PATRIOT Act

- **By:** Fritz Messere
- In: The SAGE Encyclopedia of Journalism
- **Chapter DOI:**https://doi.org/10.4135/9781544391199.n304
- Subject: Journalism, Mass Communication
- **Keywords:**law; law enforcement; Patriot Act; terrorism

The USA PATRIOT Act (full name: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001) was a law passed overwhelmingly by Congress on October 24, 2001. Two days later, President George W. Bush signed the act into law creating legislation that gave sweeping new powers to government to collect information that could thwart potential terrorist attacks against the United States.

In 1996, President Bill Clinton asked Congress to give law enforcement expanded wiretap authority and increased access to personal records in terrorism cases. This request occurred shortly after the Oklahoma City bombing in April 1995. Congress refused, citing concerns that loosening surveillance rules would be unconstitutional. However, in the wake of the horrific attacks on the World Trade Center and the Pentagon on September 11, 2001, Congress was ready to act. The Bush administration drafted legislation to expand powers of government to investigate and detain suspected terrorists and to increase the powers of law enforcement. Different House and Senate draft bills were merged into a compromise bill that greatly expanded the ability of law enforcement to seek information in the course of federal investigations against acts of terrorism, both foreign and domestic.

Additional powers given to law enforcement included:

The use of surveillance and roving wiretaps for computer and terrorist crimes, for money laundering, immigration, and other potential criminal areas. Roving wiretaps occur when a court grants surveillance warrants without naming either the communication carrier and/or other third parties involved in the operation.

The ability to subpoena telephone subscribers' credit cards or bank account numbers to prevent money laundering.

The use of trap-and-trace devices, which can record source and destinations of calls made to and from a particular telephone.

In addition, law enforcement was not required to show probable cause to initiate surveillance under the act but only certify that the information sought was likely to be relevant to a criminal investigation. The law also made changes to the way the Foreign Intelligence Surveillance Court operated, specifically removing the previous requirement that the government certify in its application that the "purpose of the surveillance was to collect foreign intelligence information." Finally, the act ended the statute of limitations for certain terror-related crimes.

The new law was aimed at improving homeland security by providing law enforcement with expanded tools to track terrorists. However, many of the controversial requirements of the PATRIOT Act were slated to expire in 2005 unless Congress and the president chose to renew them.

Many civil liberties organizations expressed deep concern about the law and the potential for law enforcement to abridge civil and privacy rights of Americans. The American Civil Liberties Union complained that the act made it easier for government to spy on ordinary citizens because law enforcement now had authority to monitor phone and email communication, collect bank and credit card records, and track activities on the Internet. Others complained that the act eliminated checks and balances that previously gave the courts the opportunity to ensure that law enforcement powers were not abused.

One section of the act that was particularly concerning to civil liberties organizations was Section 215. This section of the act modified part of the previously enacted Foreign Intelligence Surveillance Act. The language of Section 215 allows for the Foreign Intelligence Surveillance Act court to approve orders to collect "tangible things" that could be relevant to a government investigation. The list of what could be included as "tangible things" was broad and included books, records, papers, and documents. These provisions have been interpreted to permit the bulk collection of "telephony metadata" (mass collection of call log information without personal identification). Thus, if an issue with a particular number is raised and that number is attributed to a U.S. resident, that information could be passed to the FBI, which then could use publicly available information to connect the number with the subscriber information. It is this bulk collection of data under Section 215 that critics claim violates individual rights since "tangible things" could mean anything from driver's license records to Internet browsing patterns. Section 215 has been reviewed and renewed by Congress since 2006, and the Supreme

Court has ruled that phone records are not considered privileged information for purposes of the Fourth Amendment to the U.S. Constitution. On March 15, 2020, Section 215 expired due to its sunset clause after lawmakers failed to reach an agreement on a broader set of reforms to Foreign Intelligence Surveillance Act.

Despite growing concerns about the implications for Americans' civil liberties, Congress has reauthorized most sections of the law several times since 2005. But sections of the law have met with legal challenges. In the case *Doe v. Mukasey*, a federal judge ruled in 2004 that parts of the law violated fundamental constitutional safeguards by allowing federal agencies to gather information about U.S. citizens secretly under national security letters without court approval. Congress modified sections of the law and made many of the provisions that were originally temporary permanent in May 2006. But the following year, the same court ruled that the new version of the act gave federal investigators powers to spy on individuals that were unconstitutionally broad. The federal government appealed the lower court decision and the Second Circuit U.S Court of Appeals upheld the lower court ruling and said that the "gag orders" imposed on recipients of national security letters were a violation of First Amendment rights.

In 2010, the U.S. Supreme Court took up the question of whether monitoring some terrorist activities violated the First Amendment to the U.S. Constitution. While the Court upheld the constitutionality of the "material support" statute that criminalizes support for any foreign terrorist organization designated by the U.S. secretary of state, the Court also noted that other aspects of the law remain untested and may not be constitutional.

In 2013, Edward Snowden, a former government contractor, released documents that revealed that the federal government was using Section 215 as justification to collect phone records on virtually all U.S. phone customers. These leaks put Section 215 at the center of a renewed controversy and led to a series of investigations related to programs that the government uses to collect information related to foreign and domestic terrorism. While Snowden has been called both a hero and a traitor, the documents leak brought into focus the fact that the PATRIOT Act has made it possible for the government to develop large-scale data collection programs.

The USA PATRIOT Act was passed quickly and with little debate. The Senate bill closely resembled the language put forward by the attorney general, while in the House a more moderate compromise bill was rejected and replaced with legislation that closely followed the Senate bill. The Bush administration lobbied hard for

passage and implied that Congressional members who did not support the bill could be blamed for further terrorist attacks, if they were to occur.

In 2004, speaking before the U.S. Senate Committee on the Judiciary, FBI Director Robert Mueller claimed that the PATRIOT Act had been beneficial in the war on terrorism and that many counterterrorism successes were the direct result of provisions of the law. The presidential administrations of Barack Obama and Donald Trump also supported the PATRIOT Act. In 2019, the Trump administration called upon Congress to renew Section 215 of the act indefinitely, saying that future technological innovations will emerge to make the act more useful over time. But according to the American Civil Liberties Union, despite the widespread use of tens of thousands of national security letters between 2003 and 2006, only one resulted in a terror-related conviction. Congress adopted some reforms to the law in the USA Freedom Act of 2015, which curtailed data collection.

Although modified several times over the years, the PATRIOT Act continues to provide federal law enforcement and intelligence gathering agencies tools to collect information to identify and fight potential terrorist activities in the United States. The Department of Justice has claimed that the act allows federal agents to follow sophisticated terrorists trained to evade detection and to conduct investigations without tipping off terrorists. The law also facilitates information sharing and cooperation among government agencies, increases penalties for those who commit terrorist crimes, and updates the law to use new technologies. Critics of the law complain that it tramples on Americans' constitutional rights, collects data on citizens without their knowledge, and is excessively costly without providing the benefits it was intended to provide.

See also Secrecy and Leaks; Terrorism, Coverage of; War and Military Journalism

Fritz Messere

American Civil Liberties Union. (n.d.). Surveillance under the PATRIOT Act. Retrieved from https://www.aclu.org/issues/national-security/privacy-and-

surveillance/surveillance-under-patriot-act

Electronic Frontier Foundation. (n.d.). PATRIOT Act. Retrieved

from https://www.eff.org/issues/patriot-act

Smith, Cary and Hung, Li-Ching. (2004). *The PATRIOT Act: Issues and controversies*. Springfield, IL: Charles C. Thomas Pub.

U.S. Department of Justice (n.d.). The USA PATRIOT Act: Preserving life and liberty. Retrieved from https://www.justice.gov/archive/ll/highlights.htm