Breakdown of the USA Freedom Act

Al Jazeera breaks down the law that aims to rein in the NSA's bulk metadata program

Amel Ahmed

Saturday, May 23, 2015

Congress on Saturday failed to agree on whether to change or extend provisions of the USA Patriot Act that the National Security Agency (NSA) has used to justify its bulk collection of Americans' telephone records — placing the program's fate in limbo days ahead of its scheduled expiration

Shortly after blocking the USA Freedom Act, which would have replaced the bulk data collection program with a somewhat more targeted one, the Senate also thwarted a measure to extend the program for two months.

The body's inability to take decisive action on the program will force lawmakers to end their Memorial Day holiday recess early and return to Washington on Sunday to attempt a last-minute deal.

The House voted last week by a wide margin to pass the Freedom Act, which would end the NSA's collection of domestic calling records under Section 215 after a six-month transition period. It also attempts to reform the secret FISA court, which approves NSA surveillance requests.

The bill would also end the use of national security letters, a law enforcement investigative tool used to secretly request data from Internet and phone companies.

GOP leaders opposed to the bill want to extend the current NSA program by two months, followed by a two-year transition period.

But following the Second Circuit's historic ruling earlier this month declaring the NSA bulk collection of phone metadata illegal, the bill has emerged as the easiest way forward for the Senate, which faces the June 1 sunset of some provisions in the Patriot Act, including Section 215.

If the Senate fails to act by June 1, officials say they will lose valuable surveillance tools.

Privacy advocates have criticized the legislation as a watered-down version of its previous iterations and are pushing for a stronger reform bill.

"It's a bill that would reauthorize programs that should have never existed in the first place – and the federal courts are finally saying that these programs are illegal and unconstitutional," said Patrick Eddington, a policy analyst specializing in homeland security and civil liberties at the Cato Institute.

He added, "It's an amazing spectacle, to see Congress authorize a program that doesn't work, is illegal, and costs billions of dollars. We have to ask, why does Congress want to reauthorize a digital bridge to nowhere?"

Below is a breakdown of the bill's major provisions.

End of bulk collection

The USA Freedom Act includes language that would terminate the bulk collection of telephone metadata under Section 215 of the Patriot Act. Telephone metadata includes the time, location, date, contacted parties, but not the content of calls.

Instead of the government storing the bulk data, the bill requires phone companies to retain the call records. In order to access certain records, the government would have to supply the FISA court with a "specific selection term" identifying the records to be searched.

But privacy advocates say that the bill fails to adequately define the "specific selection term." They point to loopholes in the law that serve to vastly expand the class of items that can be searched, even with a specific selection term in place.

For instance, problematic Patriot Act definitions are left intact in the new bill and "person" is broadly defined to include any group, entity, association, corporation, or foreign power. Such an expansive definition leaves open the possibility of continued bulk metadata surveillance, says Eddington.

"An IP address can be linked to a single computer or an entire organization. So the idea that this law is going to really limit bulk collection is illusory," Eddington said.

In addition, while the bill prevents the government from collecting bulk data during the initial stage of the investigation, it permits the government to conduct a broad sweep of records during a second step in the process known as the "second hop."

Under the bill, the government can gather all the metadata that have been in contact with the records collected in the first step, without any additional authorization.

Privacy advocates say that the law is vague in terms of what the government is authorized to collect during the second hop: the government may conduct a second "hop" if there's a "direct connection" to the first specific selection term, but the law does not define what a "direct connection" is.

"[T]he government could interpret 'direct connection' to include the physical proximity of two mobile devices, or being in someone's address book, since both might be called 'direct,'" write Cindy Cohn and Nadia Kayyali of the Electronic Frontier Foundation.

Privacy advocates say the bill should include a provision requiring the government to file another application for any further data it wants to collect beyond the first instance. The application should show a nexus exists between terrorism and the second round of data gathered.

Privacy advocates warn that while the Freedom Act will end the bulk collection of phone metadata under Section 215, that's not the only source of legal authority for federal officials to collect mass amounts of private information.

The bill leaves in place other controversial mass surveillance programs – such as the PRISM program and Section 702 of the FISA Amendments Act – leaving many privacy advocates deeply critical of the bill.

The NSA's PRISM program collects users' Internet data while Section 702 allows the government to collect without a warrant Americans' international call and email records.

"I think we should always be worried, but that's why we spoke so forcefully. If you say we've ended bulk collection that's not correct," Rep. Zoe Lofgren, D-Calif., told Reason, a libertarian magazine.

Lofgren told the magazine that she only approved the Freedom Act under the condition that other forms of mass surveillance will be eventually addressed by Congress.

Privacy advocates also want to see eliminated from the bill an "emergency exception" that allows the government to spy within the U.S. on any "non-United States person" for 72 hours without any court authorization.

Expanding corporate immunity

The USA Freedom Act includes a provision that expands immunity provided to companies who participate in the government's surveillance program.

While Section 215 currently provides immunity to companies who cooperate in good faith, the new legislation changes this in two ways.

First, it eliminates the "good faith" language, although it makes clear that the production must be in accordance with an order issued under the statute, which cuts back on the potential for bad

faith actions, says Elizabeth Goitein, co-director of the Brennan Center for Justice's national security program.

Second, it extends liability protection, not just to the production of records but also to supplying technical assistance to the government.

"That is potentially more problematic in my view, since it's so vague," Goiten said.

In what has been a trend for the past decade, insulating companies from liability will place the public at a greater disadvantage, warn privacy advocates.

"We think it's a problematic trend because it drives a bigger wedge between companies and their customers," Patrick Toomey, staff attorney at the ACLU told Al Jazeera. "They will have less incentive to push back against government overreach."

The Second Circuit ruling addressed the standing provision at length in its opinion, holding that government cannot preclude individual citizens from raising legal challenges against surveillance programs that target them.

But as legal experts point out, unless another Edward Snowden comes along and absent an officially acknowledged surveillance program, it will remain extremely difficult for people targeted by surveillance to bring legal challenges.

"Absent an officially acknowledged bulk surveillance program, then there's no standing to challenge a narrower program unless you can somehow cut through the secrecy to demonstrate that you're targeted," said Heidi Kitrosser, a law professor at the University of Minnesota Law School who has extensively studied executive secrecy at the federal level.

"Plus, even if another Snowden were to come along and reveal targets or categories of targets, the government will probably be able to argue successfully that it has not officially acknowledged that information and so it remains a state secret," she said.

Toomey adds that participating companies – as the first line of defense against privacy violations – will be less likely to challenge mass surveillance programs if granted greater immunity.

"Companies have one of the easiest avenues to court because they know about the surveillance. That makes it all the more important to ensure that companies are standing up for the privacy interests of their users when it comes to resisting sweeping demands for customer data," he said.

Increased transparency

In a bid to make the FISA court more transparent and less of a rubber stamp for government conduct, the new legislation will reform the FISA court in three important ways.

First, the law will mandate the appointment of five special advisors to provide limited oversight of the FISA court by providing "legal arguments that advance the protection of individual privacy and civil liberties."

Second, the law will require the government to declassify significant FISA Court opinions, allowing for greater public scrutiny. It defines “significant” as any novel construction or interpretation of a "specific selection term."

Finally, the law will require the government to disclose information about the number and type of applications for FISA Court orders, along with estimates of the number of people targeted, according to Lawfare.

Not included in the current iteration of the bill are "minimization" measures that would have required the government to delete any information collected that later turned out to be unrelated to the investigation. That provision was eliminated from the current bill.

"Given the extent to which the current bill could be construed to conduct broad surveillance impacting individuals with no demonstrable connection to terrorism, such minimization procedures are critical to protecting personal information from improper government retention, use, and dissemination," writes the ACLU.