Everyone's heard of the Patriot Act. Here's what it actually does.

Dara Lind

June 2, 2015

The Patriot Act has become a symbol of the massive expansion of government surveillance after 9/11. So if you're concerned about excessive government surveillance, or if you've ever talked with someone who is, you've probably heard or used "the Patriot Act" as a shorthand for the problem.

That's not exactly right. The Patriot Act was a big, broad law, and a lot of it has nothing to do with surveillance. And the government's current surveillance powers are drawn from some parts of the Patriot Act, but also from other laws.

The current fight in Congress over surveillance programs has led to a lot of confusion about whether "the Patriot Act has expired." It hasn't; most of the Patriot Act is permanent. But three of the many, many individual provisions within the law expired, or "sunsetted," at the end of May 2015. The most significant of these is Section 215, which the government used to justify the National Security Agency's controversial phone records program.

But other controversial programs remain in effect. And ultimately, the expiration of three Patriot Act provisions will have only modest effects on the government's spying powers. Here's what you need to know about the original Patriot Act, the three expired provisions within it, and the other ways the government can collect Americans' information.

What is the Patriot Act?

Just weeks after the attacks of September 11, 2001, Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act — the USA PATRIOT Act. (Over the course of the bill's existence, most journalistic outlets have given up on the all-caps "PATRIOT" because it's dumb and looks like something out of the Marvel Cinematic Universe.)

The bill passed overwhelmingly. Only one senator (Russ Feingold of Wisconsin) voted against it.

The Patriot Act covered a lot of ground. Some of its provisions have since been struck down by the courts (the Supreme Court has ruled that it's illegal to indefinitely detain immigrants who aren't charged with crimes, for example); others have become part of the mission of the Department of Homeland Security, which didn't exist when the law was passed. Others have stuck around and aren't the subject of a lot of controversy: the law created a slew of new federal crimes related to terrorism, created federal funds to assist victims of terrorism, and gave the federal government a range of new powers to track and seize money being used by organizations connected to terrorism.

But what "Patriot Act" tends to mean to most Americans — and the reason the parts of the bill that need to be renewed by Congress have faced increasing opposition over the past several years — is several provisions that made it much easier for the government to collect millions of Americans' communications records.

Why are some parts of the Patriot Act expiring?

Back when the Patriot Act was first being debated, Sen. Ron Wyden (D-OR) was worried about some of the powers the Patriot Act was giving the federal government. He voted for the bill, but not before adding a five-year countdown clock to three of the sketchiest-looking provisions. After five years, if Congress hadn't passed a new law renewing the programs, they would "sunset." Wyden hoped "these provisions would be more thoughtfully debated at a later, less panicked time."

Waiting for a less panicked time.

In 2006, there was a little more "thoughtful debate" — including a filibuster, led by Feingold, that caused senators to tweak the surveillance provisions slightly. By 2011, though, Ron Wyden was on the Senate floor warning that there was a "secret Patriot Act": that the federal government secretly believed the law allowed it to conduct way more surveillance of Americans than people assumed. Despite Wyden's warnings, Congress passed a four-year extension — which reset the countdown clock for May 31, 2015.

What did the expired parts of the Patriot Act actually do?

The parts of the law that expired at the end of May cover three of the most controversial programs for domestic and international surveillance.

The one you're most likely to have heard of is Section 215, which is officially called the "business records" provision — it gives the government broad power to ask businesses for their records relating to someone who might be involved in terrorism. For example, if the FBI had been tracking Timothy McVeigh before the Oklahoma City bombing, it might have learned from business records that he'd rented a truck and bought a truckload of fertilizer.

When the Patriot Act was first passed, 215 came under some mild criticism because of fears that the government could force public libraries to turn over someone's borrowing records. (Remember libraries?) But in 2013, documents leaked by former government contractor Edward Snowden revealed that the government had been collecting the phone records of every single customer of phone companies including Verizon. And it was using Section 215 as the justification that made it legal.

The Snowden leaks put Section 215 at the center of a renewed controversy about government surveillance of Americans — which ultimately led to the current legislative fight. But two other, less discussed provisions have also expired.

The "roving wiretap" provision (Section 206) allows the government to tap every device a person uses — landline, cell phone, laptop, etc. — with just one approval from the (famously permissive) Foreign Intelligence Surveillance Court. And the "lone wolf" provision (Section 207) allows the government to surveil someone who might be engaged in international terrorism, even if he or she is not actually connected to any existing terrorist group.

Have any of these provisions actually prevented terrorist attacks?

The Obama administration says that Section 215, in particular, has been extremely helpful in terrorism investigations. But when the government's Privacy and Civil Liberties Oversight Board reviewed the program in January 2014, that is ... not what it found (emphasis added):

Where the telephone records collected by the NSA under its Section 215 program have provided value, they have done so primarily in two ways. The first is by offering additional leads regarding the contacts of terrorism suspects already known to investigators, which can help investigators confirm suspicions about the target of an inquiry or about persons in contact with that target. But our review suggests that the Section 215 program offers little unique value here, instead largely duplicating the FBI's own information-gathering efforts. The second is by demonstrating that known foreign terrorism suspects do not have U.S. contacts or that known terrorist plots do not have a U.S. nexus. [...]

We have not identified a single instance involving a threat to the United States in which the telephone records program made a concrete difference in the outcome of a counterterrorism investigation. Moreover, **we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack.** And we believe that in only one instance over the past seven years has the program arguably contributed to the identification of an unknown terrorism suspect. In that case, moreover, the suspect was not involved in planning a terrorist attack and there is reason to believe that the **FBI may have discovered him without the contribution of the NSA's program.**

There's less information about the other two provisions. Section 207, for example — the "lone wolf" program — has apparently never even been used.

Are these the only controversial parts of the Patriot Act?

Hardly. They're just the ones that Congress put the countdown clock on when it passed the original law. In the 15 years since the Patriot Act has passed, Congress and the public have realized that the federal government is using all sorts of provisions to justify surveillance.

The most controversial permanent program under the Patriot Act is the "National Security Letters" program, which lets the government demand communications records from telecom companies without even going through the surveillance court for approval first.

National Security Letters have been used extremely broadly, and some privacy advocates have pointed out that they could simply replace some of the powers the government lost at the end of May. As Julian Sanchez of the Cato Institute wrote last month:

the FBI didn't even bother using 215 for more than a year after the passage of the Patriot Act.[...] In at least one case, when the secret court refused an application for journalists' records on First Amendment grounds, the Bureau turned around and obtained the same data using National Security Letters.

And the Patriot Act isn't the only law that has led to problematic surveillance programs:

What is the USA Freedom Act?

Most members of Congress who want to scale back government surveillance have decided that the best way to fix the Patriot Act is to let surveillance programs continue but put serious restrictions on how they can be used. That's the purpose of the USA Freedom Act. (Its official name is the USA FREEDOM Act: Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection, and Online Monitoring Act. That is even stupider than the USA PATRIOT Act and sounds like something out of *Team America: World Police.*)

The USA Freedom Act would force the government to ask the Foreign Intelligence Surveillance Court for approval before being able to access phone records, and would only give it access for specific searches — not just passive bulk collection of everyone's data.

Furthermore, the Freedom Act tackles National Security Letters — it would hold them to the same standards that requests under Section 215 meet, so that the government couldn't use the letters to get data they were banned from getting through the courts. And it would force the surveillance court — which currently operates completely in secret — to publish data about its major decisions.

Other privacy advocates, including Sen. Rand Paul (R-KY), oppose the USA Freedom Act because it would allow some surveillance under Section 215. They'd prefer to see collection of phone records end entirely, and think that simply not renewing the Patriot Act provisions and not replacing them with a new bill is the best way to do that. Other advocates disagree, using National Security Letters as an example of how the government can just use other routes to get the same amount of data.