

**Join Reps. Massie, Lofgren, Sensenbrenner, Conyers, Poe, DelBene, Jordan, O'Rourke, Amash, Pocan, Nadler, Gabbard, Farenthold, Lieu, Issa, Butterfield, Labrador, and Gosar to close backdoors used for unconstitutional surveillance**

**From:** The Honorable Thomas Massie  
**Sent By:** [Seana.Cranston@mail.house.gov](mailto:Seana.Cranston@mail.house.gov)  
**Date:** 6/15/2016

**Join Reps. Massie, Lofgren, Sensenbrenner, Conyers, Poe, DelBene, Jordan, O'Rourke, Amash, Pocan, Nadler, Gabbard, Farenthold, Lieu, Issa, Butterfield, Labrador, and Gosar in standing for the Constitution.**

Twice in the last two years the House of Representatives has overwhelmingly passed our bipartisan amendment, last year by a [255-174 vote](#). Once again, our bipartisan group is reuniting to shut surveillance backdoors that do not meet the expectations of our constituents or the standards required by our Constitution.

Our amendment shuts one “backdoor” by prohibiting warrantless searches of government databases for information that pertains to U.S. citizens. The Director of National Intelligence has confirmed that the government searches vast amounts of data—including the content of emails and telephone calls—without individualized suspicion or probable cause. The director of the FBI has also confirmed that it uses this information to build criminal cases against U.S. persons. But the Director of National Intelligence and the FBI are not above the Fourth Amendment, and this practice should end.

Our amendment also prohibits the NSA and CIA from placing “backdoors” into commercial products. In December of 2013, it was reported that a U.S. security company had received \$10 million from the NSA to use a flawed encryption method. And in May of 2014, a major security flaw was found in software used by law enforcement to intercept communications. This flaw allowed a hacker to listen in to any call recorded by the system. Even if such a backdoor is created with the best of intentions, it is only a matter of time before a hacker finds and exploits it. Such flaws put the data security of every person and business using the internet at risk. Our government should strengthen the technology that protects our privacy, not take advantage of it.

**A dear colleague circulated earlier today claims that, if this amendment passed, the “Intelligence Community would not be able to look through information lawfully collected under FISA Section 702 to see if Omar Siddiqui Mateen, the Orlando nightclub attacker, was in contact with any terrorist groups outside the United States.” This statement is wrong. It is factually inaccurate and attempts to exploit a national tragedy.**

Massie-Lofgren allows the NSA to query the 702 database for information about U.S. persons—provided that the government first gets proper legal process. In Orlando, where the shooter pledged loyalty to multiple foreign terrorist organizations, the government would have no difficulty securing a warrant.

Stand up for our Constitution. There is still work to be done.

Join our bipartisan group and a broad coalition, including FreedomWorks, Demand Progress, Electronic Frontier Foundation, R Street, American Civil Liberties Union, Niskanen Center, Campaign for Liberty, and Center for Democracy & Technology in supporting our amendment.