



# What happens if parts of the Patriot Act really expire?

By [Kevin Collier](#)

May 28, 2015

It's coming down to the wire.

Hyper-aware that a key provision of the controversial [USA Patriot Act, Section 215](#), is set to expire at midnight June 1, the Senate last week pulled a marathon, confusing near all-nighter that ended in the wee hours of Saturday morning.

Section 215, best known as the authority behind the [NSA](#)'s most infamous domestic spying program—the very first of [Edward Snowden](#)'s leaked revelations—will no longer be used to collect Americans' phone records in bulk. That specific program is by all accounts doomed: The U.S. Department of Justice ([DOJ](#)) told the National Security Agency to [start winding the program down](#) by last Friday, and for the first time, the agency [finally didn't bother](#) to submit a legal request to reauthorize the program for another 90-day period.

If the program is to continue in any form, it will almost certainly be as a hybrid version, authorized by the controversial [USA Freedom Act](#), which would mandate phone companies keep your records on their own—many already do—rather than the NSA. The records would then be accessible to the NSA only through a warrant.

But lost in this hullabaloo is that the U.S.'s intelligence community uses Section 215 for far more than just the NSA's best-known program. That's in some ways the real battle behind whether the Senate agrees to the USA Freedom Act—it's a fight for the future of those programs, too.

So what happens if Section 215 does expire?

---

## Gone but not forgotten

First, it's worth noting, the NSA will still have your old phone records—it just will no longer indiscriminately collect new ones. And it certainly could get new ones if it wanted them, if you were targeted in an investigation.

Section 215 is very far from the only legal tool in the intelligence community's legal toolshed. It still has Section 214 of the Patriot Act, National Security Letters, and authorities under Executive Order 12333, the granddaddy of modern surveillance authorities, signed by President Reagan in 1981, which gives all kinds of [permissions](#) for foreign bulk collections.

“It certainly doesn't mean they'll stop getting phone records,” Julian Sanchez, a senior fellow at the Cato Institute who specializes in privacy, technology, and national security, told the Daily Dot. “As long as they're doing it in a more targeted way—that is to say, they're going to specific numbers rather than collecting in bulk—they can continue getting all the information they need about suspicious phone numbers without 215.

## Not just the NSA

There isn't yet an Edward Snowden for the [FBI](#) or [CIA](#), someone who has thoroughly exposed classified programs for all the world to see. But we do have some information about each of those agencies' use of the authority.

Section 215 allows for the bulk collection of “business records” for general terrorism investigations. As we've seen with the FISA court orders that allowed the NSA's phone-data collection program in the first place, that can be a pretty broad definition. As revealed in a 2013 [New York Times report](#), the CIA relies on Section 215 for a program that also collects information in bulk, also including American info—but in that agency's case, it tracks financial data, like Western Union transfers.

The FBI, on the other hand, uses it for a myriad of reasons. “In terms of the actual orders that they get, most of those are for Internet data, Internet records,” Sanchez said.

For a while, the FBI used Section 215 somewhat modestly. The DOJ regularly audits the agency's use of the authority, and it conspicuously released a report last week that documents its uses and abuses of Section 215 from 2007 to 2009. In those years, the FBI made requests through that authority at minimum 51 times—the number of times the Foreign Intelligence Surveillance Court ([FISC](#)) said yes. The number of times it *tried* is redacted, but it's presumably no more than three digits, because the redacted part isn't too big.

Of the [REDACTED] requests, 51 applications were submitted to and granted by the FISA Court. Of the 51 applications, the Department filed [REDACTED] on behalf of the FBI and filed [REDACTED] in connection with counterterrorism programs [REDACTED].<sup>5</sup> The

## What is metadata? It's complicated.

What were the FBI's requests for? Sometimes, it's for financial data, like that CIA program. Usually, it's for metadata—generally defined as the details surrounding communications, but not the actual communications themselves. But even the "what" that constitutes "metadata" is somewhat subjective. "Metadata generally is considered to exclude the content of communications," the report says. But the FBI's own attorneys "told us that the terms used to define metadata themselves lack standardized definitions and that applying them to rapidly changing technology can be difficult," it says.

One example is [United States v. Forster](#) in 2007, in which a court found that the IP addresses to and from an email could be considered metadata, and thus the FBI could obtain them under 215 without a specific warrant. But to look at which URLs a person had visited? That was content, and it *would* probably require a warrant.

The FBI has definitely used 215 to get their guy in ways that pushes the boundaries of legal, a practice that calls to mind the NSA's [parallel construction scandal](#). In one anecdote described in the report, the authority was used—we don't know precisely how—to help identify a person claiming to be an employee at Tennessee's Oak Ridge National Laboratory, who was trying to sell stolen nuclear converter parts. Non-redacted details indicate this is a reference Roy Lynn Oakley, who in 2009 was sentenced to a six-year prison sentence after he tried to sell such parts to an undercover agent in 2007.

According to the FBI's [own writeup](#) at the time, the agency set up an undercover agent to catch Oakley in the act, but only after determining through some other means that Oakley had a desire to sell to an agent of a foreign government. According to the report, the FBI issued a 215 request the same month it busted Oakley, the report contained "misstatement of a material fact," and that he didn't explain a key discrepancy. The 215 information wasn't used in the prosecution against Oakley, and he received a 6-year prison sentence.

In addition to that, the report makes ominous reference to requests for "customer information," and "medical and educational records," though the details there are redacted.

But that's small time. These examples are all before 2009, when everything changed.

That year, thanks to a [court ruling](#), 215's importance to the FBI skyrocketed. "The FBI used to get everything with National Security letters, because they didn't have to go to a court," Sanchez said. In 2009, a legal opinion counsel said essentially NSLs are actually narrower than the FBI had interpreted them to be and can't be used for any old type of Internet data," he added. We know from an American Civil Liberties Union Freedom of Information Act request that the FBI applied for hundreds in 2012 and 2013, though we don't know how broadly they were written or for what.

## The lingering truth

So will the USA Freedom Act, if it passes, end dragnet surveillance of Americans? The short answer: no. The NSA will have to get warrants for your phone records, yes. But, [as the Sunlight Foundation points out](#), "mass surveillance will still occur under Section 215"—even if the USA Freedom Act becomes law—"and the FBI, under the act, won't be required to report on it."

One more wrinkle? If Section 215 expires, that doesn't mean it'll stay that way. "If it expires, I think we'll immediately see a bill by the intelligence community to reinstitute Section 215 or a bill to expand the government's power," Mark Jaycox, a legislative analyst at the EFF, told the Daily Dot.

So when Senate Majority Leader [Mitch McConnell](#) (R-Ky.) makes a push to partially or wholesale save Section 215 on Sunday, or if another member of Congress demands more spying authority in the days after, know that it's probably not a stubborn push for the NSA to still collect your phone records. It's for what other intelligence agencies are doing in the shadows.