed to a specific location or device.<sup>[166]</sup>

The Act also allows access to voicemail through a search warrant rather than through a title III wiretap order.<sup>[167]</sup> James Dempsey, of the [CDT](#), believes that it unnecessarily overlooks the importance of notice under the [Fourth Amendment](#) and under a Title III wiretap,<sup>[168]</sup> and the EFF criticizes the provision's lack of notice. However, the EFF's criticism is more extensive—they believe that the amendment "is in possible violation of the Fourth Amendment to the U.S. Constitution" because previously if the FBI listened to voicemail illegally, it could not use the messages in evidence against the defendant.<sup>[169]</sup> Others disagree with these assessments. Professor [Orin Kerr](#), of the [George Washington University](#) school of law, believes that the [ECPA](#) "adopted a rather strange rule to regulate voicemail stored with service providers" because "under ECPA, if the government knew that there was one copy of an unopened private message in a person's bedroom and another copy on their remotely stored voicemail, it was illegal for the FBI to simply obtain the voicemail; the law actually compelled the police to invade the home and rifle through peoples' bedrooms so as not to disturb the more private voicemail." In Professor Kerr's opinion, this made little sense and the amendment that was made by the USA PATRIOT Act was reasonable and sensible.<sup>[170][171]</sup>

The USA PATRIOT Act's expansion of court jurisdiction to allow the nationwide service of search warrants proved controversial for the EFF.<sup>[172]</sup> They believe that agencies will be able to "'shop' for judges that have demonstrated a strong bias toward law enforcement with regard to search



warrants, using only those judges least likely to say no—even if the warrant doesn't satisfy the strict requirements of the Fourth Amendment to the Constitution",<sup>[173]</sup> and that it reduces the likelihood that smaller ISPs or phone companies will try to protect the privacy of their clients by challenging the warrant in court—their reasoning is that "a small San Francisco ISP served with such a warrant is unlikely to have the resources to appear before the New York court that issued it."<sup>[173]</sup> They believe that this is bad because only the communications provider will be able to challenge the warrant as only they will know about it—many warrants are issued *ex parte*, which means that the target of the order is not present when the order is issued.<sup>[173]</sup>

For a time, the USA PATRIOT Act allowed for agents to undertake "sneak and peek" searches.<sup>[27]</sup> Critics such as EPIC and the ACLU strongly criticized the law for violating the Fourth Amendment,<sup>[174]</sup> with the ACLU going so far as to release an advertisement condemning it and calling for it to be repealed.<sup>[175][176]</sup>

However supporters of the amendment, such as Heather Mac Donald, a fellow at the Manhattan Institute and contributing editor to the *New York City Journal*, expressed the belief that it was necessary because the temporary delay in notification of a search order stops terrorists from tipping off counterparts who are being investigated.<sup>[177]</sup>

In 2004, FBI agents used this provision to search and secretly examine the home of Brandon Mayfield, who was wrongfully jailed for two weeks on suspicion of involvement in the Madrid train bombings. While the U.S. Government did publicly apologize to Mayfield and his family,<sup>[178]</sup> Mayfield took it further through the courts. On September 26, 2007, Judge Ann Aiken found the law was, in fact, unconstitutional as the search was an unreasonable imposition on Mayfield and thus violated the Fourth Amendment.<sup>[28][29]</sup>

Laws governing the material support of terrorism proved contentious. It was criticized by the EFF for infringement of freedom of association. The EFF argues that had this law been enacted during

[Apartheid](#), U.S. citizens would not have been able to support the [African National Congress](#) (ANC) as the EFF believe the ANC would have been classed as a terrorist organization. They also used the example of a humanitarian social worker being unable to train [Hammas](#) members how to care for civilian children orphaned in the conflict between Israelis and Palestinians, a lawyer being unable to teach [IRA](#) members about [international law](#), and peace workers being unable to offer training in effective peace negotiations or how to petition the [United Nations](#) regarding human rights abuses.<sup>[179]</sup>

Another group, the [Humanitarian Law Project](#), also objected to the provision prohibiting "expert advise and assistance" to terrorists and filed a suit against the U.S. government to have it declared unconstitutional. In 2004 a Federal District Court struck the provision down as unconstitutionally vague,<sup>[130]</sup> but in 2010 the Supreme Court reversed that decision.<sup>[131]</sup>

Perhaps one of the biggest controversies involved the use of [National Security Letters](#) (NSLs) by the FBI. Because they allow the FBI to search telephone, email, and financial records without a [court order](#), they were criticized by many parties, including the [American Civil Liberties Union](#). Although FBI officials have a series of internal "checks and balances" that must be met before the issue of an NSL, Federal Judge Victor Marrero ruled the NSL provisions unconstitutional.<sup>[180][181][182][183][184]</sup> In November 2005, [BusinessWeek](#) reported that the FBI had issued tens of thousands of NSLs and had obtained one million financial, credit, employment, and in some cases, health records from the customers of targeted [Las Vegas](#) businesses. Selected businesses included casinos, storage warehouses and car rental agencies. An anonymous Justice official claimed that such requests were permitted under section 505 of the USA PATRIOT Act and despite the volume of requests insisted "We are not inclined to ask courts to endorse fishing expeditions".<sup>[185]</sup> Before this was revealed, however, the ACLU challenged the constitutionality of NSLs in court. In April 2004, they filed suit against the government on behalf of an unknown [Internet Service Provider](#) who had been issued an NSL, for reasons unknown. In [ACLU v. DoJ](#), the

ACLU argued that the NSL violated the First and Fourth Amendments of the U.S. Constitution because the USA PATRIOT Act failed to spell out any legal process whereby a telephone or Internet company could try to oppose an NSL subpoena in court. The court agreed, and found that because the recipient of the subpoena could not challenge it in court it was unconstitutional.<sup>[110]</sup> Congress later tried to remedy this in a reauthorization Act, but because they did not remove the non-disclosure provision a Federal court again found NSLs to be unconstitutional because they prevented courts from engaging in meaningful judicial review.<sup>[181][186][187]</sup>

Another provision of the USA PATRIOT Act has caused a great deal of consternation among librarians. Section 215 allows the FBI to apply for an order to produce materials that assist in an investigation undertaken to protect against international terrorism or clandestine intelligence activities. Among the "tangible things" that could be targeted, it includes "books, records, papers, documents, and other items".<sup>[33]</sup>

Supporters of the provision point out that these records are held by third parties, and therefore are exempt from a citizen's reasonable expectations of privacy and also maintain that the FBI has not abused the provision.<sup>[188]</sup> As proof, then Attorney General John Ashcroft released information in 2003 that showed that section 215 orders had never been used.<sup>[189]</sup>

However, despite protestations to the contrary, the [American Library Association](#) strongly objected to the provision, believing that library records are fundamentally different from ordinary business records, and that the provision would have a chilling effect on free speech. The association became so concerned that they formed a resolution condemning the USA PATRIOT Act, and which urged members to defend free speech and protect patrons' privacy.<sup>[190]</sup>

They urged librarians to seek legal advice before complying with a search order and advised their members to only keeping records for as long as was legally needed.<sup>[191]</sup>

Consequently, reports started filtering in that librarians were shredding records to avoid having to

comply with such orders.<sup>[192][193][194]</sup>

In 2005, Library Connection, a nonprofit consortium of 27 libraries in Connecticut, known as the [Connecticut Four](#) worked with the ACLU to lift a gag order for library records, challenging the government's power under Section 505 to silence four citizens who wished to contribute to public debate on the PATRIOT Act. This case became known as [Doe v. Gonzales](#). In May 2006, the government finally gave up its legal battle to maintain the gag order. In a summary of the actions of the Connecticut Four and their challenge to the USA PATRIOT Act, Jones (2009: 223) notes: "Librarians need to understand their country's legal balance between the protection of freedom of expression and the protection of national security. Many librarians believe that the interests of national security, important as they are, have become an excuse for chilling the freedom to read."<sup>[195]</sup>

Another controversial aspect of the USA PATRIOT Act is the immigration provisions that allow for the indefinite detention of any alien who the Attorney General believes may cause a terrorist act.<sup>[93]</sup> Before the USA PATRIOT Act was passed, [Anita Ramasastry](#), an associate professor of law and a director of the Shidler Center for Law, Commerce, & Technology at the [University of Washington School of Law](#) in [Seattle, Washington](#), accused the Act of depriving basic rights for immigrants to America, including legal permanent residents. She warned that "Indefinite detention upon secret evidence—which the USA PATRIOT Act allows—sounds more like [Taliban](#) justice than ours. Our claim that we are attempting to build an international coalition against terrorism will be severely undermined if we pass legislation allowing even citizens of our allies to be incarcerated without basic U.S. guarantees of fairness and justice."<sup>[196]</sup> Many other parties have also been strongly critical of the provision. Russell Feingold, in a Senate floor statement, claimed that the provision "falls short of meeting even basic constitutional standards of due process and fairness [as it] continues to allow the Attorney General to detain persons based on mere suspicion".<sup>[197]</sup> The [University of California](#) passed a resolution condemning (among other things) the indefinite

detention provisions of the Act,<sup>[198]</sup> while the ACLU has accused the Act of giving the Attorney General "unprecedented new power to determine the fate of immigrants ... Worse, if the foreigner does not have a country that will accept them, they can be detained indefinitely without trial."<sup>[199]</sup>

Another controversial aspect of the USA PATRIOT Act is its effect on the privacy of Canadians living in the province of [British Columbia](#) (B.C.). British Columbia's privacy commissioner raises concerns that the USA PATRIOT Act will allow the United States government to access Canadians' private information, such as personal medical records, that are outsourced to American companies. Although the government of B.C. has taken measures to prevent United States authorities from obtaining information, the widespread powers of the USA PATRIOT Act could overcome legislation that is passed in Canada.<sup>[200]</sup> B.C. Privacy Commissioner David Loukidelis stated in a report on the consequences of the USA PATRIOT Act, "once information is sent across borders, it's difficult, if not impossible, to control".<sup>[201]</sup>

In an effort to maintain their privacy, British Columbia placed amendments on the *Freedom of Information and Protection of Privacy Act* (FOIPPA), which was enacted as law on October 21, 2004. These amendments aim to place more firm limitations on "storing, accessing, and disclosing of B.C. public sector data by service providers."<sup>[202]</sup> These laws only pertain to public sector data and do not cover trans-border or private sector data in Canada. The public sector establishments include an estimated 2,000 "government ministries, hospitals, boards of health, universities and colleges, school boards, municipal governments and certain Crown corporations and agencies."<sup>[202]</sup> In response to these laws, many companies are now specifically opting to host their sensitive data outside the United States.<sup>[203]</sup>

Legal action has been taken in [Nova Scotia](#) to protect the province from the USA PATRIOT Act's data collecting methods. On November 15, 2007 the government of Nova Scotia passed a legislation aimed to protect Nova Scotians' personal information from being brought forward by the USA PATRIOT Act. The act was entitled "The new *Personal Information International Disclosure*

*Protection Act*". The goal of the act is to establish requirements to protect personal information from being revealed, as well as punishments for failing to do so. Justice Minister Murray Scott stated, "This legislation will help ensure that Nova Scotians' personal information will be protected. The act outlines the responsibilities of public bodies, municipalities and service providers and the consequences if these responsibilities are not fulfilled."<sup>[171][204]</sup> In the 1980s, the Bank of Nova Scotia was the center of an early, pre-Internet data-access case that led to the disclosure of banking records.<sup>[citation needed]</sup>

After suspected abuses of the USA PATRIOT Act were brought to light in June 2013 with articles about collection of American call records by the NSA and the PRISM program (see [2013 mass surveillance disclosures](#)), Representative [Jim Sensenbrenner](#), Republican of [Wisconsin](#), who introduced the Patriot Act in 2001, said that the National Security Agency overstepped its bounds.<sup>[205]</sup> He released a statement saying "While I believe the Patriot Act appropriately balanced national security concerns and civil rights, I have always worried about potential abuses." He added: "Seizing phone records of millions of innocent people is excessive and un-American."<sup>[205][206]</sup>

## Reauthorizations [\[edit\]](#)

---

The USA PATRIOT Act was reauthorized by three bills. The first, the *USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005*, was passed by both houses of Congress in July 2005. This bill reauthorized provisions of the *USA PATRIOT Act* and the *Intelligence Reform and Terrorism Prevention Act of 2004*. It created new provisions relating to the [death penalty](#) for terrorists,<sup>[207]</sup> enhancing security at [seaports](#),<sup>[208]</sup> new measures to combat the financing of terrorism,<sup>[209]</sup> new powers for the [Secret Service](#),<sup>[210]</sup> anti-[methamphetamine](#) initiatives<sup>[211]</sup> and a number of other miscellaneous provisions. The second reauthorization act, the *USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006*, amended the first and was passed in February

2006.

The first act reauthorized all but two of the provisions of Title II that would have expired. Two sections were changed to sunset on December 31, 2009: section 206—the roving wiretap provision—and section 215, which allowed access to business records under FISA. Section 215 was amended further regardless so as to give greater judicial oversight and review. Such orders were also restricted to be authorized by only the FBI Director, the FBI Deputy Director, or the Executive Assistant Director for National Security, and minimization procedures were specified to limit the dissemination and collection of such information. Section 215 also had a "gag" provision, which was changed to allow the defendant to contact their Attorney.<sup>[212]</sup> However, the change also meant that the defendant was also made to tell the FBI who he (or she) was disclosing the order to—this requirement was removed by the *USA PATRIOT Act Additional Reauthorizing Amendments Act*.<sup>[213]</sup>

On Saturday, February 27, 2010, President [Barack Obama](#) signed into law legislation that would temporarily extend, for one year, three controversial provisions of the Patriot Act that had been set to expire.<sup>[214] [215] [216]</sup>

- Authorize court-approved roving wiretaps that permit surveillance on multiple phones.
- Allow court-approved seizure of records and property in anti-terrorism operations.
- Permit surveillance against a so-called lone wolf, a non-U.S. citizen engaged in terrorism who may not be part of a recognized terrorist group.<sup>[217]</sup>

In a vote on February 8, 2011, the House of Representatives considered a further extension of the Act through the end of 2011.<sup>[218]</sup> House leadership moved the extension bill under suspension of the rules, which is intended for noncontroversial legislation and requires two-thirds majority to pass.<sup>[218]</sup> After the vote, the extension bill did not pass; 277 members voted in favor, which was less than the 290 votes needed to pass the bill under suspension of the rules.<sup>[218]</sup> Without an

extension, the Act was set to expire on February 28, 2011. However, it eventually passed, 275-144.<sup>[219]</sup> The [FISA Sunsets Extension Act of 2011](#) was signed into law February 25, 2011.

On May 26, 2011, [President Barack Obama](#) used an [Autopen](#) to sign the PATRIOT Sunsets Extension Act of 2011, a four-year extension of three key provisions in the USA PATRIOT Act while he was in France:<sup>[3]</sup> [roving wiretaps](#), searches of business records (the "[library records provision](#)"), and conducting surveillance of "lone wolves"—individuals suspected of terrorist-related activities not linked to terrorist groups.<sup>[4]</sup> Republican leaders<sup>[220]</sup> questioned if the use of the Autopen met the constitutional requirements for signing a bill into law.<sup>[221]</sup>

As NSL provisions of the USA PATRIOT Act had been struck by the courts<sup>[110]</sup> the reauthorization Act amended the law in an attempt to make them lawful. It provided for judicial review and the legal right of a recipient to challenge the validity of the letter. The reauthorization act still allowed NSLs to be closed and all evidence to be presented *in camera* and *ex parte*.<sup>[222]</sup> Gag provisions were maintained, but were not automatic. They only occurred when the Deputy Assistant Director of the FBI or a Special Agent in Charge in a Bureau field office certified that disclosure would result in "a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person".<sup>[223]</sup> However, should there be no non-disclosure order, the defendant can disclose the fact of the NSL to anyone who can render them assistance in carrying out the letter, or to an attorney for legal advice. Again, however, the recipient was ordered to inform the FBI of such a disclosure.<sup>[223]</sup> Because of the concern over the chilling effects of such a requirement, the *Additional Reauthorization Amendments Act* removed the requirement to inform the FBI that the recipient spoke about the NSL to their Attorney.<sup>[224]</sup> Later, the *Additional Reauthorization Amendments Act* excluded libraries from receiving NSLs, except where they provide electronic communications services.<sup>[225]</sup> The reauthorization Act also ordered the Attorney General submit a report semi-annually to the House and Senate Judiciary Committees, the House



and Senate Intelligence Committees and the [House Committee on Financial Services](#) and the [Senate Committee on Banking, Housing, and Urban Affairs](#) on all NSL request made under the *Fair Credit Reporting Act*.<sup>[226]</sup>

Changes were made to the roving wiretap provisions of the USA PATRIOT Act. Applications and orders for such wiretaps must describe the specific target of the electronic surveillance if the identity of the target is not known. If the nature and location of each of the facilities or places targeted for surveillance is not known, then after 10 days the agency must provide notice to the court. The notice must include the nature and location of each new facility or place at which the electronic surveillance was directed. It must also describe the facts and circumstances relied upon by the applicant to justify the applicant's belief that each new surveillance place or facility under surveillance is or was being used by the target of the surveillance. The applicant must also provide a statement detailing any proposed minimization procedures that differ from those contained in the original application or order, that may be necessitated by a change in the facility or place at which the electronic surveillance is directed. Applicants must detail the total number of electronic surveillances that have been or are being conducted under the authority of the order.<sup>[227]</sup>

Section 213 of the USA PATRIOT Act was modified. Previously it stated that delayed notifications would be made to recipients of "sneak and peek" searches in a "reasonable period". This was seen as unreasonable, as it was undefined and could potentially be used indefinitely. Thus, the reauthorization act changed this to a period not exceeding 30 days after the date of the execution of the search warrant. Courts were given the opportunity to extend this period if they were provided good cause to do so. Section 213 states that delayed notifications could be issued if there is "reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result". This was criticized, particularly by the ACLU, for allowing potential abuse by law enforcement agencies<sup>[228]</sup> and was later amended to prevent a delayed notification "if the adverse results consist only of unduly delaying a trial."<sup>[229]</sup> In September 2007

an Oregon US District Court struck down the Sneak and Peak provisions of the USA PATRIOT ACT,<sup>[230]</sup> but in December 2009 the Ninth Circuit overturned this decision.<sup>[231]</sup>

The reauthorization act also legislates increased congressional oversight for emergency disclosures by communication providers undertaken under section 212 of the USA PATRIOT Act.<sup>[232]</sup> The duration of FISA surveillance and physical search orders were increased. Surveillance performed against "lone wolf terrorists" under section 207 of the USA PATRIOT Act were increased to 120 days for an initial order, while pen registers and trap and trace device extensions under FISA were increased from 90 days to a year. The reauthorization act also increased congressional oversight, requiring a semi-annual report into physical searches and the use of pen registers and trap and trace devices under FISA.<sup>[233]</sup> The "lone wolf terrorist" provision (Section 207) was a sunset provision that also was to have expired, however this was enhanced by the *Intelligence Reform and Terrorism Prevention Act of 2004*. The reauthorization act extended the expiration date to December 31, 2009.<sup>[234]</sup> The amendment to material support law done in the *Intelligence Reform and Terrorism Prevention Act*<sup>[132]</sup> was also made permanent.<sup>[235]</sup> The definition of terrorism was further expanded to include receiving military-type training from a foreign terrorist organization and **narcoterrorism**.<sup>[236]</sup> Other provisions of the reauthorization act was to merge the law outlawing train wrecking (18 U.S.C. § 992 [↗](#)) and the law outlawing attacks on mass transportation systems (18 U.S.C. § 1993 [↗](#)) into a new section of Title 18 of the U.S. Code (18 U.S.C. § 1992 [↗](#)) and also to criminalize the act of planning a terrorist attack against a mass transport system.<sup>[237][238]</sup> **Forfeiture law** was further changed and now assets within U.S. jurisdiction will be seized for illegally trafficking in nuclear, chemical, biological or radiological weapons technology or material, if such offense is punishable under foreign law by **death** or imprisonment for a term exceeding one year. Alternatively, this applies if similar punishment would be so punishable if committed within the U.S.<sup>[239]</sup> A sense of Congress was further expressed that victims of terrorism should be entitled to the forfeited assets of terrorists.<sup>[240]</sup>

## See also [edit]

---

- [Central Intelligence Agency](#)
- [Civil Contingencies Act 2004](#)
- [Combat Zones That See](#)
- [Data mining](#)
- [Domestic Security Enhancement Act of 2003](#)
- [Federal Bureau of Investigation](#)
- [Foreign Terrorist Organizations](#)
- [Guardian \(database\)](#)
- [Information Awareness Office](#)
- [Ohio Patriot Act](#)
- [Patriot Act II](#)
- [Reichstag Fire Decree](#)
- [USA Freedom Act](#)
- [Investigatory Powers Act 2016](#)



*Government of the United States portal*

## References [edit]

---

- <sup>^</sup> <sup>***a***</sup> <sup>***b***</sup> ["The White House: President George W. Bush"](#)<sup>[]</sup>. The White House. October 26, 2001. Retrieved January 25, 2016.
- <sup>^</sup> [Public Law Pub.L. 107–56](#)<sup>[]</sup>
- <sup>^</sup> <sup>***a***</sup> <sup>***b***</sup> ["Obama Signs Last-Minute Patriot Act Extension"](#)<sup>[]</sup>. Fox News. May 27, 2011. Retrieved May 27, 2011.
- <sup>^</sup> <sup>***a***</sup> <sup>***b***</sup> [Mascaro, Lisa \(May 27, 2011\). "Congress votes in time to extend key Patriot Act provisions"](#)<sup>[]</sup>. *Los Angeles Times*. Retrieved May 27, 2011.

5. ^ ["Parts Of Patriot Act Expire, Even As Senate Moves On Bill Limiting Surveillance"](#)
6. ^ [a b c](#) Erin Kelly (June 2, 2015). ["Senate approves USA Freedom Act"](#). USA Today. Retrieved June 3, 2015.
7. ^ ["Bill Summary & Status 107th Congress \(2001–2002\)H.R.3162 Major Congressional Actions"](#), thomas.loc.gov Retrieved August 11, 2012.
8. ^ ["FINAL VOTE RESULTS FOR ROLL CALL 398"](#), clerk.house.gov. Oct 24, 2001. Retrieved August 11, 2012.
9. ^ ["U.S. Senate Roll Call Votes 107th Congress - 1st Session"](#), www.senate.gov. Oct 25, 2001. Retrieved August 11, 2012.
10. ^ ["Safe Act Co-Sponsors say PATRIOT Act Conference Report Unacceptable"](#), Washington Times, November 5, 2005.
11. ^ 2001 *Congressional Record*, Vol. 147, Page [S9368](#) (September 11, 2001)
12. ^ USA PATRIOT Act (U.S. [H.R.](#) 3162, Public Law 107-56), Title X, Sec. 1002.
13. ^ USA PATRIOT Act (U.S. [H.R.](#) 3162, Public Law 107-56), Title II, Sec. 218.
14. ^ [Andrew C. McCarthy](#), ["Why Section 218 Should be Retained"](#). Retrieved January 23, 2006. *The Patriot Debates*.
15. ^ USA PATRIOT Act (U.S. [H.R.](#) 3162, Public Law 107-56), Title II, Sec. 214.
16. ^ USA PATRIOT Act (U.S. [H.R.](#) 3162, Public Law 107-56), Title II, Sec. 207.
17. ^ USA PATRIOT Act (U.S. [H.R.](#) 3162, Public Law 107-56), Title II, Sec. 203.
18. ^ [a b](#) USA PATRIOT Act (U.S. [H.R.](#) 3162, Public Law 107-56), Title II, Sec. 216.
19. ^ [Analysis of Specific USA PATRIOT Act Provisions: Pen Registers, the Internet and Carnivore](#), [Electronic Privacy Information Center](#). Accessed December 4, 2005.
20. ^ USA PATRIOT Act (U.S. [H.R.](#) 3162, Public Law 107-56), Title II, Sec. 219.
21. ^ USA PATRIOT Act (U.S. [H.R.](#) 3162, Public Law 107-56), Title II, Sec. 204 & 209.
22. ^ USA PATRIOT Act (U.S. [H.R.](#) 3162, Public Law 107-56), Title II, Sec. 217.
23. ^ USA PATRIOT Act (U.S. [H.R.](#) 3162, Public Law 107-56), Title II, Sec. 211.
24. ^ USA PATRIOT Act (U.S. [H.R.](#) 3162, Public Law 107-56), Title II, Sec. 210.

25. ^ [USA PATRIOT Act \(U.S. H.R. 3162, Public Law 107-56\), Title II, Sec. 212.](#)
26. ^ [Field Guidance on New Authorities \(Redacted\)](#) , [Federal Bureau of Investigation](#) (hosted by the [Electronic Privacy Information Center](#)). Retrieved September 24, 2007.
27. ^ [a b](#) [USA PATRIOT Act \(U.S. H.R. 3162, Public Law 107-56\), Title II, Sec. 213.](#)
28. ^ [a b](#) [Singel, Ryan \(September 26, 2007\). "Court Strikes Down 2 Key Patriot Act Provisions"](#) . [Wired](#).
29. ^ [a b](#) [Keller, Susan Jo \(September 27, 2007\). "Judge Rules Provisions in Patriot Act to Be Illegal"](#) . [New York Times](#).
30. ^ [United States Department of Justice, The USA PATRIOT Act: Preserving Life and Liberty](#) , pg. 2. Retrieved September 24, 2007. [Archived](#)  March 9, 2009, at the [Wayback Machine](#).
31. ^ [James Dempsey, "Why Section 206 Should be Modified"](#)  (undated), accessed January 7, 2006.
32. ^ [a b](#) ["Let the Sun Set on PATRIOT - Section 206"](#) . [Electronic Frontier Foundation](#). Archived from [the original](#)  on June 5, 2006. Retrieved December 21, 2011.
33. ^ [a b](#) [USA PATRIOT Act \(U.S. H.R. 3162, Public Law 107-56\), Title II, Sec. 215.](#)
34. ^ ["Phillips, Heather A., "Libraries and National Security Law: An Examination of the USA Patriot Act". Progressive Librarian, Vol. 25, Summer 2005". Papers.ssrn.com. SSRN 901266](#) .
35. ^ [American Library Association, Resolution on the USA PATRIOT Act and Libraries](#) , enacted June 29, 2005
36. ^ [Mac Donald, Heather \(Summer 2003\). "Straight Talk on Homeland Security"](#) . [City Journal](#).
37. ^ [USA PATRIOT Act \(U.S. H.R. 3162, Public Law 107-56\), Title II, Sec. 208.](#)
38. ^ [USA PATRIOT Act \(U.S. H.R. 3162, Public Law 107-56\), Title II, Sec. 221.](#)
39. ^ [USA PATRIOT Act \(U.S. H.R. 3162, Public Law 107-56\), Title II, Sec. 205.](#)
40. ^ [O'Harrow, Jr., Robert \(October 27, 2002\). "Six Weeks in Autumn"](#) . [The Washington Post](#). p. W06. Retrieved July 11, 2008.
41. ^ [USA PATRIOT Act \(U.S. H.R. 3162, Public Law 107-56\), Title II, Sec. 224.](#)
42. ^ [USA PATRIOT Act \(U.S. H.R. 3162, Public Law 107-56\), Title III, Subtitle A, Sec. 311.](#)
43. ^ [USA PATRIOT Act \(U.S. H.R. 3162, Public Law 107-56\), Title III, Subtitle A, Sec. 314.](#)

44. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title III, Subtitle A, Sec. 317.
45. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title III, Subtitle A, Sec. 312, 313, 319 & 325.
46. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title III, Subtitle A, Sec. 327.
47. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title III, Subtitle A, Sec. 313.
48. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title III, Subtitle A, Sec. 312.
49. ^ [a b](#) USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title III, Subtitle A, Sec. 319. Amended [31 U.S.C. § 5318\(k\)\(3\)\(C\)\(iii\)](#)
50. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title III, Subtitle A, Sec. 325.
51. ^ Amendment made to [18 U.S.C. § 1956\(c\)\(7\)\(B\)\(ii\)](#)—for some reason an extra parenthesis was inserted into [18 U.S.C. § 1956\(c\)\(7\)\(B\)\(iii\)](#), according to [Cornell University](#), this was probably mistakenly added by law makers
52. ^ Illegal export of controlled munitions is defined in the United States Munitions List, which is part of the [Arms Export Control Act](#) ([22 U.S.C. § 2778](#))
53. ^ See [18 U.S.C. § 922\(l\)](#) and [18 U.S.C. § 925\(d\)](#)
54. ^ Defined in 15 [CFR 730–774](#)
55. ^ [a b](#) USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title III, Subtitle A, Sec. 315.
56. ^ Defined in [18 U.S.C. § 541](#)
57. ^ Defined in [18 U.S.C. § 1030](#)
58. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title III, Subtitle A, Sec. 320. Amended [18 U.S.C. § 981\(A\)\(1\)\(B\)](#)
59. ^ [a b](#) USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title III, Subtitle A, Sec. 323. Amended [28 U.S.C. § 2467](#)
60. ^ Pursuant to [18 U.S.C. § 983\(j\)](#)
61. ^ [28 U.S.C. § 2467\(d\)\(3\)\(A\)](#)
62. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title III, Subtitle A, Sec. 328.
63. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title III, Subtitle A, Sec. 330.

64. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title III, Subtitle B, Sec. 356.
65. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title III, Subtitle B, Sec. 365.
66. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title III, Subtitle B, Sec. 359.
67. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title III, Subtitle B, Sec. 352, 354 & 365.
68. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title III, Subtitle B, Sec. 361.
69. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title III, Subtitle B, Sec. 362.
70. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title III, Subtitle B, Sec. 352.
71. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title III, Subtitle B, Sec. 354.
72. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title III, Subtitle B, Sec. 353.
73. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title III, Subtitle B, Sec. 364.
74. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title III, Subtitle B, Sec. 360.
75. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title III, Subtitle C, Sec. 371.
76. ^ So defined in [31 U.S.C. § 5313](#), [31 U.S.C. § 5316](#) and [31 U.S.C. § 5324](#)
77. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title III, Subtitle C, Sec. 372. Amended [31 U.S.C. § 5317\(c\)](#)
78. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title III, Subtitle C, Sec. 371. Amended [18 U.S.C. § 1960](#)
79. ^ ["The Patriot Act: Justice Department Claims Success"](#). National Public Radio. July 20, 2005.
80. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title III, Subtitle C, Sec. 374. Amended [18 U.S.C. § 1960](#)
81. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title III, Subtitle C, Sec. 376. Amended [18 U.S.C. § 1956\(c\)\(7\)\(D\)](#)
82. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title III, Subtitle C, Sec. 377.
83. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title IV, Subtitle A, Sec. 401.
84. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title IV, Subtitle A, Sec. 402.
85. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title IV, Subtitle A, Sec. 404. Amended the *Department of Justice Appropriations Act, 2001*.

86. <sup>^</sup> [USA PATRIOT Act](#) (U.S. [H.R. 3162](#), Public Law 107-56), Title IV, Subtitle A, Sec. 403. Amends [8 U.S.C. § 1105](#)
87. <sup>^ a b</sup> [USA PATRIOT Act](#) (U.S. [H.R. 3162](#), Public Law 107-56), Title IV, Sec. 403. Final regulations are specified in [22 C.F.R. 40.5](#)
88. <sup>^</sup> [USA PATRIOT Act](#) (U.S. [H.R. 3162](#), Public Law 107-56), Title IV, Subtitle A, Sec. 405.
89. <sup>^</sup> [National Institute of Standards and Technology](#), November 14, 2002. "Use of Technology Standards and Interoperable Databases With Machine-Readable, Tamper-Resistant Travel Documents"  (Appendix A)
90. <sup>^</sup> [NIST Image Group's Fingerprint Research](#), see the section "NIST Patriot Act Work" (accessed June 28, 2006)
91. <sup>^ a b c d</sup> [USA PATRIOT Act](#) (U.S. [H.R. 3162](#), Public Law 107-56), Title IV, Subtitle B, Sec. 411.
92. <sup>^</sup> As specified in section 140(d)(2) of the *Foreign Relations Authorization Act*, Fiscal Years 1988 and 1989; see [22 U.S.C. § 2656f\(d\)\(2\)](#)
93. <sup>^ a b c d e</sup> [USA PATRIOT Act](#) (U.S. [H.R. 3162](#), Public Law 107-56), Title IV, Subtitle B, Sec. 412. A new section was created by the Act—[8 U.S.C. § 1226a](#)
94. <sup>^</sup> [USA PATRIOT Act](#) (U.S. [H.R. 3162](#), Public Law 107-56), Title IV, Subtitle B, Sec. 414.
95. <sup>^</sup> [8 U.S.C. § 1372\(a\)](#)
96. <sup>^</sup> [USA PATRIOT Act](#) (U.S. [H.R. 3162](#), Public Law 107-56), Title IV, Subtitle B, Sec. 416.
97. <sup>^</sup> [USA PATRIOT Act](#) (U.S. [H.R. 3162](#), Public Law 107-56), Title IV, Subtitle B, Sec. 417.
98. <sup>^</sup> [USA PATRIOT Act](#) (U.S. [H.R. 3162](#), Public Law 107-56), Title IV, Subtitle B, Sec. 418.
99. <sup>^</sup> [USA PATRIOT Act](#) (U.S. [H.R. 3162](#), Public Law 107-56), Title IV, Subtitle C.
100. <sup>^</sup> Office of [Patrick Leahy](#), [USA PATRIOT Act Section-by-section analysis](#)  [Archived](#)  February 13, 2010, at the [Wayback Machine](#).
101. <sup>^</sup> [USA PATRIOT Act](#) (U.S. [H.R. 3162](#), Public Law 107-56), Title V, Sec 501.
102. <sup>^</sup> [USA PATRIOT Act](#) (U.S. [H.R. 3162](#), Public Law 107-56), Title V, Sec 502. Amended [22 U.S.C. § 2708\(b\)\(5\)](#)



103. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title V, Sec 502. Amended [22 U.S.C. § 2708\(b\)\(6\)](#) 
104. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title V, Sec 502. Amended [22 U.S.C. § 2708\(e\)\(1\)](#) 
105. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title V, Sec 503. Amended [42 U.S.C. § 14135a\(d\)\(2\)](#) 
106. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title V, Sec 504. Amended [50 U.S.C. § 1825](#) 
107. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title V, Sec 506.
108. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title V, Sec 507.
109. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title V, Sec 505. Amended [18 U.S.C. § 2709\(b\)](#) ; Section 1114(a)(5)(A) of the *Right to Financial Privacy Act of 1978* ([12 U.S.C. § 3414\(a\)\(5\)\(A\)](#) ) and Section 624 of the *Fair Credit Reporting Act* ([15 U.S.C. § 1681u](#) )
110. ^ [a b c](#) *Doe v. Ashcroft*, 334 F.Supp.2d 471 (S.D.N.Y. 2004) [source](#) 
111. ^ USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005 (U.S. [H.R. 3199](#), Public Law 109-177) Title I, Sec. 115 & 116
112. ^ [http://isp.yale.edu/sites/default/files/page-attachments/merrill\\_v\\_lynch\\_-\\_unredacted\\_decision\\_vacating\\_gag\\_order.pdf#page=32](http://isp.yale.edu/sites/default/files/page-attachments/merrill_v_lynch_-_unredacted_decision_vacating_gag_order.pdf#page=32) 
113. ^ [http://isp.yale.edu/sites/default/files/page-attachments/merrill\\_v\\_lynch\\_-\\_unredacted\\_decision\\_vacating\\_gag\\_order.pdf](http://isp.yale.edu/sites/default/files/page-attachments/merrill_v_lynch_-_unredacted_decision_vacating_gag_order.pdf) 
114. ^ [http://isp.yale.edu/sites/default/files/page-attachments/merrill\\_v\\_lynch\\_-\\_unredacted\\_attachment\\_to\\_2004\\_nsl.pdf](http://isp.yale.edu/sites/default/files/page-attachments/merrill_v_lynch_-_unredacted_attachment_to_2004_nsl.pdf) 
115. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title VI, Subtitle A, Sec. 611.
116. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title VI, Subtitle A, Sec. 614.
117. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title VI, Subtitle B, Sec. 621
118. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title VI, Subtitle B, Sec. 622.

119. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title VI, Subtitle B, Sec. 623. Amended [42 U.S.C. § 10603\(b\)\(1\)](#)
120. ^ [42 U.S.C. § 10603b](#)
121. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title VI, Subtitle B, Sec. 624.
122. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title VIII, Sec. 802.
123. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title VIII, Sec. 813. Amended [18 U.S.C. § 1961\(1\)](#)
124. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title VIII, Sec. 814. Amended [18 U.S.C. § 1030\(e\)](#)
125. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title VIII, Sec. 801.
126. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title VIII, Sec. 817.
127. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title VIII, Sec. 803. Created [18 U.S.C. § 2339](#)
128. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title VIII, Sec. 806. Amends [18 U.S.C. § 981](#)
129. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title VIII, Section 805(a)(2)(B).
130. ^ [a b Humanitarian Law Project et al. v. John Ashcroft](#) , *Findlaw*
131. ^ [a b Adam Liptak, Court Affirms Ban on Aiding Groups Tied to Terror](#) , [The New York Times](#), June 21, 2010.
132. ^ [a b Intelligence Reform and Terrorism Prevention Act](#) (U.S. [S. 2845](#), Public Law 108-458), Title VI, Subtitle F, Sec. 6603.
133. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title VIII, Sec. 814.
134. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title VIII, Sec. 816.
135. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title IX, Sec. 901.
136. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title IX, Sec. 905.
137. ^ [a b USA PATRIOT Act](#) (U.S. [H.R. 3162](#), Public Law 107-56), Title IX, Sec. 903.
138. ^ USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title IX, Sec. 906.








139. ^ [Senate Report 107-149](#) – "To authorize appropriations for Fiscal Year 2003 for Intelligence and Intelligence-related activities of the United States Government, the Community Management Account, and the Central Intelligence Agency Retirement Disability System, and for other purposes.", see the section "National Virtual Translation Center"
140. ^ USA PATRIOT Act (U.S. [H.R.](#) 3162, Public Law 107-56), Title IX, Sec. 907.
141. ^ [Senate Report 107-149](#) – "To authorize appropriations for Fiscal Year 2003 for Intelligence and Intelligence-related activities of the United States Government, the Community Management Account, and the Central Intelligence Agency Retirement Disability System, and for other purposes.", see the section "Foreign Terrorist Asset Tracking Center"
142. ^ USA PATRIOT Act (U.S. [H.R.](#) 3162, Public Law 107-56), Title IX, Sec. 904.
143. ^ USA PATRIOT Act (U.S. [H.R.](#) 3162, Public Law 107-56), Title IX, Sec. 908.
144. ^ USA PATRIOT Act (U.S. [H.R.](#) 3162, Public Law 107-56), Title X, Sec. 1012.
145. ^ USA PATRIOT Act (U.S. [H.R.](#) 3162, Public Law 107-56), Title X, Sec. 1001.
146. ^ USA PATRIOT Act (U.S. [H.R.](#) 3162, Public Law 107-56), Title X, Sec. 1003.
147. ^ USA PATRIOT Act (U.S. [H.R.](#) 3162, Public Law 107-56), Title X, Sec. 1004.
148. ^ USA PATRIOT Act (U.S. [H.R.](#) 3162, Public Law 107-56), Title X, Sec. 1006.
149. ^ USA PATRIOT Act (U.S. [H.R.](#) 3162, Public Law 107-56), Title X, Sec. 1005.
150. ^ USA PATRIOT Act (U.S. [H.R.](#) 3162, Public Law 107-56), Title X, Sec. 1007.
151. ^ USA PATRIOT Act (U.S. [H.R.](#) 3162, Public Law 107-56), Title X, Sec. 1008.
152. ^ USA PATRIOT Act (U.S. [H.R.](#) 3162, Public Law 107-56), Title X, Sec. 1009.
153. ^ USA PATRIOT Act (U.S. [H.R.](#) 3162, Public Law 107-56), Title X, Sec. 1010.
154. ^ USA PATRIOT Act (U.S. [H.R.](#) 3162, Public Law 107-56), Title X, Sec. 1011 (a).
155. ^ USA PATRIOT Act (U.S. [H.R.](#) 3162, Public Law 107-56), Title X, Sec. 1011 (b).
156. ^ USA PATRIOT Act (U.S. [H.R.](#) 3162, Public Law 107-56), Title X, Sec. 1011 (c).
157. ^ 2001 *Congressional Record*, Vol. 147, Page [S10991](#) (October 25, 2001)

158. ^ ["History of the Patriot Act"](#). [Electronic Privacy Information Center](#). Retrieved July 11, 2008. "Though the Act made significant amendments to over 15 important statutes, it was introduced with great haste and passed with little debate, and without a House, Senate, or conference report. As a result, it lacks background legislative history that often retrospectively provides necessary statutory interpretation."
159. ^ ["EFF Analysis Of The Provisions Of The USA PATRIOT Act That Relate To Online Activities"](#). [Electronic Frontiers Foundation](#). October 31, 2001. Retrieved October 12, 2007. "...it seems clear that the vast majority of the sections included were not carefully studied by Congress, nor was sufficient time taken to debate it or to hear testimony from experts outside of law enforcement in the fields where it makes major changes."
160. ^ [Michael Moore](#), *Fahrenheit 9/11* (documentary). Timestamp: 01:01:39–01:01:47.
161. ^ [Michael Moore](#), *Fahrenheit 9/11* (documentary). Timestamp: 01:02:02–01:02:15.
162. ^ [Michael Moore](#), *Fahrenheit 9/11* (documentary). Timestamp: 01:02:35–01:02:43.
163. ^ [Lithwick, Dahlia; Turner, Julia](#) (September 8, 2003). ["A Guide to the Patriot Act, Part 1"](#). *Jurisprudence*. [Slate](#).
164. ^ ["Analysis of Specific USA PATRIOT Act Provisions: Expanded Dissemination of Information Obtained in Criminal Investigations"](#). *Analysis*. [Electronic Privacy Information Center](#). Retrieved July 11, 2008.
165. ^ [Cole, David](#). ["The Patriot Act Violates Our Civil Liberties"](#). *Is the Patriot Act Unconstitutional?*. [Microsoft Encarta](#).
166. ^ [Rosenzweig, Paul](#). ["Terrorism is not just a crime"](#). *Patriot Debates*. [American Bar Association](#).
167. ^ [USA PATRIOT Act \(U.S. H.R. 3162, Public Law 107-56\)](#), Title II, Sec. 209.
168. ^ [James X. Dempsey](#), ["Why Sections 209, 212, and 220 Should be Modified"](#) (undated). Retrieved October 15, 2007.
169. ^ [EFF](#), ["Let the Sun Set on PATRIOT – Section 209: 'Seizure of VoiceMail Messages Pursuant to Warrants'"](#). Retrieved December 29, 2005.

170. <sup>^</sup> [Orin Kerr](#), "Why Sections 209, 212, and 220 Should be Modified"  (undated). Retrieved October 12, 2007.
171. <sup>^ a b</sup> One prime example of a controversy of the Patriot Act is shown in the recent court case [United States v. Antoine Jones](#). A nightclub owner was linked to a drug trafficking stash house via a law enforcement GPS tracking device attached to his car. It was placed there without a warrant, which caused a serious conviction obstacle for federal prosecutors in court. Through the years the case has risen to the United States Supreme Court where the conviction was overturned in favor of the defendant. The court found that increased monitoring of suspects caused by such legislation like the Patriot Act directly put the suspects Constitutional rights in jeopardy.
172. <sup>^</sup> USA PATRIOT Act (U.S. [H.R. 3162](#), Public Law 107-56), Title II, Sec. 220.
173. <sup>^ a b c</sup> [EFF](#), "Let the Sun Set on PATRIOT – Section 220: 'Nationwide Service of Search Warrants for Electronic Evidence'" . Retrieved October 12, 2007.
174. <sup>^</sup> [Analysis of Specific USA PATRIOT Act Provisions: Authority to Conduct Secret Searches \("Sneak and Peek"\)](#) , [Electronic Privacy Information Center](#). Accessed December 5, 2005.
175. <sup>^</sup> "Uncle Sam Asks: "What the hell is going on here?" in New ACLU Print and Radio Advertisements"  (Press release). [American Civil Liberties Union](#). September 10, 2003.
176. <sup>^</sup> "ACLU Ad On "Sneak-and-Peek" Searches: Overblown" . [FactCheck.org](#). September 21, 2004.
177. <sup>^</sup> [Heather Mac Donald](#) (undated), "Sneak-and-Peek in the Full Light of Day" . [American Bar Association](#). Retrieved October 12, 2007.
178. <sup>^</sup> "Apology Note from the United States Government" . [Washington Post](#). November 29, 2006.
179. <sup>^</sup> [EFF](#), "Let the Sun Set on PATRIOT – Section 201: 'Authority to Intercept Wire, Oral, and Electronic Communications Relating to Terrorism,' and Section 805, 'Material Support for Terrorism'" . Retrieved October 12, 2007.
180. <sup>^</sup> "National Security Letters" . [American Civil Liberties Union](#). September 2007. Archived from [the original](#)  on October 18, 2007. Retrieved October 13, 2007.

181. <sup>a</sup> <sup>b</sup> ["Federal Court Strikes Down National Security Letter Provision of Patriot Act"](#) (Press release). [American Civil Liberties Union](#). September 6, 2007. Archived from [the original](#) on November 6, 2007. "NEW YORK – A federal court today struck down the amended Patriot Act's National Security Letter (NSL) provision. The law has permitted the FBI to issue NSLs demanding private information about people within the United States without court approval, and to gag those who receive NSLs from discussing them. The court found that the gag power was unconstitutional and that because the statute prevented courts from engaging in meaningful judicial review of gags, it violated the First Amendment and the principle of separation of powers."
182. <sup>a</sup> ["Let the Sun Set on PATRIOT Section 505 – National Security Letters \(NSLs\)"](#). [Electronic Frontiers Foundation](#). Retrieved October 13, 2007.
183. <sup>a</sup> ["EPIC: National Security Letters \(NSLs\)"](#). [Electronic Privacy Information Center](#). Retrieved July 11, 2008.
184. <sup>a</sup> ["FBI Unbound: How National Security Letters Violate Our Privacy"](#). [Bill of Rights Defense Committee](#). Retrieved July 11, 2008.
185. <sup>a</sup> Dunham, Richard S. (November 10, 2005). ["The Patriot Act: Business Balks"](#). [BusinessWeek](#). Retrieved July 11, 2008.
186. <sup>a</sup> Eggen, Dan (September 7, 2007). ["Judge Invalidates Patriot Act Provisions"](#). [Washington Post](#). p. A01.
187. <sup>a</sup> Neumeister, Larry (September 7, 2007). ["Judge Strikes Down Part of Patriot Act"](#). [London: Guardian](#). Archived from [the original](#) on January 27, 2008.
188. <sup>a</sup> C. McCarthy, Andrew. ["Why Sections 214 and 215 Should be Retained"](#). [American Bar Association](#). Retrieved July 11, 2008.
189. <sup>a</sup> ["No Patriot Check Out At Libraries"](#). [CBS News](#). September 18, 2003.
190. <sup>a</sup> ["Resolution on the USA Patriot Act and Related Measures That Infringe on the Rights of Library Users"](#). [American Library Association](#). January 29, 2003. Retrieved July 11, 2008.
191. <sup>a</sup> Kasindorf, Martin (December 16, 2003). ["FBI's reading list worries librarians"](#). [USA Today](#). Retrieved July 11, 2008.

192. ^ [Murphy, Dean E. \(7 April 2003\). "Some Librarians Use Shredder to Show Opposition to New F.B.I. Powers"](#) . New York Times. Retrieved July 11, 2008.
193. ^ ["Libraries Rally Against USA Patriot Act"](#) . *Politics*. Fox News Channel. May 7, 2003. Retrieved July 11, 2008.
194. ^ [Graham, Judith \(April 3, 2003\). "Libraries warning patrons: Federal government may be spying on you."](#). Chicago Tribune.
195. ^ [Jones, Barbara M. 2009. "Librarians Shushed No More: The USA Patriot Act, the 'Connecticut Four,' and Professional Ethics."](#) Newsletter on Intellectual Freedom 58, no. 6: 195, 221–223.
196. ^ [Ramasastry, Anita \(October 5, 2001\). "Indefinite detention based on suspicion: How The Patriot Act Will Disrupt Many Lawful Immigrants' Lives"](#) . FindLaw. Retrieved July 11, 2008.
197. ^ [Feingold, Russell \(October 25, 2001\). "Statement Of U.S. Senator Russ Feingold On The Anti-Terrorism Bill From The Senate Floor"](#) . Retrieved July 11, 2008.
198. ^ ["Resolution Passed at the May 6, 2004 Special Meeting of the Berkeley Division of the Academic Senate"](#)  (PDF). University of California. Retrieved July 11, 2008.
199. ^ ["Surveillance Under the USA PATRIOT Act > Non surveillance provisions"](#) . American Civil Liberties Union. April 3, 2003. Retrieved July 11, 2008.
200. ^ ["Patriot Act will prevail over B.C. privacy legislation"](#) . October 29, 2004. Retrieved March 6, 2008.
201. ^ ["USA Patriot Act comes under fire in B.C. report"](#) . CBC News. October 30, 2004. Retrieved March 6, 2008.
202. ^ [<sup>a</sup> <sup>b</sup> "British Columbia Responds to USA Patriot Act with Tough New Rules on How Service Providers Manage Public Sector Data"](#) . November 11, 2004. Archived from [the original](#)  on May 6, 2006. Retrieved March 6, 2008.
203. ^ ["Hosting Sensitive Data? Canada May be the Answer"](#) . *Internet Industry Watch*. November 25, 2010. Retrieved December 7, 2010.
204. ^ ["Protection of Privacy Legislation Proclaimed"](#) . November 15, 2006. Retrieved March 6, 2008.
205. ^ [<sup>a</sup> <sup>b</sup> "President Obama's Dragnet"](#) . 6 June 2013. Retrieved June 7, 2013.

206. ^ ["Author of Patriot Act: FBI's FISA Order is Abuse of Patriot Act"](#) . 6 June 2013. Retrieved June 7, 2013.
207. ^ USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005 (U.S. [H.R.](#) 3199, Public Law 109-177), Title II ("Terrorist Death Penalty Enhancement")
208. ^ USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005 (U.S. [H.R.](#) 3199, Public Law 109-177), Title III ("Reducing Crime and Terrorism at America's Seaports")
209. ^ USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005 (U.S. [H.R.](#) 3199, Public Law 109-177), Title IV ("Combating Terrorism Financing")
210. ^ USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005 (U.S. [H.R.](#) 3199, Public Law 109-177) Title VI ("Secret Service")
211. ^ USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005 (U.S. [H.R.](#) 3199, Public Law 109-177), Title VII ("Combating Methamphetamine Epidemic Act of 2005")
212. ^ USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005 (U.S. [H.R.](#) 3199, Public Law 109-177), Title I, Sec. 106
213. ^ USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005 (U.S. [S.](#) 2271, Public Law 109-178), Sec. 3.
214. ^ The reauthorization of the Patriot Act Feb 2010  
<http://www.csmonitor.com/USA/Politics/2010/0301/Obama-signs-Patriot-Act-extension-without-reforms/> 
215. ^ Obama signs one year extension of Patriot Act <http://www.clevelandleader.com/node/13183> 
216. ^ Democratic Underground - Obama signs Patriot Act  
[http://www.democraticunderground.com/discuss/duboard.php?az=view\\_all&address=102x4287047](http://www.democraticunderground.com/discuss/duboard.php?az=view_all&address=102x4287047) 
217. ^ Sections of the Patriot act that will remain as of Feb 2010  
<http://www.foxnews.com/politics/2010/02/27/obama-signs-year-extension-patriot-act/> 
218. ^ [a](#) [b](#) [c](#) Breshahan, Jake; Cogan, Marin (February 8, 2011). "Rank-and-file take down Patriot Act in House" . *Politico*.
219. ^ ["actions"](#) . Thomas.loc.gov. Retrieved May 16, 2012.






220. ^ ["Letter to Obama"](#)  (PDF). CBS News. June 17, 2011. Retrieved November 4, 2012.
221. ^ ["Republicans protest Obama signing bill with autopen"](#) . USA Today. 2011-06-17.
222. ^ USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005 (U.S. [H.R.](#) 3199, Public Law 109-177), Title I, Sec. 115
223. ^ [a](#) [b](#) USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005 (U.S. [H.R.](#) 3199, Public Law 109-177), Title I, Sec. 116
224. ^ USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005 (U.S. [S.](#) 2271, Public Law 109-178), Sec. 4.
225. ^ USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005 (U.S. [S.](#) 2271, Public Law 109-178), Sec. 5.
226. ^ USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005 (U.S. [H.R.](#) 3199, Public Law 109-177), Title I, Sec. 118
227. ^ USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005 (U.S. [H.R.](#) 3199, Public Law 109-177), Title I, Sec. 108
228. ^ [American Civil Liberties Union, ACLU Letter to Congress Urging A "No" Vote On the USA PATRIOT Improvement and Reauthorization Act Conference Report](#)  (December 12, 2005), accessed on October 6, 2007.
229. ^ USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005 (U.S. [H.R.](#) 3199, Public Law 109-177), Title I, Sec. 114
230. ^ Singel, Ryan (September 26, 2007). ["Court Strikes Down 2 Key Patriot Act Provisions | Threat Level"](#) . Wired.com. Retrieved May 16, 2012.
231. ^ <http://www.ca9.uscourts.gov/datastore/opinions/2009/12/10/07-35865.pdf>  Full text of the Ninth Circuit's decision @ uscourts.gov
232. ^ USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005 (U.S. [H.R.](#) 3199, Public Law 109-177), Title I, Sec. 107
233. ^ USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005 (U.S. [H.R.](#) 3199, Public Law 109-177), Title I, Sec. 109

234. <sup>^</sup> [USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005](#) (U.S. [H.R.](#) 3199, Public Law 109-177), Title I, Sec. 105
  235. <sup>^</sup> [USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005](#) (U.S. [H.R.](#) 3199, Public Law 109-177), Title I, Sec. 104
  236. <sup>^</sup> [USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005](#) (U.S. [H.R.](#) 3199, Public Law 109-177), Title I, Sec. 112
  237. <sup>^</sup> Yeah, Brian T.; Doyle, Charles (December 21, 2006). "[USA PATRIOT Improvement and Reauthorization Act of 2005: A Legal Analysis](#)"  (PDF). [Congressional Research Service](#): 24. Retrieved July 11, 2008.
  238. <sup>^</sup> [USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005](#) (U.S. [H.R.](#) 3199, Public Law 109-177), Title I, Sec. 110
  239. <sup>^</sup> [USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005](#) (U.S. [H.R.](#) 3199, Public Law 109-177), Title I, Sec. 111.
  240. <sup>^</sup> [USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005](#) (U.S. [H.R.](#) 3199, Public Law 109-177), Title I, Sec. 127.
- "Warrentless GPS Tracking". [Supreme Court Databases 15.1](#) (2012): n.pag. [Galileo](#). Web. 2 May 2012.

## Further reading [\[edit\]](#)

---

### Law review articles [\[edit\]](#)

- [Chesney, Robert M. "The Sleeper Scenario: Terrorism Support Laws and the Demands of Prevention"](#) . *Harvard Journal on Legislation* (2005).
- [Gouvin, Eric J. \(2003\). "Bringing Out the Big Guns: The USA PATRIOT Act, Money Laundering and the War on Terrorism"](#) . *Baylor Law Review*. **55**: 955. Archived from the original  on September 7, 2004.

- Kerr, Orin. "Digital Evidence and the New Criminal Procedure" [↗](#). *Columbia Law Review* (2005).
- Lecours, Alain P. *USA Patriot Act, Extraterritorial Effects of the USA Patriot Act - Privacy Rights of Non-American Citizens* [↗](#)
- Mojuyé, Benjamin, "What Banks Need to Know About the PATRIOT Act", 124 *Banking L.J.* 258, 258 (2007).
- Slovo, Daniel J. "Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference" [↗](#). *Fordham Law Review* 74 (2005).
- Van Bergen, Jennifer. "In the Absence of Democracy: The Designation and Material Support Provisions of the Anti-Terrorism Laws". *Cardozo Pub. [?] Law Policy & Ethics Journal* 2 (2003): 107.
- Wong, Kam C. "Implementing the USA PATRIOT Act: A Case Study of the Student and Exchange Visitor Information System (SEVIS)". *Brigham Young University Education and Law Journal* 2 (2006).
- Wong, Kam C. "The making of the USA PATRIOT Act I: Legislative Process and Dynamics". *International Journal of the Sociology of Law* 34.3 (2006): 179–219.
- Wong, Kam C. "The making of the USA PATRIOT ACT II: Public Sentiments, Legislative Climate, Political Gamesmanship, Media Patriotism". *International Journal of the Sociology of Law* 34.2 (2006): 105–140.
- Wong, Kam C. "USA PATRIOT Act and a Policy of Alienation". *Michigan Journal of Minority Rights* 1 (2006): 1–44.
- Wong, Kam C. "USA PATRIOT Act: Some Unanswered Questions". *International Journal of the Sociology of Law* 43.1 (2006): 1–41.

## Books [\[edit\]](#)

- Brasch, Walter. *America's Unpatriotic Acts: The Federal Government's Violation of*

*Constitutional and Civil Rights*. Peter Lang Publishing, 2005. [ISBN 0-8204-7608-0](#) (A long list of civil rights abuse claims by the Bush Administration inside the United States and other countries.)

- Cole, Dave, and James X. Dempsey. *Terrorism and the Constitution: Sacrificing Civil Liberties in the Name of National Security*. 2nd ed. New York: W. W. Norton & Co., 2002. [ISBN 1-56584-782-2](#). (Full discussion of prior legislative history of the Act, going back more than ten years.)
- Harvey, Robert and H el ene Volat. *De l'exception   la r egle. USA PATRIOT Act "DE L'EXCEPTION   LA R EGLE : USA PATRIOT ACT" : Robert Harvey et H el ene Volat*. Paris: Lignes, 2006. 215 p.
- Herman, Susan N.. *Taking Liberties: The War on Terror and the Erosion of American Democracy*. Oxford University Press, 2011. [ISBN 978-0-19-978254-3](#).
- Mailman, Stanley, Jeralyn Merritt, Theresa M. B. Van Vliet, and Stephen Yale-Loehr. *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001: An Analysis*. Newark, NJ and San Francisco, CA: Matthew Bender & Co., Inc. (a member of the [LexisNexis](#) Group), 2002. (Rel.1-3/02 Pub. 1271) ("An expert analysis of the significant changes in the new USA Patriot Act of 2001 [which]...track[s] the legislation by section, explaining both the changes and their potential impact with respect to: enhanced surveillance procedures; money laundering and financial crimes; protecting the border; investigation of terrorism; information sharing among federal and state authorities; enhanced criminal laws and penalties for terrorism offenses, and more.")
- Michaels, C. William. *No Greater Threat: America Since September 11 and the Rise of the National Security State*. Algora Publishing, Completely Updated for 2005. [ISBN 0-87586-155-5](#). (Covers all ten titles of the USA PATRIOT Act; Includes review and analysis of: Homeland Security Act, "PATRIOT Act II," Intelligence Reform and Terrorism Prevention Act, Supreme Court decisions, "National Strategy" documents, 9-11 Commission recommendations, and

various ongoing developments nationally and internationally in the "war on terrorism.")

- [Phelan, James Clancy](#); PATRIOT ACT, Hachette, ISBN 978-0-7336-2283-0; 2007.
- Van Bergen, Jennifer. *The Twilight of Democracy: The Bush Plan for America*. Common Courage Press, 2004. ISBN 1-56751-292-5. (A constitutional analysis for the general public of the USA PATRIOT Act and other administrative measures, with the first half of the book spent on principles of democracy and constitutional law.)
- Wong, Kam C. *The Impact of USA Patriot Act on American Society: An Evidence Based Assessment* (N.Y.: Nova Press, 2007) (In print)
- Wong, Kam C. *The Making of USA Patriot Act: Legislation, Implementation, Impact* (Beijing: China Law Press, 2007) (In print)

## External links [\[edit\]](#)

- ["The USA PATRIOT Act"](#) [↗](#), the full text
- [H.R. 3199, Bill Summary and Status](#) [↗](#)



Wikisource has original text related to this article:  
**[USA PATRIOT Act](#)**

## Supportive views [\[edit\]](#)

- ["The USA PATRIOT Act: Preserving Life and Liberty"](#) [↗](#) by the Department of Justice
- [The Patriot Act and Related Provisions: The Heritage Foundation's Research](#) [↗](#)
- Lowry, Rich (August 28, 2003). "Patriot Hysteria: The Zacarias Moussaoui Protection Act" [↗](#). *National Review*. Archived from [the original](#) [↗](#) on August 29, 2003.
- [The Patriot Act, Reauthorized](#) [↗](#), JURIST

## Critical views [\[edit\]](#)

- [PATRIOT Games: Terrorism Law and Executive Power](#) [↗](#), JURIST
- [American Library Association's resolution on the PATRIOT Act](#) [↗](#)

- [Sneak and Peek Search Warrants](#)
- ["Analysis of the USA PATRIOT Act"](#). PEN American Center. Archived from the original on March 1, 2005.
- [League of Women Voters' Resources on the USA PATRIOT Act and Individual Liberties](#)

## Other [\[edit\]](#)

- [National Security and Freedom](#) A series of short readings exploring historical and current issues of national security from Constitutional Rights Foundation.
- [Patriot Act news and resources](#), JURIST
- [Phillips, Heather A., "Libraries and National Security Law: An Examination of the USA Patriot Act". Progressive Librarian, Vol. 25, Summer 2005](#)
- [More on Wikipedia and its PATRIOT Act overview](#); Volokh Conspiracy, Orin Kerr

V · T · E · <b>USA PATRIOT Act</b>	
<b>Titles</b> I – II – III – IV – V – VI – VII – VIII – IX – X	
<b>Statute</b>	<a href="#">History of the USA PATRIOT Act</a> ·
<b>Legislative and Judicial History</b>	<a href="#">Wiretap Statute</a> · <a href="#">Electronic Communications Privacy Act</a> · <a href="#">Computer Fraud and Abuse Act</a> · <a href="#">Foreign Intelligence Surveillance Act</a> · <a href="#">Family Educational Rights and Privacy Act</a> · <a href="#">Money Laundering Control Act</a> · <a href="#">Bank Secrecy Act</a> · <a href="#">Right to Financial Privacy Act</a> · <a href="#">Fair Credit Reporting Act</a> · <a href="#">Immigration and Nationality Act of 1952</a> · <a href="#">Victims of Crime Act of 1984</a> · <a href="#">Telemarketing and Consumer Fraud and Abuse Prevention Act</a> ·
<b>Acts modified</b>	<a href="#">George W. Bush</a> · <a href="#">John Ashcroft</a> · <a href="#">Alberto Gonzales</a> · <a href="#">Patrick Leahy</a> · <a href="#">Orrin Hatch</a> · <a href="#">Jon Kyl</a> · <a href="#">Dianne Feinstein</a> · <a href="#">Viet D. Dinh</a> · <a href="#">Joe Biden</a> ·

<b>People</b>	<a href="#">Michael Chertoff</a> · <a href="#">Barack Obama</a> · <a href="#">Eric Holder</a> · <a href="#">Jim Dempsey</a> · <a href="#">Chuck Schumer</a> · <a href="#">Lamar S. Smith</a> · <a href="#">Bob Graham</a> · <a href="#">Jay Rockefeller</a> · <a href="#">Arlen Specter</a> · <a href="#">Mike Oxley</a> · <a href="#">Dick Arme</a> y · <a href="#">Paul Sarbanes</a> · <a href="#">Trent Lott</a> · <a href="#">Tom Daschle</a> · <a href="#">Russ Feingold</a> · <a href="#">Ellen Huvelle</a> · <a href="#">Ron Paul</a> · <a href="#">Lisa Murkowski</a> · <a href="#">Ron Wyden</a> · <a href="#">Dennis Kucinich</a> · <a href="#">Larry Craig</a> · <a href="#">John E. Sununu</a> · <a href="#">Richard Durbin</a> · <a href="#">Bernie Sanders</a> · <a href="#">Jerrold Nadler</a> · <a href="#">John Conyers, Jr.</a> · <a href="#">Butch Otter</a> ·
<b>Government organizations</b>	<a href="#">Federal Bureau of Investigation</a> · <a href="#">Department of Justice</a> · <a href="#">Select Committee on Intelligence</a> · <a href="#">Department of the Treasury</a> · <a href="#">FinCEN</a> · <a href="#">National Crime Information Center</a> · <a href="#">Department of State</a> · <a href="#">National Institute of Standards and Technology</a> · <a href="#">Customs Service</a> · <a href="#">U.S. Immigration and Customs Enforcement</a> ·
<b>Non-government organizations</b>	<a href="#">American Civil Liberties Union</a> · <a href="#">American Library Association</a> · <a href="#">Center for Democracy and Technology</a> · <a href="#">Center for Public Integrity</a> · <a href="#">Electronic Frontier Foundation</a> · <a href="#">Electronic Privacy Information Center</a> · <a href="#">Humanitarian Law Project</a> ·

<b>Major U.S. Intelligence Reforms</b>	
<b>U.S. Legislation</b>	<a href="#">National Security Act of 1947</a> (1947) · <a href="#">Foreign Intelligence Surveillance Act</a> (1978) · <a href="#">National Intelligence Reorganization and Reform Act</a> (1978) · <a href="#">Patriot Act</a> (2001) · <a href="#">Intelligence Reform and Terrorism Prevention Act</a> (2004) · <a href="#">Protect America Act of 2007</a> ·
<b>U.S. Commissions</b>	<a href="#">The First Hoover Commission</a> · <a href="#">The Second Hoover Commission</a> (1953) · <a href="#">The Rockefeller Commission</a> (1975) · <a href="#">Aspen-Brown Commission</a> (1995) · <a href="#">U.S. Commission on National Security/21st Century</a> (2001) · <a href="#">Weapons of Mass Destruction Commission</a> (2005) ·
<b>U.S. Committees</b>	<a href="#">The Church Committee</a> (1976) · <a href="#">The Pike Committee</a> (1976) ·
<b>U.S. Executive Orders</b>	<a href="#">EO 11905</a> (Ford, 1976) · <a href="#">EO 12036</a> (Carter, 1978) · <a href="#">EO 12333</a> (Reagan, 1981) · <a href="#">EO 13355</a> (G.W. Bush, 2004) · <a href="#">EO 13470</a> (G.W. Bush, 2008) ·
<b>U.S. Investigations</b>	<a href="#">The Murphey Investigation</a> (1974) · <a href="#">Iran-Contra Investigation</a> (1987) ·

<b>U.S. Reports</b>	<ul style="list-style-type: none"> <li>Eberstadt Report (1947)</li> <li>The Dulles–Jackson–Correa Report (1949)</li> <li>The Doolittle Report (1954)</li> <li>The Bruce-Lovett Report (1956)</li> <li>The Taylor Report (1961)</li> <li>The Kirkpatrick Report (1961)</li> <li>The Schlesinger Report (1971)</li> <li>Clifford/Cline Proposals (1976)</li> <li>Boren-McCurdy Proposals (1992)</li> <li>IC21 (1996)</li> <li>9/11 Commission Report (2004)</li> </ul>
---------------------	--

V·T·E· **War on Terror**

War in Afghanistan · Iraq War · War in North-West Pakistan · Symbolism of terrorism ·

<b>Participants</b>	<b>Operational</b>	<ul style="list-style-type: none"> <li>ISAF</li> <li>Operation Enduring Freedom participants</li> <li>Afghanistan</li> <li>Northern Alliance</li> <li>Iraq (Iraqi Armed Forces)</li> <li>NATO</li> <li>Pakistan</li> <li>United Kingdom</li> <li>United States</li> <li>European Union</li> <li>Philippines</li> <li>Ethiopia</li> </ul>
	<b>Targets</b>	<ul style="list-style-type: none"> <li>al-Qaeda</li> <li>Osama bin Laden</li> <li>al-Qaeda in the Arabian Peninsula</li> <li>Abu Sayyaf</li> <li>Anwar al-Awlaki</li> <li>Al-Shabaab</li> <li>Harkat-ul-Jihad al-Islami</li> <li>Hizbul Mujahideen</li> <li>Islamic Courts Union</li> <li>Jaish-e-Mohammed</li> <li>Jemaah Islamiyah</li> <li>Lashkar-e-Taiba</li> <li>Taliban</li> <li>Islamic Movement of Uzbekistan</li> </ul>

<b>Conflicts</b>	<b>Operation Enduring Freedom</b>	<ul style="list-style-type: none"> <li>War in Afghanistan</li> <li>OEF – Philippines</li> <li>Georgia Train and Equip Program</li> <li>Georgia Sustainment and Stability</li> <li>OEF – Horn of Africa</li> <li>OEF – Trans Sahara</li> <li>Drone strikes in Pakistan</li> </ul>
	<b>Other</b>	<ul style="list-style-type: none"> <li>Operation Active Endeavour</li> <li>Insurgency in the Maghreb (2002–present)</li> <li>Insurgency in the North Caucasus</li> <li>Moro conflict in the Philippines</li> <li>Iraq War</li> <li>Iraqi insurgency</li> <li>Operation Linda Nchi</li> <li>Terrorism in Saudi Arabia</li> <li>War in North-West Pakistan</li> <li>War in Somalia (2006–09)</li> <li>2007 Lebanon conflict</li> <li>al-Qaeda insurgency in Yemen</li> </ul>

**See also**

- Abu Ghraib torture and prisoner abuse
- Axis of evil
- Black sites
- Bush Doctrine
- Clash of Civilizations
- Cold War
- Combatant Status Review Tribunal
- Criticism of the War on Terror
- Death of Osama bin Laden
- Enhanced interrogation techniques
- Torture Memos
- Extrajudicial prisoners
- Extraordinary rendition
- Guantanamo Bay detention camp
- Iranian Revolution
- Islamism
- Military Commissions Act of 2006
- Terrorist Surveillance Program
- Operation Noble Eagle



[Operation Eagle Assist](#) · [Pakistan's role](#) · [President's Surveillance Program](#) · [Protect America Act of 2007](#) · [September 11 attacks](#) · [Targeted killing](#) · [Targeted Killing in International Law](#) · [Targeted Killings: Law and Morality in an Asymmetrical World](#) · [Unitary executive theory](#) · [Unlawful combatant](#) · [USA PATRIOT Act](#) · [Withdrawal of U.S. troops from Afghanistan](#) · [CAGE](#) ·

 [Terrorism portal](#) ·  [War portal](#) ·

#### Authority control

[WorldCat Identities](#)  · [VIAF: 180875257](#)  · [LCCN: no2002012008](#)  · [GND: 4759646-6](#)   
· [SUDOC: 098746421](#)  · [BNF: cb14637868w](#)  (data)  ·

Categories: [Patriot Act](#) | [107th United States Congress](#) | [2001 in American politics](#) | [2001 in American law](#) | [Emergency laws](#) | [George W. Bush administration controversies](#) | [Political repression in the United States](#) | [Privacy law in the United States](#) | [Terrorism laws in the United States](#) | [United States federal criminal legislation](#) | [United States federal defense and national security legislation](#)

This page was last edited on 11 May 2017, at 22:24.

Text is available under the [Creative Commons Attribution-ShareAlike License](#); additional terms may apply. By using this site, you agree to the [Terms of Use](#) and [Privacy Policy](#). Wikipedia® is a registered trademark of the [Wikimedia Foundation, Inc.](#), a non-profit organization.

[Privacy policy](#) [About Wikipedia](#) [Disclaimers](#) [Contact Wikipedia](#) [Developers](#) [Cookie statement](#) [Mobile view](#)

