# Senators Should Oppose Senator McConnell's Amendments and Pass a Clean Version of the USA FREEDOM Act

This past Sunday night, the Senate took the historic step of voting 77-17 to allow debate on the USA FREEDOM Act (H.R. 2048) as well as any proposed amendments to the bill. Unfortunately, it looks like all of the amendments to be offered on that surveillance reform bill, which New America's Open Technology Institute supports, are intended to water down or delay implementation of its reforms. We therefore urge Senators to oppose those amendments and pass a clean version of the bill, which is the result of nearly two years of intense debate, negotiation, and bipartisan compromise.

Last month, the House overwhelmingly approved the USA FREEDOM Act with a vote of 338-88, and the vast majority of "no" votes came from members who do not believe the bill's reforms go far enough. With this much support for strong surveillance reform in the House, any amendment to weaken USA FREEDOM will seriously endanger the bill's ability to pass the House again—which is why the both the Republican and Democratic leaders of the House Judiciary Committee have called on the Senate to quickly pass the bill as is. Particularly if Senate leaders want to minimize the amount of time that key USA PATRIOT Act provisions are not in effect due to the June 1st "sunset" of those provisions, the fastest, easiest, and most responsible thing for the Senate to do is to simply pass the House bill without amendment and immediately send it to the President for his signature.

Instead, Senate Majority Leader Mitch McConnell (R-KY) has introduced four amendments that would undermine USA FREEDOM's reforms, while making clear he will not allow votes on any amendments that would strengthen the bill. Those four amendments will likely be debated and voted on in the next day or two, after which the Senate is expected to vote on final passage of the USA FREEDOM Act. While the Open Technology Institute (OTI) supports the House-passed bill and would support and welcome amendments that would strengthen its reforms, we strongly oppose any amendment that would weaken the bill such as those proposed by Senator McConnell.

Senator McConnell has made very clear that he believes that Sunday night's sunset of PATRIOT Act Section 215 puts the nation in danger. However, under his leadership, the Senate's national security hawks allowed these provisions to expire by trying to block the USA FREEDOM Act that would have preserved those authorities while also protecting Americans' privacy. The bill even has the support of the Director of National Intelligence (DNI) and the Attorney General, who have not only assured Congress that it "preserves vital national security authorities," but also that it "preserves the essential operational capabilities of the telephone metadata program and enhances other intelligence capabilities needed to protect our nation and its partners." The Director of the National Security Agency (NSA) also wrote to the Senate, making clear that the NSA knows of "no technical or security reasons why [information collection consistent with the USA FREEDOM Act] cannot be tested and brought online within the 180 day period" currently provided for in the bill.

Given the broad support of the Intelligence Community, Congress, the Administration, the American tech industry, and privacy advocates, it is unclear why Senator McConnell is playing games with authorities that he deems essential to Americans' safety by pushing for amendments that would delay or threaten their reinstatement. As we explain in more detail below, all of these amendments seek to address problems that the leaders of the Intelligence Community have already stated do not exist. Rather than stalling this bill and lengthening the lapse in these authorities, the Senate should reject these amendments and move forward on passage of a clean bill.

What follows is a brief explanation of each amendment, and the serious concerns they would raise:

**For more information, please contact Robyn Greene, OTI Policy Counsel, at greene@opentechinstitute.org.**

**Amendment No. 1452:** This amendment would require –

- **Removal of the Requirement to Declassify Significant FISA Court Opinions:** Currently the USA FREEDOM Act requires the DNI to review all significant FISA Court decisions and either declassify and publicly release the opinions or release summaries of the opinions that would be sufficient to inform Americans and Congress of the general context of the decision, the legal issues in question, and how the court ruled. If this amendment passed, the DNI would no longer have to conduct a declassification review of FISA Court decisions or release any new information about them.
    - **Why This Is A Problem:** This is one of the most important accountability mechanisms in the bill. The release of significant FISA Court decisions is essential to ensuring that the government and the FISA Court are interpreting the surveillance authorities as Congress intended, and to ensuring that secret law cannot again be used to authorize massive spying programs that Congress did not intend, as was the case with bulk collection under Patriot Act Section 215. Additionally, no one in the Intelligence Community has suggested that this declassification provision would be harmful to national security. This amendment would therefore needlessly reduce transparency and accountability while providing no countervailing benefit.

- **Watered-Down Amicus Provision:** Under the House-passed bill, the FISA Court must appoint an amicus curiae ("friend of the court") to serve in any case that "presents a novel or significant interpretation of the law," or issue a written finding that an appointment is not appropriate. The amicus would, as appropriate, provide the court with legal arguments that advance the protections of privacy and civil liberties, information relating to intelligence collection or technology, or any other relevant legal arguments, and it would have access to all legal or other materials that the court deems relevant to its duties. The amendment would significantly weaken this provision by removing the requirement that the FISA Court provide written notice about when and why it chooses not to appoint an amicus. It would also limit the amicus' duties to whatever the court assigns, without any mention of the duty to advocate for the advancement of privacy and civil liberties. Additionally, the amicus would only have access to applications, certifications, petitions, and motions at the discretion of the court and would not necessarily have access to legal precedent or other relevant materials.
    - **Why This Is A Problem:** The amicus provision in the House-passed bill is already crafted in a way that gives the FISA Court an enormous amount of discretion in deciding when and how to call upon an amicus. This amendment would needlessly further weaken this provision, which was already significantly watered-down from the version included in the 2014 Senate bill, and in the process render it completely toothless. All this despite any indication from the Intelligence Community that the House-passed provision would harm national security or interfere with the FISA Court's ability to expeditiously carry out its function.

- **A Notice Requirement for Data Retention:** This amendment would require electronic communications service providers (phone and Internet companies) that hold call detail records (CDRs) and have previously received government orders requesting CDRs to give the Attorney General at least 180 days advance notice if they intend change their retention policies, where that change would result in their holding customer records for less than 18 months.
    - **Why This Is A Problem:** This amendment is entirely unnecessary given the DNI's statements that no new data retention requirement is needed, and that the Intelligence Community would immediately inform Congress if that were to change. Requiring private businesses to alert the government ahead of time before it can change its internal data retention policies is harmful to innovation, threatens privacy, and could be intended as a prelude to a requirement that companies keep certain records for a specified period of time. Such a mandate is bad public policy and would be uniformly opposed by the House, the tech industry, and the privacy community. This amendment too would likely meet the same strong opposition from all of these groups, and is strongly opposed by OTI.

**For more information, please contact Robyn Greene, OTI Policy Counsel, at greene@opentechinstitute.org.**

- **Certification of Effectiveness to Congress:** This amendment would require the DNI to certify to Congress 30 days before the deadline for final implementation of the reforms in USA FREEDOM that the new processes and procedures work, that they will not harm national security, and that they will effectively protect classified information.
    - **Why This Is A Problem:** Again, this amendment is unnecessary. The DNI has already written to Congress confirming that the USA FREEDOM Act "preserves the essential operational capabilities of the telephone metadata program and enhances other intelligence capabilities." Like the delay in implementation of the bill's reforms, and the other provisions that this amendment seeks to weaken, this certification adds no benefit, but if passed, the amendment would stall passage of the bill, and is also likely designed to give opponents of the bill the opportunity to interrupt the implementation process, or roll back its important reforms.

**Amendment No. 1450:**

- **Doubled Wait Period Before Implementation of Reforms:** The current bill requires the government to implement the required reforms in 180 days. This amendment would extend the implementation period to 12 months.
    - **Why This Is A Problem:** Like the data retention provision of the amendment, this provision is also entirely unnecessary. The Director of the NSA wrote to Senator McConnell assuring him that there are "no technical or security reasons" why the changes to the NSA's CDR program that would be made in response to USA FREEDOM could not be brought online within the 180 day period set forth in the bill. Given that there is no technological or operational reason to delay the implementation of these important reforms, this amendment is likely intended to give opponents of reform additional time to interrupt the process and roll back the reforms in USA FREEDOM, and would likely be staunchly opposed in the House.

The following two amendments offered by Senator McConnell draw on individual portions of the first Amendment (No. 1452). They include the following changes to the underlying House-passed bill:

**Amendment No. 1449:**

- Notice Requirement for Data Retention
- Certification of Effectiveness to Congress

**Amendment No. 1451:** Watered-Down Amicus Provision

Instead of taking the last five months to consider and debate reform legislation, Senate national security hawks' stalled and obstructed passage of the USA FREEDOM Act, and promulgated myths about problems with the bill that simply never existed. Their actions caused the lapse of the very authorities they were attempting to preserve. Now, instead of moving forward on the swift passage of the House-passed bill, Senator McConnell has introduced and is expected to allow votes on four amendments that would unnecessarily weaken the bill and threaten its final passage. The USA FREEDOM Act not only has the backing of a vast majority of the House of Representatives, it also has the support of the Intelligence Community, the Administration, the American tech industry, and major privacy and advocacy groups. It is time for the Senate to follow the House's lead by rejecting these problematic amendments and passing a clean version of the USA FREEDOM Act.

**For more information, please contact Robyn Greene, OTI Policy Counsel, at greene@opentechinstitute.org.**