New US Bill would require makers of encrypted devices to leave a backdoor

Dave LeClair

The Lawful Access to Encrypted Data Act could be a crushing blow to privacy in the US.

The bill would require manufacturers to leave a backdoor that the government could access when needed.

There's plenty of opposition to the bill from security and privacy advocates.

US Senators have introduced a new anti-encryption bill called the "Lawful Access to Encrypted Data Act," which would require makers of encrypted devices and operating systems to leave a backdoor that could allow law enforcement to access encrypted information when requested. Basically, this means that all manufacturers would need to leave a backdoor in their encryption, which defeats the entire point of encryption in the first place.

Lawful Access to Encrypted Data Act

The Lawful Access to Encrypted Data Act would bring an end to warrant-proof encryption in devices, platforms, and systems, which could be a huge deal for both companies who make encrypted services and devices and the users who enjoy the privacy offered by them, according to the plan laid out in the bill.

Senate Judiciary Committee Chairman Lindsey Graham said, "Terrorists and criminals routinely use technology, whether smartphones, apps, or other means, to coordinate and communicate their daily activities."

Graham went on: "This bill will ensure law enforcement can access encrypted material with a warrant based on probable cause and help put an end to the Wild West of crime on the internet."

There are a few issues that would be a problem for end-users. First, there's the argument of whether this is in violation of any rights to privacy. Second, there's the issue that once a backdoor is purposefully left in for the use by law enforcement, that same backdoor could be found and exploited by more malicious individuals, thus making the encryption all but useless.

According to Bitcoin.com, Riana Pfefferkorn, associate director of surveillance and cybersecurity at the Center for Internet and Society at Stanford Law School, said that the bill is "a full-frontal nuclear assault on encryption in the United States." That's just about as terrifying as it sounds. Even if you're not worried about the government gaining access to your private information because you're not doing anything illegal, there are far worse people than the government that you need to worry about.

EDITOR'S PICK
How does encryption work? – Gary explains

There are those who question the true intent of the Lawful Access to Encrypted Data Act. For example, Andi Wilson Thompson, a senior policy analyst at New America's Open Technology Institute, says, "This bill is just another attack on encryption, and trying to portray it as a 'balanced solution' that could protect privacy is just an attempt to distract from its true intent."

Thompson also added that "This bill would ensure that companies that provide products and services used by millions in the United States have to offer weaker encryption technology, putting all of their users at risk." That's some scary stuff when you sit back and think about how much you have stored on the internet and how much of it is private in nature.

It's not like this is a theoretical issue, either. There have already been multiple instances of the government demanding encryption keys from major tech companies where the companies refused. Both Telegram and Apple had this happen, and the privacy of the users was protected. If this new bill goes through, that wouldn't happen anymore in the US, as the companies in question wouldn't be allowed to forbid access.