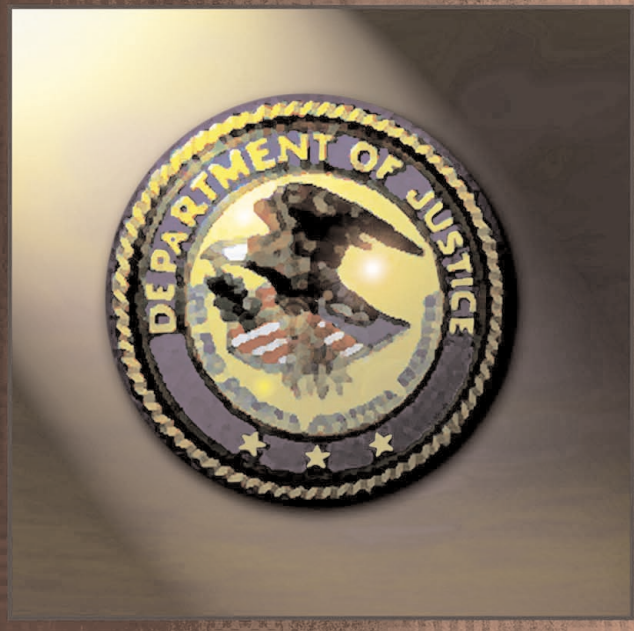
THE BASICS

THE USA PATRIOT ACT



A CENTURY FOUNDATION
GUIDE TO THE ISSUES

THE BASICS

THE USA PATRIOT ACT

A CENTURY FOUNDATION GUIDE TO THE ISSUES

The Century Foundation Press ◆ New York City

This pamphlet was prepared for The Century Foundation by Susan Hansen.

The Basics Series

America is engaged in difficult and complex policy debates over critical issues. There are conflicting claims and disagreements over the meaning of the facts and figures relating to the significance of the social safety net, the way our political system works, and the economic issues facing our nation. The Century Foundation hopes to help clarify these issues by collecting the best available information and presenting it in a series of pamphlets called The Basics.

The intent of this series is in keeping with the Foundation's mandate. Since 1919, The Century Foundation, formerly the Twentieth Century Fund, has sponsored and supervised research on economic, social, and political issues. As a nonpartisan, but not neutral organization, our underlying philosophy regards government as an instrument, not an enemy, of the people, and therefore we strive, in the words of our bylaws, for the "improvement of economic, industrial, civic, cultural, and educational conditions."

The Century Foundation also believes in the power of well-reasoned, well-researched ideas. These pamphlets are presented in that spirit. They are our contribution to increased citizen understanding and wiser governmental decisions.

Other titles in the series:

Immigration Reform
Tax Reform
Balancing the Budget
Social Security Reform
Medicare Reform
Medicaid Reform
NAFTA Expansion and Fast-Track Authority

To order additional copies of this pamphlet or other Basics pamphlets, please contact the Foundation (see page 36).

Contents

Introduction

The USA PATRIOT Act—which gave the executive branch a vast new arsenal of powers to thwart terrorism—was introduced in Congress within days after the attacks on the World Trade Center and Pentagon on September 11, 2001. The legislation received overwhelming support in both the House and Senate and was signed into law on October 26, 2001, by President Bush.

In the aftermath of September 11, anthrax mailings exacerbated the sense that terrorism had become a new and permanent part of daily life, and that fear put enormous pressure on the administration and Congress to act quickly and decisively.

That sense of urgency led to a short-circuiting of the deliberative process—committee hearings, debate, compromise—normally associated with even minor legislation. Indeed, many Patriot Act provisions had been previously proposed and rejected at least once by Congress.

That said, some elements of the Patriot Act have gained widespread acceptance. But other provisions have aroused considerable controversy, based on concerns that they grant the government broad new powers to intrude into the lives of ordinary American citizens without sufficient safeguards to preserve individual privacy and other basic constitutional rights.

The current debate over the Patriot Act is, in many ways, more spirited than it was when the law was originally enacted. A broad coalition of critics, including civil libertarians, librarians, and pro-gun groups from across the political spectrum, are now united in their belief that the Patriot Act strikes the wrong balance between the government's need to protect public safety and the citizenry's right to privacy. That coalition has mobilized on multiple fronts—Congress, the federal courts, and grassroots initiatives across the country—in an energetic effort to roll back the Patriot legislation.

The Bush administration remains adamant that the Patriot Act has not impinged on civil liberties or personal privacy—and that it has proved enormously useful in fighting terrorism and other crimes. With significant portions of the legislation set to expire in 2005, the administration is lobbying to make those provisions permanent. Moreover, it is asking Congress to pass new legislation that would give the executive branch even broader surveillance powers.

Polls indicate that the public lacks a deep understanding of the Patriot Act. In one recent *USA Today*/CNN/Gallup survey, for example, 43 percent of respondents said the balance the act strikes between national security and civil liberties was "about right"; yet, seven in ten people in the same poll said they oppose allowing federal agents to conduct secret searches of private homes, which the Patriot Act permits. Four in ten of those polled told Gallup they had little or no knowledge of the law.[1]

I. The USA PATRIOT Act: The Short Story

"USA PATRIOT" is actually an acronym for the law's formal title. Officially, it is known as the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (hereinafter Patriot Act).[2] The act weighs in at 342 pages, divided into ten separate sections, and is intended to expand intelligence and law enforcement capabilities to identify and disrupt terrorist activities. In drafting the legislation, the bill's authors largely built on existing federal law. All told, the Patriot Act makes changes, both minor and major, to more than fifteen different statutes, including the Electronic Communications Privacy Act, the Foreign Intelligence Surveillance Act, the Immigration and Nationality Act, the wiretap statute, and the Right to Financial Privacy Act.

Many of the changes have widespread support. These include new provisions amending federal money-laundering laws, particularly those involving overseas financial activities; creating new federal crimes for attacks on mass transportation facilities and use of biological weapons; toughening the penalties for existing federal crimes related to acts of terrorism; and authorizing new appropriations to enhance border security and to help law enforcement and intelligence agencies track and prevent terrorism.

On the other hand, some of the new Patriot Act provisions have come in for sharp criticism for threatening individual privacy and potentially abridging other basic constitutional rights. The most controversial changes are contained in Section II, which gives law enforcement and intelligence agencies a host of new surveillance powers. In addition, critics such as some members of Congress, immigrant groups, and the American Civil Liberties Union (ACLU) say changes to immigration law that make it easier to exclude and deport immigrants also are problematic. The specific portions of the Patriot Act that have caused the most alarm include:

- Amended federal criminal procedure rules that make it easier for law enforcement and intelligence agents to conduct secret searches of private homes and businesses without prior notice.

- Changes to national security laws that give government agents freer access to a wide range of personal records held by libraries, health insurance companies, bookstores, schools, and businesses and nonprofits.

- New wiretap provisions that give law enforcement authority to monitor personal Internet usage, including inbound and outbound e-mail traffic and sites visited on the Web.

- Changes to federal immigration laws that significantly expand the number of immigrants who can be denied entry or deported based on a broad new definition of "terrorist activity."

- Creation of a new crime category of "domestic terrorism" that some critics believe is broad enough to include groups such as the environmental group Greenpeace and the anti-abortion organization Operation Rescue.

II. Before the Patriot Act: Limits on Government Surveillance

Under the U.S. Constitution, American citizens are assured that they can go about their daily lives without fear of government intrusion. Specifically, the guarantee of privacy is supported by the Fourth Amendment, which promises that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."

The Fourth Amendment does give the government the necessary leeway, of course, to investigate criminal activity and maintain public safety. Yet, it also imposes strict limits on when and how law enforcement officials can conduct those investigations in order to protect the rights of ordinary, law-abiding citizens. Law enforcement officials seeking to search someone's home or business therefore must first obtain and present a court warrant. And to get a judge to issue it, they need to show that there is "probable cause" to believe a crime has been or is being committed. To guard further against open-ended government fishing expeditions, courts are required to define exactly what premises can be searched and how long the search period will last (if it is part of an ongoing undercover investigation) before issuing a warrant.

In recent decades, the federal courts have interpreted the Fourth Amendment's guarantee of privacy to cover private telephone communications—the idea being that citizens should be free to talk on the phone without fear that government agents are listening in. Under Title III of the Crime Control Act, Congress did allow government eavesdropping as part of a criminal investigation. Still, it required that officials first get a court order, based on probable cause, before any wiretap device or bug could be installed. At the same time, Title III tried to limit the extent of government intrusion. For example, law enforcement officials were required to make efforts to minimize eavesdropping on innocent parties. Phone taps and bugs were only to be permitted for investigations of specific, serious crimes—and then only for a prescribed period of time. The law ensured continuing judicial oversight by requiring law enforcement agents to report back to the court on the results of the wiretapping or bug. Moreover, it

required that a targeted suspect be notified at some future point that the surveillance had occurred.[3]

Federal law also gives the government authority to conduct a more limited kind of phone surveillance.[4] "Pen registers," as they are commonly known, collect the numbers of all outbound calls from a particular phone. Trap and trace devices record the numbers from which incoming calls originate. Since the actual content (conversation) of the calls is not captured, pen register and trap and trace monitoring is seen as less intrusive than other wiretaps. Therefore, while a court order is required before those devices can be installed, the government does not need probable cause. It merely has to certify that the information it obtains is "relevant to an ongoing criminal investigation."

Different Standards for National Security Threats

Those checks on government surveillance do not all apply when it comes to national security–related investigations. In 1978, Congress specifically created a separate set of laws governing foreign-intelligence gathering operations. The guiding principle behind the Foreign Intelligence Surveillance Act (FISA) was that, since foreign intelligence work is aimed at protecting national security and has no bearing on domestic law enforcement, the restrictions on government activities should be somewhat looser. Consequently, although government intelligence agents would still have to obtain warrants to conduct searches and wiretap phones, the traditional demand for some evidence of potential criminal activity was dropped. Rather, the principal requirements are a showing of "probable cause" that the surveillance target was the agent of a foreign power or a member of an international terrorist group, as well as government certification that the purpose of the surveillance is to obtain foreign intelligence information.[5]

Under FISA, the government submits warrant applications to a specially appointed panel of federal judges (see box, page 12). But FISA imposes minimal judicial control over the scope of those warrants, and once they are issued, the government is not required to report back to the court.

The Foreign Intelligence Surveillance Court

There is a good reason that the vast majority Americans have probably never heard of the Foreign Intelligence Surveillance Court. The special court conducts all of its proceedings in secret.

Of course, that was what Congress mandated when it originally established the court under the Foreign Intelligence Surveillance Act (FISA) in 1978. The court, which meets two days a month, was expanded under the Patriot Act to include eleven federal judges appointed by the Chief Justice of the U.S. Supreme Court. Under FISA, the Department of Justice is required to submit applications to the court for surveillance warrants related to foreign intelligence investigations. The Foreign Intelligence Surveillance Court's sole job is to review the Justice Department's requests.

Since the Foreign Intelligence Surveillance Court's records are sealed, little is known about how its decisions are made. But the information that is available shows that it only rarely rejects the Justice Department's applications. From 1979 to 2001, the court's records show, the judges approved all but five of the more than fourteen thousand warrant requests submitted. In 2002, the court granted all of the Justice Department's 1,228 surveillance applications. In 2003, the number of FISA warrant requests jumped to 1,727, according to the Justice Department, all but three of which were approved.[6] It also marked the first time that the total year-end number of secret surveillance warrants authorized by the court exceeded the number of wiretaps and electronic surveillance requests granted in conventional criminal cases. For 2003, federal and state courts nationwide approved a total of 1,442 wiretap and electronic surveillance warrants.

III. Surveillance: The Patriot Act and Its Repercussions

The Patriot Act provisions that have caused the most alarm relate to the expansion of government surveillance powers. Those new capabilities fall into several categories: secret searches, access to personal records, monitoring of Internet use, broadening the purview of the Foreign Intelligence Surveillance Act, and subpoena powers.

Section 213: Secret Searches

Federal courts have long held that the Fourth Amendment requires law enforcement officials to obtain a warrant to search someone's home or business. They also need to notify that person before they conduct the search. This requirement, known as "knock and announce," dates back through centuries of common law to the Magna Carta and is codified in U.S. federal criminal procedure rules. The courts did make some exceptions to the prior notice rule when evidence was likely to be destroyed or there was grave danger of physical harm, but those exceptions were only granted on a narrow, case-by-case basis.

The Patriot Act makes it far easier for law enforcement officials to get exceptions to the prior notice rule and conduct what are known as "sneak and peek" searches. Now government agents need simply show reasonable cause that immediate notification of a search "may have an adverse result" on a law enforcement matter, and the law allows a "reasonable period" for which notice can be delayed.

The Justice Department contends that giving law enforcement officials that extra time will allow them to gather evidence of terrorist activity without tipping off terrorists and will help them to make arrests before attacks occur. Critics of the new rules, however, point out that the government already had far broader powers to conduct clandestine searches against suspected terrorists under FISA, so it had no need for delayed notification authority for counterterrorism work.

They also make the point that the looser prior notice rules do not just apply to terrorism—they are now in effect for all law enforcement cases. And, unlike some of the other, more controversial provisions of the Patriot Act, they do not expire in 2005.

Under the new rules, civil liberties watchdogs predict that the number of private homes and businesses subjected to clandestine government searches will increase sharply. Prior notice has traditionally served as an important check on the government's power, they say, because it forces it to operate openly and allows targets of searches to challenge a warrant (say, if the police are at the wrong address) and to make sure that a search does not exceed the scope the warrant allows. Without notice, there is no way of knowing a warrant had even been issued or that your home had been searched until long after the search was completed. The looser prior notice rules, critics say, seriously undercut Fourth Amendment guarantees against unreasonable searches.

Section 215: Access to Personal Records

Even before the Patriot Act, the federal courts generally gave government leeway to gather personal information that had been voluntarily provided to banks, schools, and other third parties. But Congress did impose some safeguards. For instance, if law enforcement officials subpoenaed someone's checking account records as part of a domestic criminal investigation, the bank was required to notify the person targeted, who then had the right to challenge the subpoena before any information was turned over.[7]

While the rules were looser for foreign intelligence gathering, the government still had to certify to the Foreign Intelligence Surveillance Court that the person whose records were being sought was an agent of a foreign power. Even then, it could normally access a limited range of information, such as financial data and records from airlines, car rental agencies, and other travel-related businesses.

Under Section 215 of the Patriot Act, many of the checks on the government's ability to collect personal information for intelligence

purposes have been removed. Now, it is no longer only the personal records of suspected foreign agents that can be accessed. The government has the right to obtain the personal records of any citizen, as long as the information being sought is "part of an authorized investigation to protect the United States from international terrorism."

Requests for that subpoena power are made to the Foreign Intelligence Surveillance Court. Once this request is submitted, however, Section 215 explicitly states the court has no authority to reject it as long as the application is complete. So, in essence, judicial "oversight" is merely a formality.

Moreover, the types of third-party records the government can access are no longer limited to banking or travel-related businesses. The new rules permit the government to obtain information from any business, including credit card companies, video rental stores, HMOs, and booksellers, as well as libraries, schools, and other nonprofit institutions. Under the new rules, businesses and nonprofits are required to produce "any tangible thing" that the government believes will aid a terror-related investigation, including personnel files, medical and education records, and computer hard drives and disks. And businesses and nonprofits are prohibited from disclosing the government's request to the person whose records are being sought or to anyone else.

"Under the new rules, civil liberties watchdogs predict that the number of private homes and businesses subjected to clandestine government searches will increase sharply."

The new rules do make some attempt to prevent government overreach in that they explicitly bar searches of the records of U.S. citizens that are based solely on someone's practice of his or her First Amendment rights. For example, government agents cannot start demanding confidential information about someone simply for having written a letter to the editor slamming U.S. Attorney General John Ashcroft.

The Justice Department, meanwhile, has also tried to allay fears about the potential for abuse. It claims it has no interest in the shopping or reading habits of ordinary Americans. Rather, it says it intends to use its broader subpoena power to get information that might uncover terrorist plots, such as records from a hardware store or chemical plant where bomb-making material might be obtained.[8]

"Under Section 215 of the Patriot Act, many of the checks on the government's ability to collect personal information for intelligence purposes have been removed."

Nonetheless, there is widespread concern that the new provisions give the government far too much power to invade individual privacy rights—while permitting no meaningful judicial oversight. Despite the First Amendment safeguards, the new rules still allow the government to access records based (at least in part) on the political groups someone belongs to or the books and magazines that person reads (see box on the Patriot Act and libraries).

The "gag order" the new rules impose on business owners and other individuals who are compelled to turn over records has raised free speech concerns as well. Section 215 of the Patriot Act is scheduled to expire in 2005. The Justice Department contends it should be made permanent, while civil liberties groups are lobbying to phase it out.

Libraries and Section 215

No piece of the Patriot Act has caused a bigger public uproar than the rules pertaining to public libraries, which, like many other nonprofits, are now required to turn over records to government agents conducting terrorism-related investigations as part of Section 215.

The American Library Association has been particularly outspoken in its opposition to these rules, which it claims will discourage library patrons from checking out certain kinds of books and have a chilling effect on what people read. Many libraries around the country have taken steps to protect the privacy of their patrons. Some, for instance, have installed computer systems that erase a library user's borrowing record as soon as a book is returned. Others post signs warning patrons that their borrowing records and library Internet usage may be secretly inspected by government officials.

The Justice Department contends that it has no interest in the kinds of books ordinary Americans borrow. Yet, it also claims that terrorists and spies have used libraries in the past to plan and carry out activities that threaten national security, and it says the new rules are necessary to ensure that libraries do not serve as "terrorist safety zones."

Nevertheless, it is unclear to what extent government officials have actually used the new rules to obtain library records. One 2002 University of Illinois study found that 178 public libraries in the United States had received FBI visits in the first year after the Patriot Act passed. The Justice Department, however, has maintained that any requests for records were conducted in the course of criminal investigations and were not authorized under the new Patriot rules. According to a memo the Justice Department made public last September, the number of times Section 215 had actually been invoked to obtain library records was "zero."[9]

Section 216: New Powers to Monitor Internet Use

The rules for use of pen registers and trap and trace devices in phone surveillance were relatively loose even before the Patriot Act became law. Since those pen/trap devices only record the numbers dialed out and received at a particular phone, and not actual conversations, they were viewed as less an invasion of privacy than other wiretaps. Therefore, when law enforcement officials wanted a court order to install them as part of an ordinary criminal investigation, they simply needed to certify that the pen register or trap and trace were "relevant" to that investigation. The law did not require that the person whose phone was being monitored be a suspect in the matter, and law enforcement officials did not have to report back to the court on the results of the surveillance.

The Patriot Act expands the scope of what a pen/trap order can cover to include "dialing, routing, and signaling"—a change that allows the government to track Internet use as well. The law specifically states that the monitoring of "content of any communication" is prohibited. Thus, the body of incoming and outgoing e-mail messages would be off-limits to law enforcement officials under a pen/trap order.

Even so, civil liberties groups point out that logs of someone's e-mail and Web transmissions are far more revealing than just looking at phone numbers. With routing data, the government can learn what Web sites someone visited and what kinds of documents were downloaded while visiting those sites. That, Patriot Act critics say, is virtually the same as knowing what books someone checked out of a library or what movies they rented from the local video store.[10]

Another major change is that court orders covering pen/trap surveillance no longer just cover the jurisdiction in which they were issued. They can be used to monitor the phone and Internet traffic of a suspected criminal anywhere in the United States. Some Patriot Act opponents fear that change will further reduce the already limited oversight of pen/trap orders, since judges will have less ability to monitor surveillance operations that are being conducted in far-off jurisdictions.

The Justice Department counters that being able to get one nationwide order will save prosecutors valuable time because they will not have to apply for permission every time an investigation leads to new jurisdictions. It also contends that not only are rules prohibiting collection of content clear but the law requires the government to file annual reports on how the pen/trap statute is being used.

Even those who object to the new pen/trap rules concede that Internet surveillance could prove to be an essential tool in fighting terrorism. But, they also point out that the new pen/trap provisions do not apply just to counterterrorism investigations—they can be used to set up surveillance of phone and Internet traffic in any criminal investigation, even when there is no convincing evidence that laws are being broken. The sole requirement is that the information to be obtained may "be relevant to an ongoing criminal investigation."

"The new pen/trap provisions do not apply just to counterterrorism investigations—they can be used to set up surveillance of phone and Internet traffic in any criminal investigation, even when there is no convincing evidence that laws are being broken."

The new pen/trap provision contains no sunset clause and is therefore a permanent part of the law. Civil liberties advocates, however, maintain it should be either repealed or limited to cases where terrorism is actually suspected.

Section 218: Expanding the Reach of FISA

Before the Patriot Act, government agents focused on foreign intelligence matters already had relatively free rein to install clandestine wiretaps and conduct secret searches under FISA. But there was an important rationale for giving the foreign intelligence operations that extra latitude. Their work involved national security matters, not domestic law enforcement, and their surveillance targets were foreign powers or agents of foreign powers. Therefore, Congress reasoned, they should not have to show evidence of likely criminal activity to obtain a search warrant, as is normally required. Instead, the guiding rule was that "*the* purpose of the surveillance had to be to obtain foreign intelligence information" [emphasis added].

Under Section 218 of the Patriot Act, however, the wording of that rule changed. Now, to get search warrants under FISA, government agents simply have to certify that "*a significant purpose* of the surveillance is to obtain foreign intelligence information" [emphasis added].

While that change may appear fairly minor, it has caused considerable alarm. Because of it, in fact, Section 218 has actually become one of the most widely criticized portions of the Patriot Act. The new wording makes it far easier for the government to get search warrants under the looser FISA standards, even if the main purpose for the surveillance is to investigate a domestic criminal matter—intelligence gathering need only be a "significant" purpose of the investigation.

Consequently, one big fear is that government will be able to sidestep normal Fourth Amendment requirements for probable cause in ordinary criminal investigations where law enforcement otherwise might not have enough evidence that a crime is being committed to get a warrant. Once obtained, the FISA warrants now give law enforcement officials far freer range. Under new Patriot Act rules, FISA-authorized wiretaps of U.S. citizens can last up to ninety days (three times the period allowed in investigating domestic crime), and the time limit for clandestine searches of private homes (normally impermissible for domestic criminal investigations) has doubled—from forty-five to ninety days.

Another major concern centers on how information obtained under FISA's looser search standards can be used. Before the Patriot Act, the ability to share information uncovered in FISA-authorized searches with government prosecutors was strictly limited. Now, intelligence gleaned through FISA warrants can be more easily passed along for prosecution purposes.

The Justice Department contends that that the expanded information-sharing capability is vital to national security, in that it allows intelligence and law enforcement agents to work in concert to identify and arrest terrorists before they strike (see box, page 22). As a result, it is asking that Section 218, which is scheduled to expire in 2005, be made permanent. The Patriot Act's critics concede that, in the wake of September 11, some degree of coordination between the law enforcement and intelligence community is appropriate—especially, for example, if it helps uncover a terrorist weapons factory and foils a potentially catastrophic attack. But in their view, the new provisions do not contain sufficient safeguards to prevent government from using information gathered under the looser FISA standards to pursue and prosecute less urgent domestic crimes.

A Word Can Make a World of Difference

Changing the rule for obtaining search warrants from *"the* purpose of the surveillance had to be to obtain foreign intelligence information" to "*a significant purpose* of the surveillance is to obtain foreign intelligence information" may open a Pandora's box.

Breaking Down the Walls between Intelligence and Law Enforcement

To Patriot Act defenders, one of the law's greatest benefits has been to overturn the rules that inhibited the sharing of information between intelligence agencies and law enforcement officials and also impeded their ability to work in tandem to combat the terrorist threat. Now, law enforcement officials are expressly empowered to share foreign-intelligence-related information obtained during a wiretapping operation or a grand jury investigation with CIA and immigration officials, and the CIA is specifically permitted to team up with federal law enforcement officials on national security matters.

The Justice Department maintains that this sort of coordination has made it far easier to "connect the dots" in terrorism investigations—which is something that even the Patriot Act's opponents regard as invaluable. Even so, those critics note that the old restrictions on information-sharing were largely the result of administrative rules, and they argue that those rules could have been modified without easing the standards for foreign intelligence gathering, as Section 218 does.

There is no question that greater coordination between intelligence agencies and law enforcement is essential. But civil liberties advocates claim that the new provisions do not provide the necessary protections, such as ongoing court supervision, to prevent a repeat of the days when the CIA and FBI spied on thousands of law-abiding citizens because of their political views.

Section 505: National Security Letters

The government does not always need to get a court-sanctioned subpoena when it wants access to personal records held by third parties. Even before the Patriot Act, the Federal Bureau of Investigation had the power to issue what is known as a "national security letter" to compel banks, credit unions, and phone companies to turn over information on private citizens.

The rule, however, was that the government had to have "specific and articulable facts" that showed the person whose records they were seeking was an agent of a foreign power.[11] Under Section 505 of the Patriot Act that requirement was dropped. Now FBI agents can issue national security letters to obtain credit reports, bank and financial information, and telephone and e-mail logs, as long as that information is "relevant" to an authorized intelligence investigation. Even in the absence of a court order or grand jury subpoena, third-party holders of those records are required to produce them, and they are prohibited from disclosing the fact that the information was sought.

When the Patriot Act first went into effect, national security letters could only be used to get information from financial institutions, phone companies, and Internet service providers. But in a little-publicized change, Congress recently expanded the scope of Section 505 as part of an intelligence authorization bill. Under the new law, the FBI can issue national security letters to a much broader range of businesses, including travel agencies, real estate agents, the U.S. Postal Service, and even jewelry stores, casinos, and car dealerships. The only requirement is that the information the FBI is seeking be relevant to an intelligence investigation.[12]

Since the government claims that specific information about the use of national security letters is classified, it is impossible to know exactly

how many times they have been issued. Indeed, the only information available shows that between October 26, 2001, and January 2003, the government issued enough national security letters to fill five pages of logs. Those pages were obtained through a Freedom of Information Act lawsuit filed by the ACLU, the Electronic Privacy Information Center, and other groups. Still, the pages were almost entirely blacked out, so there were no hints about where the letters were directed or what sort of information the government sought.[13]

"Now FBI agents can issue national security letters to obtain credit reports, bank and financial information, and telephone and e-mail logs, as long as that information is 'relevant' to an authorized intelligence investigation."

Given the complete absence of judicial oversight, critics maintain the use of national security letters may pose an even more serious threat to privacy rights than the more widely publicized Section 215 provisions. The national security letter provision is scheduled to expire in 2005.

IV. Other Threats to Civil Liberties?

Beyond the changes related to surveillance, several other Patriot Act provisions have also raised civil liberties concerns.

Section 411: Denying Entry to Noncitizens Accused of Endorsing Terrorism

The Patriot Act dramatically increases the number of immigrants that can be denied entry or deported from the United States on terrorism grounds. Under the changes to federal immigration laws, the list of considerations that can be used to exclude noncitizens is longer and includes far broader definitions of the terms "terrorist activity," "engage in terrorist activity," and "representative of a foreign terrorist organization."

A "terrorist organization," for example, is construed to mean "any political, social, or other similar group whose public endorsement of acts of terrorist activity the Secretary of State has determined undermines United States efforts to reduce or eliminate terrorist activities."

The new provision threatens exclusion of not only those who provide "material support" for such organizations but anyone who offers "encouragement" as well. It also bars entry of immigrants who have "used their position of prominence in any country" to "endorse or espouse" terrorist activity.

Ignorance of the fact that a given group has been designated a "terrorist organization" is no excuse, even if it also engages in legitimate political and humanitarian activities. Under Section 411, a noncitizen who donated money to such a group could still be excluded for offering material support even if he or she was seeking only to support political or charitable efforts. Likewise, any alien who is deemed to have made statements in support of or to have contributed funds to "terrorist organizations," or who is associated with alleged members thereof, is subject to deportation.

Section 412: Indefinite Detentions of Noncitizens

Under the Patriot Act, the U.S. attorney general has new authority to order detentions based on a certification that there are "reasonable grounds to believe" that a noncitizen endangers national security. Aliens may be held for up to seven days without being charged with a crime. After that the attorney general must either bring criminal charges or initiate the process of deportation. If aliens do not have a country willing to accept them, they can be detained indefinitely without a trial. The only recourse available is a petition of habeas corpus to a federal court—which at best is considered an uphill avenue of appeal.

The Justice Department maintains that under this provision only a narrow class of noncitizens could be detained and that keeping them in detention is equivalent to holding a criminal defendant without bail. It also contends that the new immigrant detention rules are critical to ensure that "terrorists are not released to live among the people they are seeking to harm."

Still, this provision, together with the new exclusion rules in Section 411, has prompted a loud outcry from a broad range of civil liberties and human rights groups. The federal courts, they point out, have long recognized that even noncitizens have the right to basic constitutional protections. Holding immigrants indefinitely without trial is a clear denial of their right to due process, these advocates say, while excluding them from the United States based on the grounds that they espoused or otherwise supported a vaguely defined range of "terrorist activities" violates their First Amendment right to free association and free speech.[14] Both Section 411 and Section 412 are scheduled to expire in 2005.

Section 802: Domestic Terrorism: A New Federal Crime

As part of the antiterror agenda, the Patriot Act gives federal prosecutors new tools to go after U.S. citizens deemed to be engaged in suspect activity. Section 802 creates a new category of crime called

"domestic terrorism," which is broadly defined as "acts dangerous to human life that are a violation of the criminal laws of the United States" and that "appear to be intended . . . to influence the policy of a government by intimidation or coercion" and "occur primarily within the territorial jurisdiction of the United States."

Civil liberties advocates warn that such broad language opens the door to government abuse and poses a serious threat to First Amendment rights to free speech and political association. The government, they say, could easily use it as a license to launch investigations and surveillance operations against political activists and organizations based on their opposition to government policies. Moreover, they contend that the law could make even legitimate political dissent a federal crime. Civil disobedience and other confrontational forms of protest, by their very nature, could be interpreted as acts that "appear to be intended . . . to influence the policy of a government by intimidation or coercion" and that are "dangerous to human life." Indeed, critics claim that any group that uses direct action to advance a political agenda could conceivably fall within the law's broad sweep. That includes Greenpeace activists, anti-abortion protesters with Operation Rescue, and animal rights activists connected to People for the Ethical Treatment of Animals (PETA).[15]

"Civil liberties advocates warn that such broad language opens the door to government abuse and poses a serious threat to First Amendment rights to free speech and political association."

The Justice Department insists that such warnings are overblown. In its view the new law is narrowly defined to cover only actions that violate federal or state criminal laws and endanger human life. Therefore, peaceful groups that dissent from government policies without breaking laws have nothing to fear.

Other observers point out that the Justice Department has yet to use Section 802 to charge anyone with "domestic terrorism." Some believe the provision is more bark than bite. (For more on the implementation of the act, see the box below.) The counterargument is that, if so, there is no justifiable reason for such a law to be on the books, especially in light of the chilling effect it could have on free political activity and free speech. Section 802 is scheduled to expire in 2005.

Implementation of the Patriot Act

The Patriot Act does include certain safeguards to help ensure that government does not abuse its broad new powers. For instance, the Justice Department's inspector general is required to investigate public complaints of alleged civil liberties violations by FBI agents and other Department of Justice officials. And the inspector general must file semiannual reports to Congress on any instances of abuse.

Yet, there is little meaningful information available about how the Patriot Act is being used. The Justice Department has declared almost all specifics about implementation of its new surveillance powers classified on national security grounds, and it has provided information only in closed-door sessions or confidential correspondence with members of Congress. Given that, it is impossible to know exactly how many subpoenas the government has issued for personal records, how many times the new pen register/wiretap laws have been invoked, and what specific antiterrorism payoffs, if any, have resulted.

A bit more information was made public last spring on the use of Section 213 "sneak and peek" warrants. In a sixty-page response to queries by the House Judiciary Committee, the Justice Department said that as of April 2003 government

investigators had used the secret search warrants forty-seven times. It also reported seeking to extend the period of delay for notice of a search 248 times.[16] Without more information, it is difficult to know how or why such warrants were used. Still, Patriot Act opponents point out that the Justice Department's response to the committee clearly showed that at least some secret searches were used in run-of the-mill drug cases that were not related to terrorism.[17]

As for civil rights abuses stemming from the Patriot Act, the most recent report from the Justice Department inspector general uncovered no evidence of problems. That report, issued in January, noted that while 162 alleged civil rights violations by Justice Department employees had been reported, none were "related to their use of a substantive provision in the Patriot Act."[18]

Of course, some Patriot Act critics point out that many of the new provisions actually make it impossible for someone to know if his or her civil rights have been violated. Under the "sneak and peek" rules, for instance, citizens would never know if their homes had been searched or whether government agents had respected the scope of a search warrant. Likewise, the "gag orders" imposed under the new rules for record searches would prohibit a business owner who had been forced to turn over information from even bringing a complaint.

V. Post-Patriot: The Ongoing Debate

The Patriot legislation may not have inspired heated debate in Congress before it was passed. But opposition to many portions of the act has continued to mount since the bill became federal law. Indeed, over the past two years, right-wing anti-abortion and gun rights groups have joined forces with liberal citizens' watchdog groups and have been working together on multiple fronts to amend or repeal key sections of the law.

Grassroots Mobilization against the Patriot Act

Dozens of communities across the country have registered protests against the Patriot Act. As of June 2004, more than 325 cities and towns and four states had passed Civil Liberties Safe Zones resolutions calling for a rollback of the sections of the law that most intrude on basic civil liberties. Many communities also have passed new local ordinances to protect the privacy of their citizens. These measures have won support not only in liberal strongholds such as Berkeley, California, and Burlington, Vermont, but in small towns in Utah, Idaho, and Alaska, three of the most conservative states in the Union.

The Fight in the Federal Courts

Opponents are asking the federal judiciary to strike down portions of the Patriot Act as unconstitutional. In July 2003, the ACLU filed the first lawsuit challenging the new Section 215 rules that give government access to third-party records. The suit claims that Section 215 violates privacy and First Amendment rights and was filed on behalf of an Arab-American civil rights group and other organizations that claim they were targeted for investigations because of their ethnic, religious, and political associations. Another federal suit filed last year challenges the Patriot Act provision that makes it a crime to provide "expert advice and assistance" to groups designated as "terrorist" by

the secretary of state. Earlier this year a federal judge in Los Angeles agreed that on that point the law was "impermissibly vague" and struck down that portion of the Patriot Act.[19] The Justice Department is expected to appeal the decision.

The Fight in Congress

Many members of Congress who originally voted for the Patriot Act have had second thoughts. Currently, nearly a dozen different bills designed to roll back specific sections of the Patriot Act have been introduced in the House and Senate. The most comprehensive new measure is the Security and Freedom (SAFE) Act, which has strong bipartisan backing. The SAFE Act does not repeal any section of the Patriot Act but instead attempts to narrow some of the most far-reaching provisions, the better to protect individual privacy and limit the potential for government abuse.

Among other things, the SAFE Act would impose new limits on "sneak and peek" searches; would amend rules on access to third-party records to require the government to show "articulable suspicion" that the information it is seeking relates to a spy, terrorist, or other foreign agent; and would mandate that four additional sections of the Patriot Act expire in 2005, so that they will be part of the review when Congress considers whether to extend the sunset.[20]

President Bush has already vowed to veto the SAFE Act if it passes Congress. The president continues to argue that all of the Patriot Act provisions scheduled to expire in 2005 are necessary to the government's counterterrorism efforts and should be made permanent.

Last year, the Bush administration had planned to send Congress an even broader package of proposed antiterrorism legislation, known as Patriot II, but after widespread protests it abandoned that effort. The administration's allies in Congress, however, have since introduced some of the measures proposed in Patriot II as individual bills. There are currently at least half a dozen bills before Congress to expand the Patriot Act. Among other things, they would give the government even more freedom to access personal records and would allow it to

use many of the new powers it has under the Patriot Act in the war on drugs.

With the administration and some members of Congress pushing to extend the Patriot Act, and with the law's opponents in Congress and elsewhere working to roll it back, one thing seems certain: the Patriot Act will be at the center of a critical public debate over the proper balance between civil liberties and national security in the months ahead.

"Currently, nearly a dozen different bills designed to roll back specific sections of the Patriot Act have been introduced in the House and Senate. The most comprehensive new measure is the Security and Freedom (SAFE) Act, which has strong bipartisan backing."

NOTES

1. *USA Today*/CNN/Gallup poll data, February 2004, available online at http://www.usatoday.com/news/polls/tables/live/2004-02-25-patriot-act-poll.htm.

2. *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001,* Public Law 107-56, U.S. Statutes at Large 115 (2001): 272, available online at http://www.c-span.org/pdf/patriotact.pdf.

3. Title III of the *Crime Control Act,* U.S. Code 18 1968, §§ 2501 et seq.

4. Federal criminal procedure rules for pen register and trap and trace devices can be found at U.S. Code 18, § 3123.

5. *Foreign Intelligence Surveillance Act,* U.S. Code 50 (1978), § 1801.

6. Figures for Foreign Intelligence Surveillance Court approval of warrants from 1979 to 2001 come from Stephen J. Schulhofer, "No Checks, No Balances: Discarding Bedrock Constitutional Principles," in *The War on Our Freedoms: Civil Liberties in an Age of Terrorism,* ed. Richard C. Leone and Greg Anrig, Jr. (New York: PublicAffairs, 2003), p. 81. The 2003 Foreign Surveillance Act annual report and the 2002 Foreign Surveillance Act annual report are available online at http://www.fas.org/irp/agency/doj/fisa. The statistics for the total number of federal wiretap and electronic surveillance orders come from the Administrative Office of the United States Courts in its "2003 Wiretap Report," available online at http://www.uscourts.gov/wiretap03/2003WireTap.pdf.

7. Laws Congress passed to protect the confidentiality of information held by third parties include the *General Education Provisions Act,* U.S. Code 20, § 1232g; the *Bank Secrecy Act,* U.S. Code 12 (1970), §§ 1951 et seq.; and the *Right to Financial Privacy Act,* U.S. Code 12 (1978), § 3401.

8. Statements attributed to the Justice Department can be found on the department's Web site about the Patriot Act, available online at http://www.lifeandliberty.gov. See especially "Dispelling the Myths," U.S. Department of Justice, n.d., available online at http://www.lifeandliberty.gov/subs/u_myths.htm.

9. The American Library Association has posted an analysis of how Section 215 of the Patriot Act affects libraries, "The USA Patriot Act in the Library," American Library Association, Chicago, April 2002, available online at http://www.ala.org/ala/oif/ifissues/usapatriotactlibrary.htm.

More information on the survey can be found in Leigh Estabrook et al., "Public Libraries and Civil Liberties: A Profession Divided," Library Research Center, Graduate School of Library and Information Science, University of Illinois at Urbana-Champaign, n.d., available online at http://lrc.lis.uiuc.edu/web/PLCL.html. The Justice Department memorandum was widely circulated to the press on September 17, 2003, and received extensive news coverage. See Dan Eggen, "Patriot Monitoring Claims Dismissed; Government Has Not Tracked Bookstore or Library Activity, Ashcroft Says," *Washington Post,* September 19, 2003, p. A2; Eric Lichtblau, "U.S. Says It Has Not Used New Library Records Law," *New York Times,* September 19, 2003, p. A20.

10. The American Civil Liberties Union has put together a detailed analysis of the pen register and trap and trace provisions and other expanded government surveillance powers under the Patriot Act. That analysis and other information related to the Patriot Act is posted on the "Safe and Free" page of the Web site for the American Civil Liberties Union, New York, n.d., available online at http://www.aclu.org/SafeandFree.

The ACLU is not alone in urging Congress to amend or repeal the pen register and trap and trace provisions, along with other pivotal sections of Patriot Act. Other groups that have expressed similar reservations about these provisions include the Center for Democracy and Technology (http://www.cdt.org); the Electronic Frontier Foundation (http://eff.org); and the Electronic Privacy Information Center (http://www.epic.org). For further analysis of the pen register provision, see also Stephen J. Schulhofer, *The Enemy Within: Intelligence Gathering, Law Enforcement, and Civil Liberties in the Wake of September 11* (New York: The Century Foundation Press, 2002), pp. 39–40.

11. The authorization is in the *Right to Financial Privacy Act,* § 3414.

12. The provision expanding the FBI's power to issue National Security Letters was contained in the *Intelligence Authorization Act for Fiscal Year 2004,* HR 2417, 108th Cong., 1st sess., *Congressional Record* 149, no. 95 (June 25, 2003): H 5870-5881, which was signed into law by President Bush on December 13, 2003.

13. The "Safe and Free" page of the ACLU's Web site contains information on the Freedom of Information Act suit, as well as a link to the redacted list of National Security Letters issued by the FBI, available online at http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=15543&c=262.

14. The Center for Constitutional Rights and Human Rights First have been especially critical of the portions of the Patriot Act pertaining to immigrants. More of their analysis of Section 411 and 412 is available on the Center for Constitutional Rights Web site at http://www.ccr-ny.org, and on the Human Rights First Web site at http://www.humanrights first.org.

15. Both the American Civil Liberties Union and the Center for Constitutional Rights have raised concerns about the potential chilling effect of the domestic terrorism provision. For more information on their objections to Section 802, visit their Web sites at www.aclu.org for the ACLU and http://www.ccr-ny.org for the Center for Constitutional Rights.

16. Letter from Jamie E. Brown, acting assistant attorney general, U.S. Department of Justice, to F. James Sensenbrenner, Jr., chairman, and John Conyers, Jr., ranking minority member, Committee on the Judiciary, U.S. Congress, House of Representatives, responding to questions about implementation of the Patriot Act by the House Judiciary Committee, May 13, 2003, pp. 10, 13, available online at http://www .house.gov/judiciary/patriotlet051303.pdf.

17. Ibid., p. 27.

18. "Semiannual Report to Congress," Office of the Inspector General, Department of Justice, October 1, 2003–March 31, 2004, available online at http://www.usdoj.gov/oig/semiannual/0405/final.pdf.

19. The ACLU case is *Muslim Community Association of Ann Arbor et al. v. John Ashcroft et al.*, CV no. 03-72913, 2003 U.S. Dist. (E.D. Mich., Southern Div., July 30, 2003). For more information on this suit, go to the "Safe and Free" page of the ACLU Web site, available online at http://www.aclu.org/SafeandFree. On August 27, 2003, the Center for Constitutional Rights filed *Humanitarian Law Project et al. v. Ashcroft*, CV no. 03-6107 ABC, 2004 U.S. Dist. LEXIS 926 (C.D. Calif., January 23, 2004).

20. A Congressional Research Service summary of the SAFE Act is available online at http://thomas.loc.gov/cgi-bin/bdquery/z?d108:HR033 52:@@@D&summ2=m&. For information on other congressional action related to the Patriot Act, see the "Legislation" page of the Web site for the Bill of Rights Defense Committee, Northampton, Mass., last updated June 30, 2004, available online at http://www.bordc.org/legislation .htm.

Browsing the Web?

Visit The Century Foundation's Web site featuring other pamphlets in this series; excerpts from current books, papers, and reports; and information about the Foundation and how to order its publications.

You can find us at:
www.tcf.org

You can also contact us through our e-mail address:
info@tcf.org

Of course, we can also be reached by U.S. post or phone:

The Century Foundation
41 East 70th Street
New York, New York 10021

212-535-4441