



Massie-Lofgren Amendment Would Prevent Warrantless Searches of American Citizens and Encryption Backdoors for Government Surveillance

Tomorrow, the House of Representatives is expected to vote on a bipartisan [amendment](#) to the Department of Defense (DoD) Appropriations Act ([H.R. 5293](#)) offered by Reps. Thomas Massie (R-KY) and Zoe Lofgren (D-CA). The Center for Democracy & Technology strongly supports this amendment, which passed overwhelmingly in the House in 2014 and 2015, because it would protect the privacy of U.S. persons and the cybersecurity of all internet users.

The Massie-Lofgren amendment would prohibit the use of funds for the following:

- 1) **Warrantless searches for Americans' data via the "backdoor search loophole."** Section 702 of the Foreign Intelligence Surveillance Act authorizes the warrantless collection of communications content pertaining to non-U.S. persons located abroad so long as a "significant purpose" of such collection is foreign intelligence. Although focused on non-U.S. persons located abroad, this surveillance program sweeps up a [substantial amount](#) of Americans' communications as well, and the government has been using the program to access information about U.S. persons located in the United States without judicial oversight. This practice, which has been referred to as a "backdoor search," violates the spirit of the law and undermines the protections for U.S. persons that were explicitly included by Congress when drafting the statute. The Massie-Lofgren amendment would prohibit the use of funds to take advantage of the backdoor search loophole, thereby protecting U.S. persons from these warrantless searches.
- 2) **Requesting or requiring a backdoor to encryption.** For decades, policymakers have debated whether it is possible to realize the benefits of digital security technologies such as encryption while building in access points for law enforcement, intelligence, and other government agencies. However, information security experts have consistently [answered](#) that question with a resounding "no," because a backdoor to encryption is as dangerous as it is impracticable. Vulnerabilities to encryption and other security measures can be exploited by anyone – leaving all internet users at risk of hacking, identity theft, and espionage. Moreover, encryption is a [global commodity](#), so requiring a weaker form of encryption in the United States will not prevent determined users from using alternative technologies created abroad. The Massie-Lofgren amendment ensures that funds appropriated under the Act will not be used to request or require a company to weaken the digital security of its products, unless it is already required to do so under the Communications Assistance for Law Enforcement Act (CALEA).

CDT strongly encourages Members to vote "yes" on the Massie-Lofgren amendment and stop DoD funding of two dangerous types of backdoors: one that invades Americans' privacy by permitting an end-run around the Fourth Amendment, and one that would leave all internet users less secure.

For more information, please contact Greg Nojeim at gnojeim@cdt.org, or Jadzia Butler at jbutler@cdt.org.

1401 K Street NW, 2nd Floor Washington, DC 20005