

Mother Jones

Will This Bill End the War Between the Government and the Tech Community Over Encryption?

Max J. Rosenthal

February 29, 2016

The chairman of the House Homeland Security Committee will introduce a bill on Monday afternoon aiming to help solve the long-running fight between the government and the tech and privacy communities over encryption, which has made headlines recently thanks to the FBI's attempt to force Apple to help unlock an iPhone used by one of the San Bernardino shooters.

The bill, which will be introduced by Rep. Michael McCaul (R-Texas) and is backed strongly by Sen. Mark Warner (D-Va.), would create a commission of 16 experts with a range of backgrounds—from cryptographers and intelligence officials to privacy advocates and tech executives—to "examine the intersection of security and digital security and communications technology in a systematic, holistic way, and determine the implications for national security, public safety, data security, privacy, innovation, and American competitiveness in the global marketplace," according to [text of the legislation that was provided to *Mother Jones*](#).

It's part of a larger push to have the government and private sector work together to create new ways to solve the impasse over encryption and other digital security issues. While the government wants to be able to access encrypted devices and messages when needed, tech companies and cryptographers have said there is simply no current way to create such a backdoor for the government without also potentially giving that same access to cybercriminals and hackers. Hillary Clinton has called for a "[Manhattan-like project](#)" to square that circle, with other presidential candidates calling for similar public-private cooperation.

McCaul and the commission's backers hope the panel may find a new, previously undiscovered way to reconcile the legal and technical demands of the two sides, but there appears to be little idea of what that could be. In conversations with lawmakers, privacy advocates, national security lawyers, and technologists, none were able to offer *Mother Jones* any concrete notion of what a solution may look like. Many members of the technology and privacy communities also view calls for more cooperation and discussion as disingenuous. They argue the technical questions are settled, and that more talking won't solve anything—but may produce bad legislation that harms security and privacy. "They say they can't do it, but let's pass the legislation to find out,

and I bet they'll figure out the solution after we've mandated it.' That seems like a bad idea to me," Julian Sanchez of the libertarian Cato Institute told *Motherboard* last year.

Each party would get to nominate eight members of the commission, with each nominee coming from a different one of eight fields. Six of the slots would go to law enforcement and intelligence community representatives, with the other 10 given to tech business and economics experts along with two cryptographers and two members of the civil liberties community. The group would have a year to draft a final report, which would require the approval of 12 of the 16 members*.