PHYS.ORG

US could force firms to help break encryption, under new bill

April 13 2016

Senators Richard Burr (R) and Dianne Feinstein (C) of the Senate Intelligence Committee, pictured on February 9, 2016, unveiled legislation to require technology firms to help law enforcement unlock encrypted devices

Two key US lawmakers Wednesday unveiled legislation to require technology firms to help law enforcement unlock encrypted devices—prompting a fierce outcry from the industry and privacy activists.

The bill released by Senators Richard Burr and Dianne Feinstein of the Senate Intelligence Committee comes in the wake of a heated legal battle pitting the FBI against Apple as part of an investigation into last year's San Bernardino attacks.

"No entity or individual is above the law," said Feinstein, the top Democrat on the committee chaired by Republican Burr.

"Today, terrorists and criminals are increasingly using encryption to foil law enforcement efforts, even in the face of a court order. We need strong encryption to protect personal data, but we also need to know when terrorists are plotting to kill Americans."

The lawmakers in a joint statement said the proposal was a "discussion draft" and that they would "solicit input from the public and key stakeholders before formally introducing the bill."

"I am hopeful that this draft will start a meaningful and inclusive debate on the role of encryption and its place within the rule of law," Burr said. "Based on initial feedback, I am confident that the discussion has begun."

Facebook-owned WhatsApp said it had implemented end-to-end encryption for its billion users so that no other party can read the messages except for the sender and recipient

The use of strong encryption in applications and smartphones, with they keys only available to users, has raised concerns in law enforcement that criminals and others may operate in secrecy, with investigators unable to gain access to data even with a court order.

Legislation similar to the Senate proposal is also being considered in other countries, notably Britain and France, amid concerns that attackers have been using encryption to avoid detection.

But the Senate draft, which was leaked to media earlier this week, sparked intense criticism both from the technology industry and digital rights activities, claiming it would effectively create a "back door" for

law enforcement which could be exploited by hackers and other governments.

Kevin Bankston of the New America Foundation's Open Technology Institute said the bill would require "every tech vendor in America to use either backdoored encryption or no encryption at all, even though practically every security expert in the country would tell you that means laying down our arms in the constant fight to secure or data against thieves, hackers, and spies."

Daniel Castro of the Information Technology & Innovation Foundation, a Washington think tank, said the bill "sets up a legal paradox that would further muddy the waters about how and when the government can compel the private sector to assist in gaining access to private information."

Gary Shapiro of the Consumer Technology Association, a trade group representing hundreds of technology firms, called the measure an "overreaction" to fears on encryption.

"There is no consensus in the intelligence community that a requirement to force manufacturers to open encryption is the correct policy," Shapiro said in a statement.

The US government last month withdrew its request to force Apple to help unlock an iPhone used by one of the San Bernardino shooters, saying the FBI had found another means to access the data. But several cases are pending against Apple and other firms.

Last week, Facebook-owned WhatsApp said it had implemented end-to-end encryption for its billion users, so that no other party can read the messages.