The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act, more commonly cited as the Patriot Act) is an act that has greatly increased the surveillance, investigative, and enforcement powers of governmental agencies as a central part of the War on Terrorism. The act can be read as a direct response to the September 11, 2001, attacks on the World Trade Center in New York City and the Pentagon in Washington, D.C. It quickly became one of the most controversial series of laws of the era, raising troubling questions over the nature and scope of the U.S. government’s antiterrorism and crime-prevention tactics, as well as questions over the civil liberty and privacy protections of American citizens. While its provisions allow for the surveillance of all Web content used or generated by a suspect, the act has particularly raised the ire of privacy advocates over its broad-reaching allowances for the search and surveillance of data on social networking sites.

**Historical Context**

Passed by a wide margin in both the House and Senate on October 26, 2001, the Patriot Act emerged as a compromise unification of two competing acts introduced in Congress in late September. What these bills shared was the central question asked by many American citizens following the attacks of September 11: what lapses had occurred in the nation's political, security, and counterterrorism apparatuses in order to allow such a catastrophe to occur? While there had been attacks that occurred on U.S. soil in the recent past, most notably the bombings of the World Trade Center in 1993 and the Alfred P. Murrah Federal Building in Oklahoma City in 1994, one would have to look back to the Pearl Harbor bombing of 1941 to find a comparable attack on American soil.

Yet if the attacks of September 2001 had little precedent in the history of American foreign policy, equally unprecedented was the exigency that led to the speedy passage of this sweeping legislation. Historically, it is often the case that tragedy in the face of domestic threats to safety leads to expedient action, and this bill was no different. The urgency of the situation was clear, and the bill faced relatively little debate, a fact that later led to much criticism of both the bill and many of the congressional members who voted for its provisions. The political and popular goodwill historically granted to heads of state following a state of emergency notwithstanding, the act’s passage was also encouraged by the decisive policy action of the George W. Bush administration's attorney general, John Ashcroft, who urged swift passage. The process was further hurried along by warnings that future terrorist acts were imminent and, from Ashcroft, that members of Congress themselves would bear the responsibility if an attack were to occur while the legislation was still in debate. As such, it faced few proposals for amendments and no formal reports from committees were requested. Some legislative provisions of the act, mostly dealing with electronic surveillance, were given sunset stipulations for the end of 2005 (most of which ended up being renewed at that time) to allow a compromise support for quick passage of the bill with the understanding of later legislative revisitation, but the majority of the act’s titles had no such conditions.

The Patriot Act passed in the House with a vote of 357 to 66, with only Democrats dissenting. It passed in the Senate with a vote of 99 to 1, with only Wisconsin Democrat Russ Feingold's opposition...
on the grounds of too little debate over such a granting of powers to the government. The reconciled bill was signed into law by President George W. Bush on October 26, 2001.

The content of the act represented an unprecedented expansion of the federal government’s legal authority to conduct surveillance, investigate, and prosecute criminal acts and acts of terrorism. The Patriot Act was incredibly lengthy, at 342 pages of text through 10 separate titles of law. These titles dealt with such issues as redefining terrorism criminal law (Title VIII), compensation for the families of terrorism victims (Title VI), border security (Title IV), new legislation for financial disclosures (Title III), and other issues that were particularly of importance for quick passage in the early months following the September 11 attacks. It also created new, more stringent requirements for immigration to the United States; trade sanctions against nation-states that supported terrorists; and, in a move largely viewed as court-stacking, an expansion of the number of judges on the secret Foreign Intelligence Surveillance Court from six to 11, with the five new members to be appointed by the Bush administration.

Problems Arise

The bill soon became deeply controversial. When the actual legislation was afforded a more in-depth examination of exactly what permissions were granted to the government, there quickly grew concerns over the act’s legal and moral legitimacy. Legislative and judicial critics chided the ambiguously clumsy and often murky wording of the bill, the granting of extraordinary powers to the executive and judicial branches at the expense of the legislative, and the questionable constitutionality of many of the enacted laws.

Political leaders on all levels of national governance revisited their positions on the bill as the political goodwill in the weeks following its passage wore off, perhaps most notably in presidential candidate John Kerry’s 2004 critique of the Patriot Act as creating a “knock-in-the-night police state” three years after voting for the act and having drafted several sections of the bill himself.

With time, the act proved to be quite divisive in Washington, with political parties commonly divided on the questions between the act’s protection of national security on one hand and the erosion of civil liberties and privacy protections on the other. Politician supporters of the bill largely argued that its intelligence-gathering and surveillance provisions were essential law-enforcement tools necessary to prevent future terrorist attacks, making a compelling argument that had these provisions been afforded to government prior to September 11, the attacks could have been prevented. Opponents argued that the bill was an unparalleled erosion of constitutional civil liberties through the voiding of long-precedented protections on privacy and due process rights of both American citizens and foreigners. While the issue raised concerns among legal and political circles, it was citizen and advocacy organizations that raised the greatest tumult from both of these countering perspectives and many points in between. Yet the bill has its fair share of defenders, as well; as of early 2011, most provisions of the Patriot Act were still in place.

Implications for Social Networks

The bill granted new latitude to the government’s law enforcement agencies in three central areas. The first two were the sanctioning of indefinite detention of foreigners suspected of planning or actually enacting attacks on American soldiers or civilians and the granting of powers to the secretary of the treasury to regulate international and domestic financial transactions. However, notwithstanding the debate over the legal, political, and moral merits of the Patriot Act undertaken in the media, in the halls
of Washington and around the dinner tables of citizens, it is the central issues of concern over networks of electronic communication—the government’s expanded surveillance and data-collection powers—that are of particular concern to social networks and electronic communication. This is especially the case as social networks have become closely embedded with the day-to-day activities of American citizens.

Judged by the media and popular dialogues that continued to take place in the years following its passage, the most controversial of the Patriot Act’s titles was Title II, whose provisions amending both the Foreign Intelligence Surveillance Act (FISA) of 1978 and the Electronic Communications Privacy Act of 1986 were primarily focused on the expansion and updating of governmental agency permissions to intercept and share the results of electronic surveillance and monitoring. The issue of governmental interference in the daily private lives of citizens is always a contentious issue among advocates of civil liberties and individual rights, but in this case, one defended by a number of supporters who argued that the September 11 attacks were as much a failure of intelligence as of security. This title also set out a section for individuals to redress the government should they feel their civil rights had been violated, but its functional efficacy has been questioned.

Title II laid out in 25 sections the guidelines of who may be the target of electronic surveillance and under what circumstances. What was most notable about this section of the Patriot Act was that its central focus was the granting of sweeping powers of electronic and traditional wiretapping and surveillance practices over citizens and noncitizens alike. The government was now allowed to eliminate the historical (if ill-defined) wall that had previously existed between federal criminal investigations and foreign intelligence gathering, a subtle but substantial alteration in law.

The title allowed the interception of communications coming into or going out of the United States, regardless of recipient, and encompassed e-mail, telephone, and Web content, including both public and private material sent over social networking sites. In addition, this title also allowed the governmental seizure of communication records. This wide-reaching authority included the recipients, duration, and global positioning satellite (GPS) location of telephone calls, text messages, and voicemail records; records of all electronic data from Internet service providers, including e-mail, Websites visited, chat records, and histories of search terms; purchasing histories from online and brick-and-mortar retailers, as well as credit card companies; records of programs watched from cable providers; and borrowing records from libraries.

Furthermore (and to great controversy), in order to not jeopardize ongoing investigations, the providers of this information would not be permitted to disclose to customers or patrons that their records had been requested by law enforcement agencies, nor was the government required to disclose the reasons behind the order. Under the provisions of the act, telecommunications corporations such as AT&T, Verizon, Google, and Microsoft would be forced to hand over the communication records and content for persons of interest to governmental agencies upon request. Libraries and bookstores would also be required to do so, although many protested the act by deleting user purchases or purging library checkout records.

Social networking sites were not exempt from this section. Facebook, MySpace, Twitter, and other commonly used social networking sites were subject to the same search-and-seizure provisions, the same nonnotification clauses as other telecommunication companies. This section created great distress among privacy advocates, who argued that government access to information, given the

https://search.credoreference.com/content/topic/usa_patriot_act
personal nature of social networking sites, was not unlike searching an individual's postal mail or peeking in through their windows to garner details on their personal habits, expressions, and behaviors.

**Sneak and Peek Warrants**

Similarly controversial was Section 213 of Title II, which dealt with the requirements for the issuance of warrants. Conventional search warrants require advance permission from a judge in order to justify entry into a person's or organization's physical or electronic property, as well as notification to owners and occupants that their property was searched. However, Section 213 specifically allowed “covert entry search warrants” or “delayed notification search warrants” (more commonly known as “sneak and peek warrants”), which allowed authorities to covertly surveil physical or electronic property of suspects without notification to the occupant, effectively granting law enforcement a free hand in searching citizens and noncitizens alike. These covert searches could take place repeatedly in both physical and electronic sites without reissuance of the warrant, often with a time frame of months or years. If illegal activities were found, an after-the-fact conventional warrant could be issued in order to seize evidence, which was customarily issued after an arrest had already occurred. Prior to the Patriot Act, sneak and peek warrants had been used by law enforcement with contradictory rulings in various district courts as to whether or not they violated the Fourth Amendment, but it was not until the Patriot Act that this type of warrant was expressly authorized in U.S. law.

Supporters of the bill argued that it was necessary to permit quickly executed and covert searches of criminals in order to prevent terrorists from disposing of evidence or tipping off their colleagues, both of which may occur in the time necessary to obtain a conventional search warrant or through notification that individuals were under investigation, particularly in the world of immaterial evidence, such as online communication or electronic data. Critics argued that despite the fact the Patriot Act was intended to be a tool for fighting terrorism, Section 213 allowed the use of this type of warrant with any suspected violation of federal law, including both felonies and misdemeanors. On a more systemic level, enforcement agencies were granted covert search and surveillance liberties that effectively negated the very warrant system that upheld a broad reading of protections under the Fourth Amendment.

https://search.credoreference.com/content/topic/usa_patriot_act
A pay phone sticker in Wisconsin protests Sec. 216 of the USA PATRIOT Act: allowing phone call monitoring without a warrant.

Ultimately, the Patriot Act presents a case study for the prescient questions surrounding the nature, scope, and role of government practices at the intersection of homeland security and civil rights in the digital age, particularly in social networks, where users' day-to-day activities are very much centered in the digital realm. As information becomes a necessary commodity for competitive business practices through the use of microlevel user data algorithms (such as http://Amazon.com, Facebook, and iTunes), and as the price of digital storage has become effectively negligible, there becomes a complete and permanent record of user communication, behavior, purchases, and characteristics that is available for governmental agencies' retrieval without users' knowledge. Political questions aside, the case of the Patriot Act revolves around the central and still-unanswered question for the digital age: where do citizens draw the line between civil rights for safety and security and the civil right for privacy in a networked society?

See Also:

https://search.credoreference.com/content/topic/usa_patriot_act
Further Readings


Tewksbury, Doug
Niagara University

APA

Chicago

Harvard

MLA


SAGE Publications, Inc.
APA

Chicago

Harvard

MLA