**USA PATRIOT Act**

From Wikipedia, the free encyclopedia

|  |
| --- |
| **USA PATRIOT Act** |
|  |
| **Full title** | Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 |
| **Acronym** | USA PATRIOT Act, also Patriot Act |
| **Enacted by the** | [107th United States Congress](http://en.wikipedia.org/wiki/107th_United_States_Congress) |
| **Citations** |
| **Public Law** | [107-56](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107) |
| [**Stat.**](http://en.wikipedia.org/wiki/United_States_Statutes_at_Large) | 115 Stat. 272 (2001) |
| **Codification** |
| **Act(s) amended** | [*Electronic Communications Privacy Act*](http://en.wikipedia.org/wiki/Electronic_Communications_Privacy_Act) – [*Computer Fraud and Abuse Act*](http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act) – [*Foreign Intelligence Surveillance Act*](http://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act) – [*Family Educational Rights and Privacy Act*](http://en.wikipedia.org/wiki/Family_Educational_Rights_and_Privacy_Act) – [*Money Laundering Control Act*](http://en.wikipedia.org/wiki/Money_Laundering_Control_Act) – [*Bank Secrecy Act*](http://en.wikipedia.org/wiki/Bank_Secrecy_Act) – [*Right to Financial Privacy Act*](http://en.wikipedia.org/wiki/Right_to_Financial_Privacy_Act) – [*Fair Credit Reporting Act*](http://en.wikipedia.org/wiki/Fair_Credit_Reporting_Act) – [*Immigration and Nationality Act*](http://en.wikipedia.org/wiki/Immigration_and_Nationality_Act_of_1952) – [*Victims of Crime Act of 1984*](http://en.wikipedia.org/wiki/Victims_of_Crime_Act_of_1984) – [*Telemarketing and Consumer Fraud and Abuse Prevention Act*](http://en.wikipedia.org/wiki/Telemarketing_and_Consumer_Fraud_and_Abuse_Prevention_Act) |
| **Title(s) amended** | [8](http://en.wikipedia.org/wiki/Title_8_of_the_United_States_Code), [12](http://en.wikipedia.org/wiki/Title_12_of_the_United_States_Code), [15](http://en.wikipedia.org/wiki/Title_15_of_the_United_States_Code), [18](http://en.wikipedia.org/wiki/Title_18_of_the_United_States_Code), [20](http://en.wikipedia.org/wiki/Title_20_of_the_United_States_Code), [31](http://en.wikipedia.org/wiki/Title_31_of_the_United_States_Code), [42](http://en.wikipedia.org/wiki/Title_42_of_the_United_States_Code), [47](http://en.wikipedia.org/wiki/Title_47_of_the_United_States_Code), [49](http://en.wikipedia.org/wiki/Title_49_of_the_United_States_Code), [50](http://en.wikipedia.org/wiki/Title_50_of_the_United_States_Code) |
| [**U.S.C.**](http://en.wikipedia.org/wiki/United_States_Code) **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 substantially amended** | 8 USC §1105, 8 USC §1182g, 8 USC §1189, 8 USC §1202, 12 USC §248, 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, 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, 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**](http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR03162:@@@X) |
| * **Introduced in the** [**House of Representatives**](http://en.wikipedia.org/wiki/United_States_House_of_Representatives) **as** H.R. 3162 **by** [Frank James Sensenbrenner, Jr.](http://en.wikipedia.org/wiki/Jim_Sensenbrenner) **on** October 23, 2001
* **Committee consideration by:** [United States House Committee on the Judiciary](http://en.wikipedia.org/wiki/United_States_House_Committee_on_the_Judiciary); [Permanent Select Committee on Intelligence](http://en.wikipedia.org/wiki/Permanent_Select_Committee_on_Intelligence); [Committee on Financial Services](http://en.wikipedia.org/wiki/Committee_on_Financial_Services); [Committee on International Relations](http://en.wikipedia.org/wiki/Committee_on_International_Relations); [Committee on Energy and Commerce](http://en.wikipedia.org/wiki/Committee_on_Energy_and_Commerce) (Subcommittee on Telecommunications and the Internet); [Committee on Education and the Workforce](http://en.wikipedia.org/wiki/Committee_on_Education_and_the_Workforce); [Committee on Transportation and Infrastructure](http://en.wikipedia.org/wiki/Committee_on_Transportation_and_Infrastructure); [Committee on Armed Services](http://en.wikipedia.org/wiki/Committee_on_Armed_Services)
* **Passed the** [**House**](http://en.wikipedia.org/wiki/United_States_House_of_Representatives) **on** October 24, 2001 ([Yeas: 357; Nays: 66](http://clerk.house.gov/cgi-bin/vote.asp?year=2001&rollnumber=398))
* **Passed the** [**Senate**](http://en.wikipedia.org/wiki/United_States_Senate) **on** October 25, 2001 ([Yeas: 98; Nays: 1](http://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=107&session=1&vote=00313))
* **Signed into law by President** [Bush](http://en.wikipedia.org/wiki/George_W._Bush) **on** October 26, 2001
 |
| **Major amendments** |
|  |
| **Relevant Supreme Court cases** |
| None |

The **USA PATRIOT Act** (commonly known as the "Patriot Act") is an [Act of the U.S. Congress](http://en.wikipedia.org/wiki/Act_of_Congress%22%20%5Co%20%22Act%20of%20Congress) and signed into law by [President George W. Bush](http://en.wikipedia.org/wiki/George_W._Bush%22%20%5Co%20%22George%20W.%20Bush) on October 26, 2001. The title of the Act is a contrived acronym, which stands for **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001**.

The Act dramatically reduced restrictions on law enforcement agencies' ability to search telephone, e-mail communications, medical, financial, and other records; eased restrictions on foreign intelligence gathering within the United States; expanded the [Secretary of the Treasury’s](http://en.wikipedia.org/wiki/United_States_Secretary_of_the_Treasury%22%20%5Co%20%22United%20States%20Secretary%20of%20the%20Treasury) authority to regulate financial transactions, particularly those involving foreign individuals and entities; and broadened the discretion of law enforcement and immigration authorities in detaining and deporting [immigrants](http://en.wikipedia.org/wiki/Immigration_in_the_United_States%22%20%5Co%20%22Immigration%20in%20the%20United%20States) suspected of terrorism-related acts. The act also expanded the definition of terrorism to include [domestic terrorism](http://en.wikipedia.org/wiki/Domestic_terrorism%22%20%5Co%20%22Domestic%20terrorism), thus enlarging the number of activities to which the USA PATRIOT Act’s expanded law enforcement powers could be applied.

The Act was passed by wide margins in both houses of [Congress](http://en.wikipedia.org/wiki/United_States_Congress%22%20%5Co%20%22United%20States%20Congress) and was supported by members of both the Republican and Democratic parties. Many of the act's provisions were to [sunset](http://en.wikipedia.org/wiki/Sunset_provision%22%20%5Co%20%22Sunset%20provision) beginning December 31, 2005, approximately 4 years after its passage. In the months preceding the sunset date, supporters of the act pushed to make its sunsetting 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. 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.

**Background**

See also: [History of the USA PATRIOT Act](http://en.wikipedia.org/wiki/History_of_the_USA_PATRIOT_Act%22%20%5Co%20%22History%20of%20the%20USA%20PATRIOT%20Act)

The PATRIOT Act has made a number of changes to [U.S. law](http://en.wikipedia.org/wiki/Law_of_the_United_States%22%20%5Co%20%22Law%20of%20the%20United%20States). Key acts changed were the *[Foreign Intelligence Surveillance Act of 1978](http://en.wikipedia.org/wiki/Foreign_Intelligence_Act%22%20%5Co%20%22Foreign%20Intelligence%20Act)* (FISA), the *[Electronic Communications Privacy Act of 1986](http://en.wikipedia.org/wiki/Electronic_Communications_Privacy_Act%22%20%5Co%20%22Electronic%20Communications%20Privacy%20Act)* (ECPA), the *[Money Laundering Control Act of 1986](http://en.wikipedia.org/wiki/Money_Laundering_Control_Act%22%20%5Co%20%22Money%20Laundering%20Control%20Act)* and *[Bank Secrecy Act](http://en.wikipedia.org/wiki/Bank_Secrecy_Act%22%20%5Co%20%22Bank%20Secrecy%20Act)* (BSA), as well as the *[Immigration and Nationality Act](http://en.wikipedia.org/wiki/Immigration_and_Nationality_Act_of_1952%22%20%5Co%20%22Immigration%20and%20Nationality%20Act%20of%201952)*. The Act itself came about after the [September 11 terrorist attacks](http://en.wikipedia.org/wiki/September_11_attacks%22%20%5Co%20%22September%2011%20attacks) on New York City and the Pentagon. After these attacks, Congress immediately started work on several proposed antiterrorist bills, before the Justice Department finally drafted a bill called the *Anti-Terrorism Act of 2001*. This was introduced to the House as the *Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act of 2001*, and was later passed by the House as the *Uniting and Strengthening America (USA) Act* (H.R. 2975) on October 12. It was then introduced into the Senate as the *USA Act of 2002* (S. 1510) where a number of amendments were proposed by Senator [Russ Feingold](http://en.wikipedia.org/wiki/Russ_Feingold), all of which were passed. The final bill, the *USA PATRIOT Act* was introduced into the House on October 23 and incorporated H.R. 2975, S. 1510 and many of the provisions of H.R. 3004 (the *Financial Anti-Terrorism Act*). It was vehemently opposed by only one Senator, [Russ Feingold](http://en.wikipedia.org/wiki/Russ_Feingold%22%20%5Co%20%22Russ%20Feingold), who was the only Senator to vote against the bill. Senator [Patrick Leahy](http://en.wikipedia.org/wiki/Patrick_Leahy%22%20%5Co%20%22Patrick%20Leahy) also expressed some concerns. However, many parts were seen as necessary by both detractors and supporters. The final Act included a number of sunsets which were to expire on December 31, 2005.

Due to its controversial nature, a number of bills were proposed to amend the USA PATRIOT Act. These included the *Protecting the Rights of Individuals Act*, the [*Benjamin Franklin True Patriot Act*](http://en.wikipedia.org/wiki/Benjamin_Franklin_True_Patriot_Act), and the [*Security and Freedom Ensured Act*](http://en.wikipedia.org/wiki/Security_and_Freedom_Ensured_Act) (SAFE), none of which passed. In late January 2003, the founder of the [Center for Public Integrity](http://en.wikipedia.org/wiki/Center_for_Public_Integrity%22%20%5Co%20%22Center%20for%20Public%20Integrity), Charles Lewis, published a leaked draft copy of an Administration proposal titled the [Domestic Security Enhancement Act of 2003](http://en.wikipedia.org/wiki/Domestic_Security_Enhancement_Act_of_2003%22%20%5Co%20%22Domestic%20Security%20Enhancement%20Act%20of%202003). This highly controversial document was quickly dubbed "PATRIOT II" or "Son of PATRIOT" by the media and organizations such as the [Electronic Frontier Foundation](http://en.wikipedia.org/wiki/Electronic_Frontier_Foundation). The draft, which was circulated to 10 divisions of the Department of Justice, proposed to make further extensive modifications to extend the USA PATRIOT Act. It was widely condemned, although the Department of Justice claimed that it was only a draft and contained no further proposals.

**Titles**

**Titles I and X: Miscellaneous provisions**

Main articles: [USA PATRIOT Act, Title I](http://en.wikipedia.org/wiki/USA_PATRIOT_Act%2C_Title_I%22%20%5Co%20%22USA%20PATRIOT%20Act%2C%20Title%20I) and [USA PATRIOT Act, Title X](http://en.wikipedia.org/wiki/USA_PATRIOT_Act%2C_Title_X%22%20%5Co%20%22USA%20PATRIOT%20Act%2C%20Title%20X)

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 FBI's Technical Support Center. The military was authorized to provide assistance in some situations that involve weapons of mass destruction when so requested by the [Attorney General](http://en.wikipedia.org/wiki/United_States_Attorney_General%22%20%5Co%20%22United%20States%20Attorney%20General). The National Electronic Crime Task Force was expanded, along with the [President](http://en.wikipedia.org/wiki/President_of_the_United_States%22%20%5Co%20%22President%20of%20the%20United%20States)'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](http://en.wikipedia.org/wiki/Tom_Harkin%22%20%5Co%20%22Tom%20Harkin) ([D](http://en.wikipedia.org/wiki/Democratic_Party_%28United_States%29)-[IA](http://en.wikipedia.org/wiki/Iowa%22%20%5Co%20%22Iowa)) in an amendment to the *Combatting Terrorism Act of 2001*, though in a different form. It originally included "the prayer of [Cardinal](http://en.wikipedia.org/wiki/Cardinal_%28Catholicism%29%22%20%5Co%20%22Cardinal%20%28Catholicism%29) [Theodore McCarrick](http://en.wikipedia.org/wiki/Theodore_Edgar_McCarrick), the [Archbishop of Washington](http://en.wikipedia.org/wiki/Roman_Catholic_Archdiocese_of_Washington%22%20%5Co%20%22Roman%20Catholic%20Archdiocese%20of%20Washington) in a [Mass](http://en.wikipedia.org/wiki/Mass_%28liturgy%29%22%20%5Co%20%22Mass%20%28liturgy%29) 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.](http://en.wikipedia.org/wiki/Washington%2C_D.C.%22%20%5Co%20%22Washington%2C%20D.C.), and [Pennsylvania](http://en.wikipedia.org/wiki/Pennsylvania%22%20%5Co%20%22Pennsylvania) 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.' Further condemnation of racial vilification and violence is also spelled out in Title X, where there was condemnation of such activities against [Sikh](http://en.wikipedia.org/wiki/Sikh%22%20%5Co%20%22Sikh) Americans, who were mistaken for Muslims after the September 11th terrorist attack.

Title X created or altered a number of miscellaneous laws that didn't really fit into the any other section of the USA PATRIOT Act. [Hazmat](http://en.wikipedia.org/wiki/Dangerous_goods%22%20%5Co%20%22Dangerous%20goods) licenses were limited to drivers who pass background checks and who can demonstrate they can handle the materials. The [Inspector General of the Department of Justice](http://en.wikipedia.org/wiki/United_States_Department_of_Justice_Office_of_the_Inspector_General%22%20%5Co%20%22United%20States%20Department%20of%20Justice%20Office%20of%20the%20Inspector%20General) was directed to appoint an official to monitor, review and report back to Congress all allegations of civil rights abuses against the DoJ. 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. Money laundering cases may now be brought in the district the money laundering was committed or where a money laundering transfer started from. Aliens who committed money laundering were also prohibited from entering the U.S. Grants were provided to [first responders](http://en.wikipedia.org/wiki/First_responder%22%20%5Co%20%22First%20responder) to assist them with responding to and preventing terrorism. US$5,000,000 was authorized to be provided to the [Drug Enforcement Administration](http://en.wikipedia.org/wiki/Drug_Enforcement_Administration%22%20%5Co%20%22Drug%20Enforcement%20Administration) (DEA) to train police in [South](http://en.wikipedia.org/wiki/South_Asia%22%20%5Co%20%22South%20Asia) and [East Asia](http://en.wikipedia.org/wiki/East_Asia). The Attorney General was directed to commission a study on the feasibility of using [biometric](http://en.wikipedia.org/wiki/Biometrics%22%20%5Co%20%22Biometrics) 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. Another study was also commissioned to determine the feasibility of providing [airlines](http://en.wikipedia.org/wiki/Airline%22%20%5Co%20%22Airline) names of suspected terrorists before they boarded flights. The Department of Defense was given temporary authority to use their funding for private contracts for security purposes. The last title also created a new Act called the *Crimes Against Charitable Americans Act* which amended the *Telemarketing and Consumer Fraud and Abuse Prevention Act* to require [telemarketers](http://en.wikipedia.org/wiki/Telemarketing%22%20%5Co%20%22Telemarketing) who call on behalf of [charities](http://en.wikipedia.org/wiki/Charitable_organization%22%20%5Co%20%22Charitable%20organization) to disclose the purpose and other information, including the name and mailing address of the charity the telemarketer is representing. It also increased the penalties from one year imprisonment to five years imprisonment for those committing fraud by impersonating a [Red Cross](http://en.wikipedia.org/wiki/International_Red_Cross_and_Red_Crescent_Movement) member.

**Title II: Surveillance procedures**

Main article: [USA PATRIOT Act, Title II](http://en.wikipedia.org/wiki/USA_PATRIOT_Act%2C_Title_II%22%20%5Co%20%22USA%20PATRIOT%20Act%2C%20Title%20II)

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. 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. 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. The title also expanded the duration of FISA physical search and surveillance orders, and gave authorities the ability to share information gathered before a federal grand jury with other agencies.

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](http://en.wikipedia.org/wiki/Packet_switched_network) — the [Electronic Privacy Information Center](http://en.wikipedia.org/wiki/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. The Act allowed any district court judge in the United States to issue such surveillance ordersand search warrants for terrorism investigations. 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.

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. The definition of a "protected computer" is defined in [18 U.S.C.](http://en.wikipedia.org/wiki/Title_18_of_the_United_States_Code%22%20%5Co%20%22Title%2018%20of%20the%20United%20States%20Code) [§ 1030(e)(2)](http://www.law.cornell.edu/uscode/18/1030.html) 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](http://en.wikipedia.org/wiki/Cable_television%22%20%5Co%20%22Cable%20television) 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](http://en.wikipedia.org/wiki/Pen_register%22%20%5Co%20%22Pen%20register) and [trap and trace](http://en.wikipedia.org/wiki/Trap_and_trace%22%20%5Co%20%22Trap%20and%20trace) devices (chapter 206) and stored communications (121), though it excluded the disclosure of cable subscriber viewing habits. [Subpoenas](http://en.wikipedia.org/wiki/Subpoena) issued to [Internet Service Providers](http://en.wikipedia.org/wiki/Internet_Service_Providers%22%20%5Co%20%22Internet%20Service%20Providers) 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](http://en.wikipedia.org/wiki/IP_address%22%20%5Co%20%22IP%20address)), payment method and bank account and credit card numbers. Communication providers are also allowed to disclose customer records or communications if they suspect there is a danger to "life and limb".

Title II established three very controversial provisions: ["sneak and peek"](http://en.wikipedia.org/wiki/Sneak_and_peek_warrant) warrants, [roving wiretaps](http://en.wikipedia.org/wiki/Roving_wiretap%22%20%5Co%20%22Roving%20wiretap) 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" — and it may be extended at the court's discretion. These sneak and peek provisions were struck down by judge [Ann Aiken](http://en.wikipedia.org/wiki/Ann_Aiken%22%20%5Co%20%22Ann%20Aiken) on September 26, 2007 after a [Portland](http://en.wikipedia.org/wiki/Portland%2C_Oregon%22%20%5Co%20%22Portland%2C%20Oregon) attorney, [Brandon Mayfield](http://en.wikipedia.org/wiki/Brandon_Mayfield%22%20%5Co%20%22Brandon%20Mayfield) 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.

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, while opponents see it as violating the particularity clause of the [Fourth Amendment](http://en.wikipedia.org/wiki/Fourth_Amendment_to_the_United_States_Constitution). 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." Though it was not targeted directly at libraries, the [American Library Association](http://en.wikipedia.org/wiki/American_Library_Association%22%20%5Co%20%22American%20Library%20Association) (ALA), in particular, opposed this provision. 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." However, the ALA's stance did not go without criticism. One prominent critic of the ALA's stance was the [Manhattan Institute](http://en.wikipedia.org/wiki/Manhattan_Institute%22%20%5Co%20%22Manhattan%20Institute)'s [Heather Mac Donald](http://en.wikipedia.org/wiki/Heather_Mac_Donald%22%20%5Co%20%22Heather%20Mac%20Donald), who argued in an article for the *[New York City Journal](http://en.wikipedia.org/wiki/City_Journal_%28New_York%29%22%20%5Co%20%22City%20Journal%20%28New%20York%29)* that "[t]he furor over section 215 is a case study in Patriot Act fear-mongering."

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](http://en.wikipedia.org/wiki/District_of_Columbia)), trade sanctions against [North Korea](http://en.wikipedia.org/wiki/North_Korea) and [Taliban](http://en.wikipedia.org/wiki/Taliban%22%20%5Co%20%22Taliban)-controlled [Afghanistan](http://en.wikipedia.org/wiki/Afghanistan%22%20%5Co%20%22Afghanistan) and the employment of [translators](http://en.wikipedia.org/wiki/Translation%22%20%5Co%20%22Translation) by the FBI.

At the insistence of Republican Representative [Richard Armey](http://en.wikipedia.org/wiki/Dick_Armey), the Act had a number of [sunset provisions](http://en.wikipedia.org/wiki/Sunset_provision%22%20%5Co%20%22Sunset%20provision) 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. The provisions that were to expire are below.

|  |
| --- |
| Title II sections that were to originally expire on December 31, 2005 |
| **Section** | **Section title** |
| 201 | Authority to intercept wire, oral, and electronic communications relating to terrorism |
| 202 | Authority to intercept wire, oral, and electronic communications relating to computer fraud and abuse offenses |
| 203(b) | Authority to share electronic, wire and oral interception information |
| 204 | Clarification of intelligence exceptions from limitations on interception and disclosure of wire, oral, and electronic communications |
| 206 | Roving surveillance authority under the Foreign Intelligence Surveillance Act of 1978. |
| 207 | Duration of FISA surveillance of non-United States persons who are agents of a foreign power |
| 209 | Seizure of voice-mail messages pursuant to warrants |
| 212 | Emergency disclosure of electronic communications to protect life and limb |
| 214 | Pen register and trap and trace authority under FISA |
| 215 | Access to records and other items under the Foreign Intelligence Surveillance Act. |
| 217 | Interception of computer trespasser communications |
| 218 | Foreign intelligence information |
| 220 | Nationwide service of search warrants for electronic evidence |
| 223 | Civil liability for certain unauthorized disclosures |
| 225 | Immunity for compliance with FISA wiretap |

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

Main article: [USA PATRIOT Act, Title III](http://en.wikipedia.org/wiki/USA_PATRIOT_Act%2C_Title_III%22%20%5Co%20%22USA%20PATRIOT%20Act%2C%20Title%20III)

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](http://en.wikipedia.org/wiki/Money_laundering%22%20%5Co%20%22Money%20laundering) and the financing of [terrorism](http://en.wikipedia.org/wiki/Terrorism%22%20%5Co%20%22Terrorism). It primarily amends portions of the *[Money Laundering Control Act of 1986](http://en.wikipedia.org/wiki/Money_Laundering_Control_Act_of_1986%22%20%5Co%20%22Money%20Laundering%20Control%20Act%20of%201986)* (MLCA) and the *[Bank Secrecy Act of 1970](http://en.wikipedia.org/wiki/Bank_Secrecy_Act_of_1970%22%20%5Co%20%22Bank%20Secrecy%20Act%20of%201970)* (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, such as the Hans Vierck case of 2001.

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](http://en.wikipedia.org/wiki/Beneficial_owner%22%20%5Co%20%22Beneficial%20owner) of bank accounts and those who are authorized to use or route funds through [payable-through accounts](http://en.wikipedia.org/wiki/Payable-through_account). The U.S. Treasury was charged with formulating regulations intended to foster information sharing between financial institutions to prevent money-laundering. 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. If money laundering was uncovered, the subtitle legislated for the [forfeiture of assets](http://en.wikipedia.org/wiki/Asset_forfeiture%22%20%5Co%20%22Asset%20forfeiture) of those suspected of doing the money laundering. 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](http://en.wikipedia.org/wiki/Bank_holding_company%22%20%5Co%20%22Bank%20holding%20company) and [banks](http://en.wikipedia.org/wiki/Bank%22%20%5Co%20%22Bank) 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.

Restrictions were placed on accounts and foreign banks. It prohibited [shell banks](http://en.wikipedia.org/wiki/Shell_bank%22%20%5Co%20%22Shell%20bank) 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. Financial institutions must now undertake steps to identify the owners of any privately owned bank outside the U.S. who have a [correspondent account](http://en.wikipedia.org/wiki/Correspondent_account%22%20%5Co%20%22Correspondent%20account) 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. Bank 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](http://en.wikipedia.org/wiki/Politician%22%20%5Co%20%22Politician) where there is reasonable suspicion of [corruption](http://en.wikipedia.org/wiki/Political_corruption%22%20%5Co%20%22Political%20corruption). Any deposits made from within the U.S. into foreign banks are now deemed to have been deposited into any [interbank account](http://en.wikipedia.org/wiki/Interbank_network%22%20%5Co%20%22Interbank%20network) the foreign bank may have in the U.S. Thus any [restraining order](http://en.wikipedia.org/wiki/Injunction%22%20%5Co%20%22Injunction), seizure warrant or [arrest warrant](http://en.wikipedia.org/wiki/Arrest_warrant%22%20%5Co%20%22Arrest%20warrant) 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. Restrictions were placed on the use of internal bank [concentration accounts](http://en.wikipedia.org/wiki/Concentration_account%22%20%5Co%20%22Concentration%20account) because such accounts do not provide an effective [audit trail](http://en.wikipedia.org/wiki/Audit_trail%22%20%5Co%20%22Audit%20trail) 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. 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. the bribery of public officials and fraudulent dealing with public funds; the smuggling or illegal export of controlled munition and the importation or bringing in of any firearm or ammunition not authorized by the U.S. Attorney General and the smuggling of any item controlled under the Export Administration Regulations. It also includes any offense where the U.S. would be obligated under a [mutual treaty](http://en.wikipedia.org/wiki/Mutual_treaty%22%20%5Co%20%22Mutual%20treaty) with a foreign nation to [extradite](http://en.wikipedia.org/wiki/Extradition%22%20%5Co%20%22Extradition) 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; [computer crime](http://en.wikipedia.org/wiki/Computer_crime); and any [felony](http://en.wikipedia.org/wiki/Felony) violation of the *[Foreign Agents Registration Act of 1938](http://en.wikipedia.org/wiki/Foreign_Agents_Registration_Act%22%20%5Co%20%22Foreign%20Agents%20Registration%20Act)*. 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. Foreign nations may now seek to have a forfeiture or judgment notification enforced by a district court of the United States. This is done through new legislation that specifies how the U.S. government may apply for a restraining order to preserve the availability of property which is subject to a foreign forfeiture or confiscation judgement. In taking into consideration such an application, emphasis is placed on the ability of a foreign court to follow [due process](http://en.wikipedia.org/wiki/Due_process). 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](http://en.wikipedia.org/wiki/Wire_transfer%22%20%5Co%20%22Wire%20transfer) 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. The Secretary was also ordered to encourage international cooperation in investigations of money laundering, financial crimes, and the finances of terrorist groups.

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 [$US](http://en.wikipedia.org/wiki/United_States_dollar%22%20%5Co%20%22United%20States%20dollar)10,000 for each day the account remains open after the 10 day limit has expired.

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](http://en.wikipedia.org/wiki/Suspicious_activity_report%22%20%5Co%20%22Suspicious%20activity%20report) to notify U.S. intelligence agencies. 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. 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](http://en.wikipedia.org/wiki/Informal_value_transfer_system%22%20%5Co%20%22Informal%20value%20transfer%20system) outside of the mainstream financial system — were included in the definition of a financial institution. 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. [FinCEN](http://en.wikipedia.org/wiki/Financial_Crimes_Enforcement_Network) was made a [bureau](http://en.wikipedia.org/wiki/Government_agency%22%20%5Co%20%22Government%20agency) of the [United States Department of Treasury](http://en.wikipedia.org/wiki/United_States_Department_of_Treasury%22%20%5Co%20%22United%20States%20Department%20of%20Treasury)and the creation of a secure [network](http://en.wikipedia.org/wiki/Computer_network%22%20%5Co%20%22Computer%20network) to be used by financial institutions to report suspicious transactions and to provide alerts of relevant suspicious activities was ordered. Along with these reporting requirements, a considerable number of provisions relate to the prevention and prosecution of money-laundering. Financial institutions were ordered to establish anti-money laundering programs and the BSA was amended to better define anti-money laundering strategy. Also increased were civil and criminal penalties for money laundering and the introduction of penalties for violations of [geographic targeting orders](http://en.wikipedia.org/wiki/Geographic_targeting_order) and certain record-keeping requirements. A number of other amendments to the BSA were made through subtitle B, including granting the [Board of Governors of the Federal Reserve System](http://en.wikipedia.org/wiki/Board_of_Governors_of_the_Federal_Reserve_System%22%20%5Co%20%22Board%20of%20Governors%20of%20the%20Federal%20Reserve%20System) 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. 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.

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. It also made the civil and criminal penalty violations of currency reporting cases be the forfeiture of all a defendant's property that was involved in the offense, and any property traceable to the defendant. The Act prohibits and penalizes those who run unlicensed money transmitting businesses. 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](http://en.wikipedia.org/wiki/Somalia) militant. 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. Money laundering "unlawful activities" was expanded to include the [provision of material support or resources to designated foreign terrorist organizations](http://en.wikipedia.org/wiki/Provision_of_material_support_or_resources_to_designated_foreign_terrorist_organizations%22%20%5Co%20%22Provision%20of%20material%20support%20or%20resources%20to%20designated%20foreign%20terrorist%20organizations). The Act specifies that anyone who commits or conspires to undertake a fraudulent activity [outside the jurisdiction](http://en.wikipedia.org/wiki/Extraterritorial_jurisdiction%22%20%5Co%20%22Extraterritorial%20jurisdiction) of the United States, and which would be an offense in the U.S., will be prosecuted under [18 U.S.C.](http://en.wikipedia.org/wiki/Title_18_of_the_United_States_Code%22%20%5Co%20%22Title%2018%20of%20the%20United%20States%20Code) [§ 1029](http://www.law.cornell.edu/uscode/18/1029.html), which deals with fraud and related activity in connection with access devices.

**Title IV: Border security**

Main article: [USA PATRIOT Act, Title IV](http://en.wikipedia.org/wiki/USA_PATRIOT_Act%2C_Title_IV%22%20%5Co%20%22USA%20PATRIOT%20Act%2C%20Title%20IV)

Title IV amends the *[Immigration and Nationality Act of 1952](http://en.wikipedia.org/wiki/Immigration_and_Nationality_Act_of_1952%22%20%5Co%20%22Immigration%20and%20Nationality%20Act%20of%201952)* to give more law enforcement and investigative power to the United States Attorney General and to the [Immigration and Naturalization Service](http://en.wikipedia.org/wiki/Immigration_and_Naturalization_Service%22%20%5Co%20%22Immigration%20and%20Naturalization%20Service) (INS). The Attorney General was authorized to waive any cap on the number of full time [employees](http://en.wikipedia.org/wiki/Employee%22%20%5Co%20%22Employee) (FTEs) assigned to the INS on the [Northern border](http://en.wikipedia.org/wiki/Canada%E2%80%93United_States_border%22%20%5Co%20%22Canada%E2%80%93United%20States%20border) of the United States. Enough funds were set aside to triple the maximum number of [Border Patrol](http://en.wikipedia.org/wiki/United_States_Border_Patrol%22%20%5Co%20%22United%20States%20Border%20Patrol) 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](http://en.wikipedia.org/wiki/United_States_Customs_Service%22%20%5Co%20%22United%20States%20Customs%20Service) to improve technology for monitoring the Northern Border and acquiring additional equipment at the Canadian northern border. The INS was also given the authority to authorize overtime payments of up to an extra US$30,000 a year to INS employees. Access was given to the [Department of State](http://en.wikipedia.org/wiki/Department_of_State%22%20%5Co%20%22Department%20of%20State) and the INS to criminal background information contained in the [National Crime Information Center's Interstate Identification Index](http://en.wikipedia.org/wiki/National_Crime_Information_Center%27s_Interstate_Identification_Index%22%20%5Co%20%22National%20Crime%20Information%20Center%27s%20Interstate%20Identification%20Index) (NCIC-III), [Wanted Persons File](http://www.amw.com/fugitives/most_wanted_lists.cfm) and any other files maintained by the [National Crime Information Center](http://en.wikipedia.org/wiki/National_Crime_Information_Center%22%20%5Co%20%22National%20Crime%20Information%20Center) to determine whether [visa](http://en.wikipedia.org/wiki/Visa_%28document%29%22%20%5Co%20%22Visa%20%28document%29) applicants and applicants could be admitted to the U.S. The [Department of State](http://en.wikipedia.org/wiki/United_States_Department_of_State%22%20%5Co%20%22United%20States%20Department%20of%20State) 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. Additionally, the [National Institute of Standards and Technology](http://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology%22%20%5Co%20%22National%20Institute%20of%20Standards%20and%20Technology) (NIST) was ordered to develop a technology standard to verify the identity of persons applying for a United States visa. The reason was to make the standard the technology basis for a cross-agency, cross-platform electronic system used for conducting [background checks](http://en.wikipedia.org/wiki/Background_check%22%20%5Co%20%22Background%20check), confirming identities and ensuring that people have not received visas under different names. This report was released on November 13, 2002, 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." This report was later superseded by section 303(a) of the *[Enhanced Border Security and Visa Entry Reform Act of 2002](http://en.wikipedia.org/wiki/Enhanced_Border_Security_and_Visa_Entry_Reform_Act_of_2002%22%20%5Co%20%22Enhanced%20Border%20Security%20and%20Visa%20Entry%20Reform%20Act%20of%202002)*.

Under subtitle C, various definitions relating to terrorism were altered and expanded. The INA was [retroactively](http://en.wikipedia.org/wiki/Retroactive_legislation%22%20%5Co%20%22Retroactive%20legislation) 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. The definition of "terrorist activity" was strengthened to include actions involving the use of any dangerous device (and not just explosives and firearms). 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](http://en.wikipedia.org/wiki/Safe_house%22%20%5Co%20%22Safe%20house), transportation, communications, funds, transfer of funds or other material financial benefit, false documentation or identification, weapons (including [chemical](http://en.wikipedia.org/wiki/Chemical_warfare%22%20%5Co%20%22Chemical%20warfare), [biological](http://en.wikipedia.org/wiki/Biological_warfare), or [radiological weapons](http://en.wikipedia.org/wiki/Radiological_weapon%22%20%5Co%20%22Radiological%20weapon)), explosives, or training to perform the terrorist act. 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. 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.](http://en.wikipedia.org/wiki/Title_8_of_the_United_States_Code%22%20%5Co%20%22Title%208%20of%20the%20United%20States%20Code) [§ 1189](http://www.law.cornell.edu/uscode/8/1189.html) by the Secretary of State.

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](http://en.wikipedia.org/wiki/Espionage%22%20%5Co%20%22Espionage); 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. 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. [Judicial review](http://en.wikipedia.org/wiki/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](http://en.wikipedia.org/wiki/Habeas_corpus%22%20%5Co%20%22Habeas%20corpus) proceedings. Such proceedings can be initiated by an application filed with the [United States Supreme Court](http://en.wikipedia.org/wiki/United_States_Supreme_Court%22%20%5Co%20%22United%20States%20Supreme%20Court), by any justice of the Supreme Court, by any [circuit judge](http://en.wikipedia.org/wiki/Circuit_court%22%20%5Co%20%22Circuit%20court) of the [United States Court of Appeals](http://en.wikipedia.org/wiki/United_States_Court_of_Appeals%22%20%5Co%20%22United%20States%20Court%20of%20Appeals) for the [District of Columbia Circuit](http://en.wikipedia.org/wiki/District_of_Columbia%22%20%5Co%20%22District%20of%20Columbia), or by any [district court](http://en.wikipedia.org/wiki/United_States_district_court%22%20%5Co%20%22United%20States%20district%20court) otherwise having jurisdiction to entertain the application. The final order is subject to [appeal](http://en.wikipedia.org/wiki/Appeal%22%20%5Co%20%22Appeal) to the [United States Court of Appeals](http://en.wikipedia.org/wiki/United_States_Court_of_Appeals%22%20%5Co%20%22United%20States%20Court%20of%20Appeals) for the District of Columbia Circuit. 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](http://en.wikipedia.org/wiki/Committee_on_the_Judiciary_of_the_House_of_Representatives%22%20%5Co%20%22Committee%20on%20the%20Judiciary%20of%20the%20House%20of%20Representatives) and the [Committee on the Judiciary of the Senate](http://en.wikipedia.org/wiki/Committee_on_the_Judiciary_of_the_Senate%22%20%5Co%20%22Committee%20on%20the%20Judiciary%20of%20the%20Senate).

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](http://en.wikipedia.org/wiki/Illegal_Immigration_Reform_and_Immigrant_Responsibility_Act_of_1996%22%20%5Co%20%22Illegal%20Immigration%20Reform%20and%20Immigrant%20Responsibility%20Act%20of%201996)* (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](http://en.wikipedia.org/w/index.php?title=Immigration_and_Naturalization_Service_Data_Management_Improvement_Act_of_2000&action=edit&redlink=1" \o "Immigration and Naturalization Service Data Management Improvement Act of 2000 (page does not exist))*. 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. The Attorney General was ordered to implement and expand the foreign student monitoring program that was established under section 641(a) of the IIRIRA. 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](http://en.wikipedia.org/wiki/United_States_Secretary_of_Education%22%20%5Co%20%22United%20States%20Secretary%20of%20Education) and the Secretary of State. US$36,800,000 was appropriated for the [Department of Justice](http://en.wikipedia.org/wiki/United_States_Department_of_Justice%22%20%5Co%20%22United%20States%20Department%20of%20Justice) to spend on implementing the program.

The Secretary of State was ordered to audit and report back to Congress on the Visa waiver program specified under [8 U.S.C.](http://en.wikipedia.org/wiki/Title_8_of_the_United_States_Code%22%20%5Co%20%22Title%208%20of%20the%20United%20States%20Code) [§ 1187](http://www.law.cornell.edu/uscode/8/1187.html) 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. The Secretary was also ordered to report back to Congress on whether [consulate shopping](http://en.wikipedia.org/wiki/Consulate_shopping%22%20%5Co%20%22Consulate%20shopping) was a problem.

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. 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.

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. The *[State Department Basic Authorities Act of 1956](http://en.wikipedia.org/w/index.php?title=State_Department_Basic_Authorities_Act_of_1956&action=edit&redlink=1" \o "State Department Basic Authorities Act of 1956 (page does not exist))* 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 and to identify any key leaders of terrorist organizations. 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. The [*DNA Analysis Backlog Elimination Act*](http://en.wikipedia.org/wiki/DNA_Analysis_Backlog_Elimination_Act) was amended to include terrorism or crimes of violence in the list of qualifying Federal offenses. 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.

[Secret Service](http://en.wikipedia.org/wiki/United_States_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. The *[General Education Provisions Act](http://en.wikipedia.org/w/index.php?title=General_Education_Provisions_Act&action=edit&redlink=1" \o "General Education Provisions Act (page does not exist))* 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.

One of the most controversial aspects of the USA PATRIOT Act is in title V, and relates to [National Security Letters](http://en.wikipedia.org/wiki/National_Security_Letter%22%20%5Co%20%22National%20Security%20Letter) (NSLs). An NSL is a form of administrative [subpoena](http://en.wikipedia.org/wiki/Subpoena%22%20%5Co%20%22Subpoena) used by the FBI, and reportedly by other U.S. government agencies including the CIA and the [Department of Defense](http://en.wikipedia.org/wiki/United_States_Department_of_Defense%22%20%5Co%20%22United%20States%20Department%20of%20Defense) (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. 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 to not 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. 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. 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.

**Title VI: Victims and families of victims of terrorism**

Main article: [USA PATRIOT Act, Title VI](http://en.wikipedia.org/wiki/USA_PATRIOT_Act%2C_Title_VI%22%20%5Co%20%22USA%20PATRIOT%20Act%2C%20Title%20VI)

Title VI made amendments to the *Victims of Crime Act of 1984* (VOCA) in order to make changes to how the U.S. Victims of Crime Fund was managed and funded. Changes were made to VOCA to improve the speedy provision of aid to families of public safety officers by expedited payments to officers or the families of officers. Under the changes, payments must be made no later than 30 days after the officer is injured or killed in the line of duty. The Assistant Attorney General was given expanded authority under section 614 of the USA PATRIOT Act to make grants to any organization that administers any [Office of Justice Programs](http://en.wikipedia.org/wiki/Office_of_Justice_Programs%22%20%5Co%20%22Office%20of%20Justice%20Programs), which includes the Public Safety Officers Benefits Program. Further changes to the Victims of Crime Fund increased the amount of money in the Fund, and changed the way that funds were distributed. 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](http://en.wikipedia.org/wiki/Means_test%22%20%5Co%20%22Means%20test) was also waived for those who apply for compensation. 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](http://en.wikipedia.org/wiki/District_of_Columbia), the [Commonwealth of Puerto Rico](http://en.wikipedia.org/wiki/Puerto_Rico), the [United States Virgin Islands](http://en.wikipedia.org/wiki/United_States_Virgin_Islands), and any other U.S. territory. VOCA also provides for compensation and assistance to victims of terrorism or mass violence. 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.

**Title VIII: Terrorism criminal law**

Main article: [USA PATRIOT Act, Title VIII](http://en.wikipedia.org/wiki/USA_PATRIOT_Act%2C_Title_VIII%22%20%5Co%20%22USA%20PATRIOT%20Act%2C%20Title%20VIII)

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. Terrorism is also included in the definition of [racketeering](http://en.wikipedia.org/wiki/Racket_%28crime%29%22%20%5Co%20%22Racket%20%28crime%29). Terms relating to [cyber-terrorism](http://en.wikipedia.org/wiki/Cyber-terrorism%22%20%5Co%20%22Cyber-terrorism) are also redefined, including the term "protected computer," "damage," "conviction," "person," and "loss."

New penalties were created to convict those who attack [mass transportation systems](http://en.wikipedia.org/wiki/Public_transport%22%20%5Co%20%22Public%20transport). 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](http://en.wikipedia.org/wiki/Death%22%20%5Co%20%22Death) of any person, then the punishment is a fine and life imprisonment. 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](http://en.wikipedia.org/wiki/Prophylaxis%22%20%5Co%20%22Prophylaxis), protective, [bona fide](http://en.wikipedia.org/wiki/Good_faith%22%20%5Co%20%22Good%20faith) 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.

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. U.S. [forfeiture](http://en.wikipedia.org/wiki/Asset_forfeiture%22%20%5Co%20%22Asset%20forfeiture) 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. One section of the Act (section 805) prohibited "material support" for terrorists, and in particular included "expert advice or assistance." This was struck down as unconstitutional by a [U.S. Federal Court](http://en.wikipedia.org/wiki/United_States_federal_court%22%20%5Co%20%22United%20States%20federal%20court) after the [Humanitarian Law Project](http://en.wikipedia.org/wiki/Humanitarian_Law_Project%22%20%5Co%20%22Humanitarian%20Law%20Project) filed a civil action against the U.S. government. The court found that it violated the First and Fifth Amendments to the United States Constitution and the provision was so vague it would cause a person of average intelligence to have to guess whether they were breaking the law, thus leading to a potential situation where a person was charged for an offense that they had no way of knowing was illegal. The court found that this could potentially have the effect of allowing arbitrary and discriminatory enforcement of the law, as well as possible [chilling effects](http://en.wikipedia.org/wiki/Chilling_effect_%28term%29%22%20%5Co%20%22Chilling%20effect%20%28term%29) on First Amendment rights. Congress later improved the law by defining the definitions of the "material support or resources," "training," and "expert advise or resources."

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. 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.

**Title IX: Improved Intelligence**

Main article: [USA PATRIOT Act, Title IX](http://en.wikipedia.org/wiki/USA_PATRIOT_Act%2C_Title_IX%22%20%5Co%20%22USA%20PATRIOT%20Act%2C%20Title%20IX)

Title IX amends the *[National Security Act of 1947](http://en.wikipedia.org/wiki/National_Security_Act_of_1947%22%20%5Co%20%22National%20Security%20Act%20of%201947)* to require the [Director of Central Intelligence](http://en.wikipedia.org/wiki/Director_of_Central_Intelligence%22%20%5Co%20%22Director%20of%20Central%20Intelligence) (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. 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. International terrorist activities were made to fall within the scope of foreign intelligence under the *National Security Act*.

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](http://en.wikipedia.org/wiki/National_Virtual_Translation_Center%22%20%5Co%20%22National%20Virtual%20Translation%20Center), 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. 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](http://en.wikipedia.org/wiki/United_States_Senate_Select_Committee_on_Intelligence%22%20%5Co%20%22United%20States%20Senate%20Select%20Committee%20on%20Intelligence) 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." Another report was commissioned on the feasibility and desirability of reconfiguring the Foreign Terrorist Asset Tracking Center and the [Office of Foreign Assets Control](http://en.wikipedia.org/wiki/Office_of_Foreign_Assets_Control%22%20%5Co%20%22Office%20of%20Foreign%20Assets%20Control) of the [Department of the Treasury](http://en.wikipedia.org/wiki/United_States_Department_of_the_Treasury%22%20%5Co%20%22United%20States%20Department%20of%20the%20Treasury). 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."

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. 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. 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.

**Reauthorizations**

The USA PATRIOT Act was reauthorized by two 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](http://en.wikipedia.org/wiki/Intelligence_Reform_and_Terrorism_Prevention_Act_of_2004%22%20%5Co%20%22Intelligence%20Reform%20and%20Terrorism%20Prevention%20Act%20of%202004)*. It created new provisions relating to the [death penalty](http://en.wikipedia.org/wiki/Capital_punishment%22%20%5Co%20%22Capital%20punishment) for terrorists, enhancing security at [seaports](http://en.wikipedia.org/wiki/Seaport%22%20%5Co%20%22Seaport), new measures to combat the financing of terrorism, new powers for the [Secret Service](http://en.wikipedia.org/wiki/United_States_Secret_Service), anti-[Methamphetamine](http://en.wikipedia.org/wiki/Methamphetamine) initiatives 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. However, the change also meant that the defendant was also made to tell the FBI who they were disclosing the order to — this requirement was removed by the *USA PATRIOT Act Additional Reauthorizing Amendments Act*.

As NSL provisions of the USA PATRIOT Act had been struck by the courts 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*. 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". 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. 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. Later, the *Additional Reauthorization Amendments Act* excluded libraries from receiving NSLs, except where they provide electronic communications services. 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](http://en.wikipedia.org/wiki/House_Committee_on_Financial_Services%22%20%5Co%20%22House%20Committee%20on%20Financial%20Services) and the [Senate Committee on Banking, Housing, and Urban Affairs](http://en.wikipedia.org/wiki/Senate_Committee_on_Banking%2C_Housing%2C_and_Urban_Affairs%22%20%5Co%20%22Senate%20Committee%20on%20Banking%2C%20Housing%2C%20and%20Urban%20Affairs) on all NSL request made under the *Fair Credit Reporting Act*.

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.

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 and was later amended to prevent a delayed notification "if the adverse results consist only of unduly delaying a trial."

The reauthorization act also legislates increased congressional oversight for emergency disclosures by communication providers undertaken under section 212 of the USA PATRIOT Act. 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. 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. The amendment to material support law done in the *Intelligence Reform and Terrorism Prevention Act* was also made permanent. The definition of terrorism was further expanded to include receiving military-type training from a foreign terrorist organization and [narcoterrorism](http://en.wikipedia.org/wiki/Narcoterrorism%22%20%5Co%20%22Narcoterrorism). Other provisions of the reauthorization act was to merge the law outlawing train wrecking ([18 U.S.C.](http://en.wikipedia.org/wiki/Title_18_of_the_United_States_Code%22%20%5Co%20%22Title%2018%20of%20the%20United%20States%20Code) [§ 992](http://www.law.cornell.edu/uscode/18/992.html)) and the law outlawing attacks on mass transportation systems ([18 U.S.C.](http://en.wikipedia.org/wiki/Title_18_of_the_United_States_Code%22%20%5Co%20%22Title%2018%20of%20the%20United%20States%20Code) [§ 1993](http://www.law.cornell.edu/uscode/18/1993.html)) into a new section of Title 18 of the U.S. Code ([18 U.S.C.](http://en.wikipedia.org/wiki/Title_18_of_the_United_States_Code%22%20%5Co%20%22Title%2018%20of%20the%20United%20States%20Code) [§ 1992](http://www.law.cornell.edu/uscode/18/1992.html)) and also to criminalize the act of planning a terrorist attack against a mass transport system. [Forfeiture law](http://en.wikipedia.org/wiki/Asset_forfeiture) 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](http://en.wikipedia.org/wiki/Death%22%20%5Co%20%22Death) or imprisonment for a term exceeding one year. Alternatively, this applies if similar punishment would be so punishable if committed within the U.S. A sense of Congress was further expressed that victims of terrorism should be entitled to the forfeited assets of terrorists.

**Controversy**

Main article: [Controversial invocations of the USA PATRIOT Act](http://en.wikipedia.org/wiki/Controversial_invocations_of_the_USA_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 terrorist attacks](http://en.wikipedia.org/wiki/September_11_terrorist_attacks%22%20%5Co%20%22September%2011%20terrorist%20attacks), believing there to 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](http://en.wikipedia.org/wiki/Patrick_Leahy%22%20%5Co%20%22Patrick%20Leahy) and [Russell Feingold](http://en.wikipedia.org/wiki/Russell_Feingold%22%20%5Co%20%22Russell%20Feingold) proposed amendments to modify the final revision.) The sheer magnitude of the Act itself was noted by [Michael Moore](http://en.wikipedia.org/wiki/Michael_Moore%22%20%5Co%20%22Michael%20Moore) in his controversial film *[Fahrenheit 9/11](http://en.wikipedia.org/wiki/Fahrenheit_9/11%22%20%5Co%20%22Fahrenheit%209/11)*. In one of the scenes of the movie, he records Congressman [Jim McDermott](http://en.wikipedia.org/wiki/Jim_McDermott%22%20%5Co%20%22Jim%20McDermott) alleging that no Senator read the bill and John Conyers, Jr. as saying, "We don't really read most of the bills. Do you 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". As a [dramatic device](http://en.wikipedia.org/wiki/Dramatic_device%22%20%5Co%20%22Dramatic%20device), Moore then hired an [ice-cream van](http://en.wikipedia.org/wiki/Ice-cream_van%22%20%5Co%20%22Ice-cream%20van) and drove around Washington, D.C. with a loud speaker, reading out the Act to puzzled passers-by, which included a few Senators. However, Moore was not the only commentator to notice that not many people had read the Act. When [Dahlia Lithwick](http://en.wikipedia.org/wiki/Dahlia_Lithwick%22%20%5Co%20%22Dahlia%20Lithwick) and Julia Turne for *[Slate](http://en.wikipedia.org/wiki/Slate_%28magazine%29%22%20%5Co%20%22Slate%20%28magazine%29)* asked, "How bad is Patriot, anyway?", they decided that it was "hard to tell" and stated:

The [ACLU](http://en.wikipedia.org/wiki/American_Civil_Liberties_Union%22%20%5Co%20%22American%20Civil%20Liberties%20Union), in a new fact sheet challenging the [DOJ](http://en.wikipedia.org/wiki/United_States_Department_of_Justice%22%20%5Co%20%22United%20States%20Department%20of%20Justice) 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.

Some believe the USA PATRIOT Act is too broad: it applies to terrorist, suspected terrorist, and law abiding citizens. For example, in the [United States of America](http://en.wikipedia.org/wiki/United_States_of_America%22%20%5Co%20%22United%20States%20of%20America), one cannot open a bank account using a post office box. The financial institution will decline citing the money laundering provisions [PATRIOT Act](http://en.wikipedia.org/wiki/PATRIOT_Act).

Some television shows as *[NCIS](http://en.wikipedia.org/wiki/NCIS_%28TV_series%29%22%20%5Co%20%22NCIS%20%28TV%20series%29)*, [*Law & Order: Special Victims Unit*](http://en.wikipedia.org/wiki/Law_%26_Order%3A_Special_Victims_Unit), [*Boston Legal*](http://en.wikipedia.org/wiki/Boston_Legal) and *[Las Vegas](http://en.wikipedia.org/wiki/Las_Vegas_%28TV_series%29%22%20%5Co%20%22Las%20Vegas%20%28TV%20series%29)* have been keen to use the USA PATRIOT Act as a plot device, often for purposes it was not intended.

[EPIC](http://en.wikipedia.org/wiki/Electronic_Privacy_Information_Center) has criticized the law as unconstitutional, especially when "the private communications of law-abiding American citizens might be intercepted incidentally", while the [EFF](http://en.wikipedia.org/wiki/Electronic_Frontier_Foundation) hold that the lower standard applied to wiretaps "gives the [FBI](http://en.wikipedia.org/wiki/Federal_Bureau_of_Investigation%22%20%5Co%20%22Federal%20Bureau%20of%20Investigation) a 'blank check' to violate the communications privacy of countless innocent Americans". Others do not find the roving wiretap legislation to be as concerning. Professor [David D. Cole](http://en.wikipedia.org/wiki/David_D._Cole%22%20%5Co%20%22David%20D.%20Cole) of the [Georgetown University Law Center](http://en.wikipedia.org/wiki/Georgetown_University_Law_Center%22%20%5Co%20%22Georgetown%20University%20Law%20Center), a critic of many of the provisions of the Act, found that though they come at a cost to privacy are a sensible measure while Paul Rosenzweig, a Senior Legal Research Fellow in the Center for Legal and Judicial Studies at the [Heritage Foundation](http://en.wikipedia.org/wiki/Heritage_Foundation%22%20%5Co%20%22Heritage%20Foundation), argues that roving wiretaps are just a response to rapidly changing communication technology that is not necessarily fixed to a specific location or device.

The Act also allows access to voicemail through a search warrant rather than through a title III wiretap order. James Dempsey, of the [CDT](http://en.wikipedia.org/wiki/Center_for_Democracy_and_Technology%22%20%5Co%20%22Center%20for%20Democracy%20and%20Technology), believes that it unnecessarily overlooks the importance of notice under the [Fourth Amendment](http://en.wikipedia.org/wiki/Fourth_Amendment_to_the_United_States_Constitution%22%20%5Co%20%22Fourth%20Amendment%20to%20the%20United%20States%20Constitution) and under a Title III wiretap, 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 couldn't use the messages in evidence against the defendant. Others disagree with these assessments. Professor [Orin Kerr](http://en.wikipedia.org/wiki/Orin_Kerr%22%20%5Co%20%22Orin%20Kerr), of the [George Washington University](http://en.wikipedia.org/wiki/George_Washington_University%22%20%5Co%20%22George%20Washington%20University) school of law, believes that the [ECPA](http://en.wikipedia.org/wiki/Electronic_Communications_Privacy_Act%22%20%5Co%20%22Electronic%20Communications%20Privacy%20Act) "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.

The USA PATRIOT Act's expansion of court jurisdiction to allow the nationwide service of search warrants proved controversial for the EFF. 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", and that it reduces the likelihood that smaller [ISPs](http://en.wikipedia.org/wiki/Internet_service_provider%22%20%5Co%20%22Internet%20service%20provider) 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." 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.

For a time, the USA PATRIOT Act allowed for agents to undertake "sneak and peek" searches. Critics such as EPIC and the ACLU strongly criticized the law for violating the Fourth Amendment, with the ACLU going so far as to release an advertisement condemning it and calling for it to be repealed. However supporters of the amendment, such as [Heather Mac Donald](http://en.wikipedia.org/wiki/Heather_Mac_Donald%22%20%5Co%20%22Heather%20Mac%20Donald), a fellow at the [Manhattan Institute](http://en.wikipedia.org/wiki/Manhattan_Institute%22%20%5Co%20%22Manhattan%20Institute) and contributing editor to the *[New York City Journal](http://en.wikipedia.org/wiki/City_Journal_%28New_York%29%22%20%5Co%20%22City%20Journal%20%28New%20York%29)*, 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. In 2004, FBI agents used this provision to search and secretly examine the home of [Brandon Mayfield](http://en.wikipedia.org/wiki/Brandon_Mayfield%22%20%5Co%20%22Brandon%20Mayfield), who was wrongfully jailed for two weeks on suspicion of involvement in the [Madrid train bombings](http://en.wikipedia.org/wiki/Madrid_train_bombings%22%20%5Co%20%22Madrid%20train%20bombings). While the U.S. Government did publicly apologize to Mayfield and his family, 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.

Laws governing the material support of terrorism proved contentious. It was criticized by the EFF for infringement of [freedom of association](http://en.wikipedia.org/wiki/Freedom_of_association%22%20%5Co%20%22Freedom%20of%20association). The EFF argues that had this law been enacted during [Apartheid](http://en.wikipedia.org/wiki/Apartheid%22%20%5Co%20%22Apartheid), U.S. citizens would not have been able to support the [African National Congress](http://en.wikipedia.org/wiki/African_National_Congress%22%20%5Co%20%22African%20National%20Congress) (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 [Hamas](http://en.wikipedia.org/wiki/Hamas%22%20%5Co%20%22Hamas) members how to care for civilian children orphaned in the conflict between Israelis and Palestinians, a lawyer being unable to teach [IRA](http://en.wikipedia.org/wiki/Provisional_Irish_Republican_Army%22%20%5Co%20%22Provisional%20Irish%20Republican%20Army) members about [international law](http://en.wikipedia.org/wiki/International_law%22%20%5Co%20%22International%20law), and peace workers being unable to offer training in effective peace negotiations or how to petition the [United Nations](http://en.wikipedia.org/wiki/United_Nations%22%20%5Co%20%22United%20Nations) regarding human rights abuses. Another group, the [Humanitarian Law Project](http://en.wikipedia.org/wiki/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. They succeeded, and a Federal Court found that the law was vague enough to cause a reasonable person to guess whether they were breaking the law or not. Thus they found it violated the [First Amendment](http://en.wikipedia.org/wiki/First_Amendment_to_the_United_States_Constitution%22%20%5Co%20%22First%20Amendment%20to%20the%20United%20States%20Constitution) rights of U.S. citizens, and struck it down.

Perhaps one of the biggest controversies involved the use of [NSLs](http://en.wikipedia.org/wiki/National_Security_Letter) 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. In November 2005, [*BusinessWeek*](http://en.wikipedia.org/wiki/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](http://en.wikipedia.org/wiki/Las_Vegas_metropolitan_area) 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". 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](http://en.wikipedia.org/wiki/Internet_Service_Provider) who had been issued an NSL, for reasons unknown. In [*ACLU v. DoJ*](http://en.wikipedia.org/wiki/American_Civil_Liberties_Union_v._Ashcroft_%282004%29), 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. 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.

Another provision of the USA PATRIOT Act has caused a great deal of consternation amongst 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". 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. As proof, then Attorney General John Ashcroft released information in 2003 that showed that section 215 orders had never been used. However, despite protestations to the contrary, the [American Library Association](http://en.wikipedia.org/wiki/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. 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. Consequently, reports started filtering in that librarians were shredding records to avoid having to comply with such orders.

Another controversial aspect of the USA PATRIOT Act is the immigration provisions that allow for the indefinite detention of any alien whom the Attorney General believes may cause a terrorist act. Before the USA PATRIOT Act was passed, [Anita Ramasastry](http://en.wikipedia.org/wiki/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](http://en.wikipedia.org/wiki/University_of_Washington_School_of_Law) in [Seattle, Washington](http://en.wikipedia.org/wiki/Seattle%2C_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](http://en.wikipedia.org/wiki/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." 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". The [University of California](http://en.wikipedia.org/wiki/University_of_California) passed a resolution condemning (amongst other things) the indefinite detention provisions of the Act, 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."

Another controversial aspect of the USA PATRIOT Act is its effect on the privacy of British Columbian citizens. 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 British Columbia 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. 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”.

In an effort to maintain their privacy, [British Columbia](http://en.wikipedia.org/wiki/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.” 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.”

Legal action has been taken in [Nova Scotia](http://en.wikipedia.org/wiki/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."