theguardian

Restrictions placed on NSA's data store after intense talks over surveillance bill

USA Freedom Act heads to the House with government required to 'promptly' purge phone records that do not contain 'foreign intelligence information'

By Spencer Ackerman

May 20, 2014

The government would ultimately have to 'destroy all call detail records produced under the order as prescribed by such procedures'. Photograph: Jim Watson/AFP

Last-minute negotiations over the details of a congressional surveillance bill have resulted in restrictions around the National Security Agency's massive repository of analysed call data.

Intense closed-door talks between lawmakers and Obama administration and intelligence officials that wrapped up Tuesday afternoon have finalised the language of the USA Freedom Act. The bill is expected to receive a vote on the House floor on Thursday.

The latest twist for the bill is an expanded provision that would require the government to "promptly" purge phone records that do not contain "foreign intelligence information," effectively pruning irrelevant records from the NSA's trees of analyzed phone data.

But several other changes to the bill, which civil libertarians already considered watered down after a series of legislative compromises, have cost it critical support from privacy groups ahead of Thursday's vote.

Under the new provision, the government would have to "adopt minimisation procedures that require the prompt destruction of all call detail records" turned over by the telecoms firms "that the government determines are not foreign intelligence information."

The government would ultimately have to "destroy all call detail records produced under the order as prescribed by such procedures".

A previous version of that language tasked the government merely with destroying call records "not later than five years after the production of such records, except for records that are relevant to an authorised investigation."

While several privacy protections within the USA Freedom Act have been diluted in recent weeks, several people familiar with the negotiations said they thought the new provision better

protects privacy than the old one, as it represents the first known restriction on the NSA's "corporate store" of analysed data.

The "corporate store" is the digital warehouse where the NSA stores all the US call records it has amassed when searching for connections to the target phone numbers it believes may be tied to specific terrorist groups. Until this year, data up to three "hops" from such a phone number was fit for inclusion in the store.

Once data is placed in the store, NSA analysts face virtually no restrictions on their ability to search through it.

"NSA may apply the full range of Sigint [signals intelligence] analytic tradecraft" to phone records placed in the store, according to a footnote in a Fisa court order declassified by the government last year. Searches through data placed in the corporate store can occur "without the requirement" that reasonable articulable suspicion of connection to wrongdoing exist; nor is the NSA required to keep an "auditable record" of searches performed within the corporate store.

The amount of data contained within the corporate store is voluminous. A January report from the US government's civil liberties watchdog estimated that the 300 searches of Americans' phone data the NSA said it performed in 2012 would yield "records involving over 120m phone numbers" in that year alone.

The watchdog, the Privacy and Civil Liberties Oversight Board, recommended that the NSA have to possess the same "reasonable articulable suspicion" to search data in the corporate store as it must to analyse phone records once collected.

Until now, the USA Freedom Act, increasingly the consensus bill for surveillance reforms, left the "corporate store" alone.

Under the bill, the government would no longer collect call records in bulk. But it would be permitted to acquire Americans' phone data when a judge certifies that there is reasonable articulable suspicion of a connection to terrorism or foreign espionage, and it can collect phone records from the contacts of the contacts – two "hops" – of the original person or phone account the government targets.

The new language would apparently restrict the NSA from retaining data on the contacts of the targets not believed to have a connection to foreign intelligence information – what surveillance observers sometimes refer to as the "pizza guy" problem, where the NSA amasses data on random and irrelevant people or accounts connected to targets.

But the language does not define key terms, such as how long a record can be withheld before its "prompt" destruction. Nor does it specify how the government will "determine" a call record is unrelated to foreign intelligence information if, as can occur with the corporate store today, NSA's automated programs sift through the data.

"Placing meaningful limits on the NSA's use of this vast pool of data is crucial to protecting Americans' privacy – and to any reform effort. Congress should not leave the NSA with a wide open backdoor to many of Americans' call records via the corporate store," said Patrick Toomey, a lawyer with the American Civil Liberties Union, who has focused on the corporate store.

A deal on the corporate store restriction was easier to reach than over a different critical definition contained within the USA Freedom Act – one that defines the source of the records the government will be able to collect.

That category is a "specific selection term." That is the root data from which the government must suspect of connection to terrorism or espionage to launch the collection of call records. Without possessing that term, the government cannot collect obtain the call records at issue.

The version of the USA Freedom Act that cleared House committees earlier this month defined it simply as a term that "uniquely describe[s] a person, entity, or account."

But the version that will head to the floor, at the Obama administration's insistence, has broadened the definition, opening the door to broader data collection than the bill's architect's initially envisioned.

The bill now defines a "specific selection term" as "a discrete term, such as a term specifically identifying a person, entity, account, or device, used by the government to limit the scope of the information or tangible things sought."

Sources familiar with the process said the government had pushed for an even broader definition.

Privacy groups had already watched with dismay as their favored bill gradually grew less restrictive on the NSA and its transparency requirements about what recipients of surveillance orders can disclose to their customers became weaker.

But after the finalized bill was released on Tuesday, the USA Freedom Act lost the support of the Open Technology Institute, which had strenuously advocated in its favor since its October introduction in the House.

"We cannot in good conscience support this weakened version of the bill, where key reforms – especially those intended to end bulk collection and increase transparency – have been substantially watered down," policy director Kevin Bankston said in a statement**.**

"We're gravely disappointed that rather than respecting the wishes of the unanimous Judiciary and Intelligence Committees, the House leadership and the Obama Administration have chosen to disrupt the hard-fought compromise that so many of us were willing to support just two weeks ago."

Amie Stepanovich, a lawyer with the digital-rights group Access, which also revoked its support for the bill, said: "It's greatly disappointing to witness House leaders succumb to the pressure

applied by the Obama administration and others, turning its back on the compromise version of USA Freedom that so many supported just two weeks ago."

Julian Sanchez of the Cato Institute tweeted: "So, seems like nobody's happy with New Coke USA FREEDOM, but resigned to the alternative being [the House intelligence committee's] (even worse) bill."