Forbes

These Senators Want To Force Tech Firms To Give The Cops Keys To Our Encrypted Data

Rob Pegoraro

June 24, 2020

A new bill labels the end-to-end encryption that tech companies offer to protect our data from others—including the tech companies themselves—not a feature but a bug that deserves the uglier name of "warrant-proof encryption." And a federal ban on its use.

The "Lawful Access to Encrypted Data Act" announced Tuesday by Sens. Lindsey Graham (R-SC), Tom Cotton (R-AR), and Marsha Blackburn (R-TN), would compel hardware, software and services vendors to make your data unlockable with a search warrant.

How is left as an exercise for the companies involved—what Cato Institute policy analyst Julian Sanchez calls a "nerd harder" directive.

That is a dreadful idea, but it's not a new exhibit of Congress' tradition of ignoring technical principles to make impossible or implausible demands of tech companies (Sanchez first tweeted his catchphrase in 2016).

The problem here remains that hacking tools have the bad habit of leaving the toolkits of the law-enforcement investigators who say they need them for such threats as the "terrorism, child sexual abuse, and international drug trafficking" denounced in Graham, Cotton and Blackburn's press release.

(Publicists for their offices did not respond to emails sent Wednesday morning.)

"A backdoor created for law enforcement is a back door created for everyone, including the bad guys," said Greg Nojeim, senior counsel at the Center for Democracy & Technology.

See, for instance, how the Central Intelligence Agency's failure to secure a collection of hacking techniques led to them appearing in WikiLeaks' Vault 7 disclosures.

There's also the problem that these tools exist in the first place: Police departments have been using GrayKey hardware since at least 2018 to get into locked iPhones, even some of last year's models.

This bill would not just round up the usual Big Tech suspects that theoretically have the money to engineer its security-stripping demands. A copy posted by the Electronic Privacy Information Center, a Washington non-profit, reveals it would also cover:

• any "consumer electronic device" with more than a gigabyte of storage and developed by a company that sold more than a million such gadgets in the U.S.;

• any "remote computing service" provider or operating system vendor with more than a million subscribers or users in the U.S. in 2016 or onwards;

• any communications service with more than a million active users a month in January 2016 or any more recent month.

That's way more than the full-device encryption on iOS and Android devices—one area for possible compromise suggested in a 2019 report from the Carnegie Endowment for International Peace—or the end-to-end encryption of conversations in Facebook's WhatsApp and Apple AAPL 's iMessage.

This would also sweep in the secure browser sync offered by Mozilla Firefox and the end-to-end encryption password-manager services employ to ensure that even if they get hacked, your saved logins stay safe.

The bill would not, however, stop people from installing aftermarket encryption—as it seems to admit in provisions exempting tech firms if "independent actions of an unaffiliated entity" stop them from unlocking user data.

Those alternatives include open-source efforts like the Signal encrypted-messaging app and the VeraCrypt disk-encryption software that lie beyond the reach of any one government, and which the terrorists, child abusers and drug lords can use too.

"Criminals will simply turn to those methods and the rest of the population that doesn't have the technical acumen to do that will be left vulnerable," CDT's Nojeim said.

But while his argument isn't new, some things have changed from the encryption arguments of such earlier, simpler times as the spring of 2016, when President Obama urged tech companies not to "take an absolutist view" of privacy.

The past three years have shown how much the Trump administration can politicize law enforcement, especially under the reign of Attorney General William Barr. Barr praised the bill in a statement one day before testimony in Congress provided new evidence of his willingness to act as the president's political commissar in the Justice Department.

More recently, we've seen via smartphone video and network news just how local police departments can abuse their power over suspects and even nonviolent protesters.

Now these three senators want to make tech companies giftwrap a golden key for their encryption and give it to Bill Barr and the cops that people have been protesting?

The phrase "read the room" seems made for this situation.

But the trio dropping their bill in late June of an election year—when Congress would have little time to consider it even without the novel-coronavirus pandemic—suggests they think calling for cracks in computing security is a message that will actually encourage some Americans to vote for candidates like them.