THE // INTERCEPT

Bill That Would Ban End-to-End Encryption Savaged by Critics

Jenna McLaughlin

April 8, 2016

A long-anticipated draft of anti-encryption legislation written by the leaders of the Senate Intelligence Committee circulated late Thursday night and left may critics apoplectic.

The bill, from Sens. Richard Burr and Dianne Feinstein, would force technology companies to either decrypt the contents of their customers' communications for law enforcement, or hack into their own products to do so — effectively rendering illegal the end-to-end encryption currently offered by some of the heaviest hitters in the business, like Apple, Facebook, Google, and now WhatsApp.

On Friday, Feinstein and Burr told reporters they were still working on the draft and couldn't comment on the language of an unfinished version.

Feinstein threw down the gauntlet in December, vowing to push for a bill that would mandate breakable encryption even if no one else would, including the White House. Privacy advocates who expected the worst weren't disappointed.

Senator Ron Wyden, D-Ore., told *The Intercept* in an emailed statement the draft was concerning. "This legislation says a company can design what they want their back door to look like, but it would definitely require them to build a back door. For the first time in America, companies who want to provide their customers with stronger security would not have that choice – they would be required to decide how to weaken their products to make you less safe."

"Burr-Feinstein may be the most insane thing I've ever seen seriously offered as a piece of legislation. It is 'do magic' in legalese," tweeted Julian Sanchez, a senior fellow at the Cato Institute studying privacy and technology.

"Well, the Feinstein-Burr bill is pretty much as clueless and unworkable as I expected it would be," tweeted Matthew Green, a cryptography professor at Johns Hopkins University.

Expert technologists have concluded that you can't design strong encryption that can be readily dismantled or pierced for law enforcement while still keeping customers' communications private and secure from others — like criminals and hackers.

“No person or entity is above the law,” reads the beginning of the bill draft. “All providers of communications services and products (including software) should protect the privacy of United States persons through implementation of appropriate data security and still respect the rule of law and comply with all legal requirements and court orders.”

The bill would specifically require companies to decrypt communications “in a timely manner” or provide “technical assistance” in order to override any security measures preventing access to “intelligible” data — precisely what the FBI ordered Apple to do in order to access San Bernardino killer Syed Rizwan Farook’s work phone before finding an alternate way in.

Apple fought the FBI, arguing that in order to override the phone’s security features, the company would have to design a type of software “cancer” that would risk the security of all Apple users.

The FBI in that case cited the All Writs Act as giving it the authority to force Apple to provide “reasonable assistance” to carry out its warrant and unlock the phone. The new draft bill would take the law a step further. “Feinstein-Burr decryption doesn’t require only reasonable assistance: It’s ‘assistance as is necessary’ to decrypt,” tweeted Orin Kerr, a law professor at George Washington University specializing in computer crime.

Providers of all communications “products,” including pretty much any smartphone provider, would also be responsible for third-party applications that provide encryption services on their behalf.

“Not only does this bill undermine our security, it is also a massive internet censorship bill, demanding that online platforms like Apple’s App Store and the Google Play Store police their platforms to stop the distribution of secure apps,” wrote Kevin Bankston, director of the Open Technology Institute, in a message to *The Intercept*. Computer scientist Jonathan Mayer wrote about the dangers of requiring Google to comply, noting that it would be “deeply incompatible with modern software platforms.” And for apps not relying on Google’s native Android, “The jurisdictional obstacles to regulation are insurmountable,” he continued.

The bill attempts to reassure companies that they will not have to redesign their products, “but to comply, Apple would need to do exactly that,” wrote Jonathan Zdziarski, a security researcher and iOS expert, in a tweet.