The Patriot Act Gives the FBI Unchecked Power to Spy on Ordinary Citizens

Are Privacy Rights Being Violated?, 2006

The American Civil Liberties Union works in courts, legislatures, and communities to defend and protect the individual rights and liberties guaranteed by the Constitution and laws of the United States.

After the terrorist attacks of September 11, 2001, Congress passed the USA PATRIOT Act. Several provisions of the act give the Federal Bureau of Investigation (FBI) unprecedented powers to violate privacy rights guaranteed by the U.S. Constitution. The part of the act known as Section 215, for example, gives FBI agents the right to look at people’s medical records, read their e-mails, check out the Web sites they have visited, investigate their religious affiliations, and even see which books they have checked out of the library. People forced to turn over these personal records, such as librarians and doctors, are required by law to tell no one—ever—under threat of felony prosecution. Section 215 might be used to catch suspected terrorists, but it could also be used against protesters, political enemies, or anyone else. The FBI has a well-documented history of abusing its authority, dating back to the 1950s. While the threat of terrorism is real, giving unchecked powers to secret government investigators is no way to stop it.

Imagine this scenario: You flee Iraq after being imprisoned and persecuted for your political views. When you arrive in the United States, a local charity helps you find housing and medical care. You start a small business, join a mosque, and become active in a Muslim community association. You use email at a public library to keep in touch with your extended family in Iraq, and to discuss politics with friends. Two years later, you are grateful for the freedoms you enjoy in your new home.

When the U.S. invades Iraq, you are thankful to be rid of Saddam but angry about civilian casualties and the extended U.S. occupation. You write a letter to the editor of your local newspaper encouraging a quick transfer of power to Iraqi civilians.

An FBI agent who is conducting an investigation of other Iraqi-Americans notices your letter and finds it troubling. Based on the letter, the sound of your name, and the outside possibility that you may be connected to the people he’s investigating, he decides to investigate you. He goes to a secret court and gets an order that forces the library and its Internet service provider to turn over all your email messages. Then he gets another secret order to obtain records from the charity that helped you when you first arrived in the United States. Those records lead him to the local hospital, where he obtains records of medical treatment you received. He serves another order on the local mosque to find out whether or not you’re a member or serve in a leadership position. Though he uncovered nothing suspicious about you in his fishing expedition, he gets another secret order forcing the Muslim community association to turn over its entire membership list. If not you, he thinks, maybe another member has some connection to those people he’s investigating....

As it turns out, you never learn that the FBI is spying on you. The FBI certainly doesn't tell you. And the library, the charity, the hospital, the mosque, and the community association are all prohibited—forever—from telling you or anyone else that the FBI has asked for your records. You simply never learn that the government has been
rifling through your life.

Could such a thing happen to you or someone you know? Perhaps it already has. The USA PATRIOT Act vastly expands the FBI’s authority to monitor people living in the United States. These powers can be used not only against terrorists and spies but also against ordinary, law-abiding people—immigrants from Iraq or Italy, dentists from Detroit or Denver, truck drivers from Tampa or Tulsa, painters from Peoria or Pittsburgh. Indeed, the FBI can use these powers to spy on any United States citizen or resident.

This report examines in detail one PATRIOT Act provision, Section 215, which gives the FBI unprecedented access to sensitive, personal records and any "tangible things." The report explains why Section 215 is misguided, dangerous, and unconstitutional....

**Vastly Expanding FBI Powers**

Section 215 vastly expands the FBI’s power to spy on ordinary people living in the United States, including United States citizens and permanent residents. It lets the government obtain personal records or things about anyone—from libraries, Internet service providers, hospitals, or any business—merely by asserting that the items are “sought for” an ongoing terrorism investigation. Section 215 threatens individual privacy, because it allows the government free reign to monitor our activities. It also endangers freedom of speech, because the threat of government surveillance inevitably discourages people from speaking out—and especially from disagreeing with the government.

Section 215 amends an obscure law called the Foreign Intelligence Surveillance Act (FISA), which became law in 1978. FISA set out the procedures that the FBI had to follow when it wanted to conduct surveillance for foreign intelligence purposes. The system is extraordinary—not least because the FISA Court meets in secret, almost never publishes its decisions, and allows only the government to appear before it. But of course it applied only to foreign spies. Thanks to the PATRIOT Act, the FBI can now use FISA even in investigations that don’t involve foreign spies. In fact, under Section 215 the FBI can now spy on ordinary, law-abiding Americans.

To obtain your personal records or things under Section 215, the FBI does not need to show "probable cause"—or any reason—to believe that you have done anything wrong. It does not need to show that you are involved in terrorism, directly or indirectly, or that you work for a country that sponsors terrorism. If you are a United States citizen or permanent resident, the FBI can obtain a Section 215 order against you based in part on your First Amendment activity—based, for example, on the books that you borrowed from the library, the Web sites you visited, the religious services you attended, or the political organizations that you joined. If you are not a citizen or permanent resident, the FBI can obtain a Section 215 order against you based solely on your First Amendment activity.

In fact, Section 215 authorizes federal officials to fish through personal records and belongings even if they are not investigating any person in particular. Under Section 215, the FBI could demand a list of every person who has checked out a particular book on Islamic fundamentalism. It could demand a list of people who had visited a particular Web site. It could demand a client list from a charity that offers social services to immigrants.

A gag order in the law prevents anyone served with a Section 215 order from telling anyone else that the FBI demanded information. Because the gag order remains in effect forever, surveillance targets—even wholly
innocent ones—are never notified that their privacy has been compromised. If the government uses Section 215 to keep track of the books you read, the Web sites you visit, or the political events you attend, you will simply never know.

The FBI Can Demand Any Records

There is no restriction on the kinds of records or things that the FBI can demand under Section 215. Before the PATRIOT Act, the FBI's authority under this provision was restricted to a discrete category of business records—records from vehicle rental agencies, storage facilities and other similar businesses. Section 215 expands this authority to reach "any tangible things (including books, records, papers, documents, and other items)," held by any organization or person. The FBI could use Section 215 to demand:

- personal belongings, such as books, letters, journals, or computers, directly from one's home.
- a list of people who have visited a particular Web site.
- medical records, including psychiatric records.
- a list of people who have borrowed a particular book from a public library.
- a membership list from an advocacy organization like Greenpeace, the Federalist Society, or the ACLU.
- a list of people who worship at a particular church, mosque, temple, or synagogue.
- a list of people who subscribe to a particular periodical.

In fact, the [former] Attorney General [John Ashcroft] himself has acknowledged that the FBI could use the law even more broadly. The following exchange between the Attorney General and Rep. Tammy Baldwin (D-WI) took place before the House Judiciary Committee in June 2003:

BALDWIN: Prior to the enactment of the USA PATRIOT Act, a FISA order for business records related only to common carriers, accommodations, storage facilities and vehicle rentals. Is that correct?

ASHCROFT: Yes, it is....

BALDWIN: OK. Now, under section 215 of the USA PATRIOT Act, now the government can obtain any relevant, tangible items. Is that correct?

ASHCROFT: I think they are authorized to ask for relevant, tangible items.

BALDWIN: And so that would include things like book purchase records?

ASHCROFT: ... [I]n the narrow arena in which they are authorized to ask, yes.

BALDWIN: A library book or computer records?

ASHCROFT: I think it could include a library book or computer records....

BALDWIN: Education records?
ASHCROFT: I think there are some education records that would be susceptible to demand under the court supervision of FISA, yes.

BALDWIN: Genetic information?

ASHCROFT: ... I think [we] probably could.

**Section 215 Violates the Constitution**

Section 215 violates the United States Constitution. It violates privacy and due process rights guaranteed by the Fourth Amendment, and free speech rights guaranteed by the First Amendment.

*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause....*

- Section 215 violates the Fourth Amendment by allowing the government to search and seize your personal records or belongings without a warrant and without showing probable cause.

The Fourth Amendment ordinarily prohibits the government from searching your home or office, or from seizing your records, unless it first obtains a warrant based on "probable cause" to believe that you are engaged in criminal activity. The Supreme Court has applied this protection not just to physical objects but to personal records and electronic data. Section 215 does not require the government to obtain a warrant or to establish probable cause before it demands your personal records or belongings. In fact, the FBI can use Section 215 against you even if it knows for a fact that you are not engaged in crime or espionage.

- Section 215 also violates the Fourth Amendment because it does not require the government to provide you with notice—ever—that your records or belongings have been seized.

Ordinarily the Constitution requires that the government notify you before it searches or seizes your records or belongings. Indeed, the Supreme Court has held that this "knock and announce" principle is at the core of the Fourth Amendment's protections; without notice, after all, a person whose privacy rights have been violated will never have an opportunity to challenge the government's conduct. While in some circumstances delayed notice is permitted to protect against the destruction of evidence, the Supreme Court has *never* upheld a government search for which notice is never provided.

*Congress shall make no law ... abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.*

- Section 215 violates the First Amendment because it allows the government to easily obtain information about, for example, the books you read, the Web sites you visit, and the religious institutions you attend.

Section 215 expressly authorizes the government to obtain books, records, and other items that are protected by the First Amendment. The FBI could use Section 215 to order a library or bookstore to produce records showing that you had borrowed or bought a particular book. It could force an Internet Service Provider to turn over your email messages or records of which Web sites you've visited. It could demand that a political organization confirm that you participated in a political rally. It could even order a mosque to provide a list of all its members.
The Constitution’s warrant and probable cause requirements protect First Amendment interests by prohibiting the government from spying on people based solely on their political views or religious associations. In a 1972 case involving electronic surveillance, the Supreme Court wrote:

> History abundantly documents the tendency of Government—however benevolent and benign its motives—to view with suspicion those who most fervently dispute its policies. Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs.

Section 215 is likely to chill lawful dissent. If people think that their conversations, their emails, and their reading habits are being monitored, people will feel less comfortable saying what they think—especially if they disagree with government policies. Indeed, there is a real danger that the FBI will wield its Section 215 power specifically to silence dissenters.

- Section 215 also violates the First Amendment by preventing those served with Section 215 orders from ever telling anyone that the FBI demanded information, even if the information is not tied to a particular suspect and poses no risk to national security.

Section 215 prohibits people who receive orders for personal records or belongings from disclosing that fact to others even where there is no real need for secrecy. The gag order is extremely broad. It prevents people from even telling the press and public that the government has sought records, even if the statement is made in the most general terms, without identifying the specific target of the order. For example, it would prevent a library from publicizing statistics about the number of times the FBI had sought patron records in a given time period. To ensure compliance with the gag order, individual employees served with Section 215 orders must strictly limit telling even their fellow staff members that the FBI has demanded information.

Section 215 gag orders are automatic, and do not require the government to explain to the judge why secrecy is necessary. In other contexts, gag orders are imposed only where the government has made a showing that secrecy is necessary in the particular case. Section 215 gag orders are also indefinite, which means that surveillance targets—even wholly innocent ones—will never know their privacy was compromised. In certain investigations, secrecy may sometimes be necessary, and short-term gag orders may sometimes be unavoidable. But Section 215 gag orders require no necessity and are unlimited. If the First Amendment means anything, it means that the government cannot impose an indefinite gag order without reference to the facts of the particular case.

### Targeting Innocent People

Section 215 was specifically intended to authorize the FBI to obtain information about innocent people—people who are not engaged in criminal activity or in espionage. Of course, not all innocent people are likely to be equally affected. As it has done in the past, the FBI is once again targeting ethnic, political, and religious minority communities disproportionately. In the war on terrorism, the FBI has unfairly targeted minority and immigrant communities with its surveillance and enforcement efforts. The FBI and the Immigration and Naturalization Service (INS) rounded up over a thousand immigrants as "special interest" detainees, holding many of them without charges for months. A “Special Registration” program now requires tens of thousands of Arab and Muslim immigrants to submit to a call-in interview from which other immigrants are exempted. During the war in Iraq, many Iraqis and Iraqi-Americans were asked to submit to "voluntary" interviews with the FBI. And a Jan. 28,
2003 New York Times article by Eric Lichtblau ("F.B.I. Tells Offices to Count Local Muslims and Mosques") reported that the FBI ordered its field offices to "establish a yardstick for the number of terrorism investigations and intelligence warrants" by counting the number of Muslims and mosques in their districts.

There is little doubt, then, that Section 215 is being used against minorities and immigrants disproportionately. This doesn't make us any safer, of course. (It bears noting, for example, that none of the immigrants whom the FBI and INS held as "special interest" detainees was charged with a terrorism-related offense.) Indeed, targeting minorities and immigrants simply because of their ethnicity, religion, or nationality wastes resources that could be dedicated to apprehending real terrorists.

In fact, the FBI does not need the PATRIOT Act to investigate people who are legitimately suspected of engaging in terrorist or criminal activity; it has always had this power. Nor does the FBI need the PATRIOT Act to engage in surveillance of people who are legitimately suspected of spying for foreign governments or terrorist groups; it has had this power since 1978. The government can use these powers—powers that predate the PATRIOT Act—to vigorously pursue terrorists and other criminals, consistent with the Constitution.

Further Readings
Books
- Frederick S. Lane The Naked Employee: How Technology Is Compromising Workplace Privacy. New York:


**Periodicals**


- Andrew Goldstein "Mr. Quarantine, Meet Miss Liberty," *Time*, April 8, 2002.


- Steven Levy "Can Snooping Stop Terrorism? A Data-Mining Initiative Requires Openness and Unimpeachable Leadership. The Department of Defense's TIA Flunked on Both Counts," *Newsweek*, October


• Sharlene A. McEvoy "E-mail and Internet Monitoring and the Workplace: Do Employees Have a Right to Privacy?" *Communications and the Law*, June 2002.


• Nina Riccio "To Test or Not to Test? Random Drug Testing: Is It a Valuable Tool or a Personal Violation?" *Current Health 2*, March 2003.


**Full Text:** COPYRIGHT 2006 Gale.

**Source Citation:**

Document URL
http://ic.galegroup.com/ic/ovic/ViewpointsDetailsPage/ViewpointsDetailsWindow?di splayGroupName=Viewpoints&disableHighlighting=true&prodId=OVIC&action=e&windowstate=normal&catId=documentId=GALE%7CEJ3010365214&mod e=view&userGroupName=atascocitahs&jsid=446503fe240bad2b3486eaac28a5930d

**Gale Document Number:** GALE|EJ3010365214