# Encryption battle reignited as US govt at loggerheads with Apple

January 14 2020


The US attorney general claimed Apple has failed to provide enough help to unlock iPhones used in a deadly December shooting spree, reviving a debate on law enforcement access to encrypted devices

Apple and the US government are at loggerheads for the second time in four years over unlocking iPhones connected to a mass shooting,

reviving debate over law enforcement access to encrypted devices.

Attorney General Bill Barr said Monday that Apple failed to provide "substantive assistance" in unlocking two iPhones in the investigation into the December shooting deaths of three US sailors at a Florida naval station, which he called an "act of terrorism."

Apple disputed Barr's claim, while arguing against the idea of "backdoors" for law enforcement to access its encrypted smartphones.

"We reject the characterization that Apple has not provided substantive assistance in the Pensacola investigation," the company said in a statement.

"Our responses to their many requests since the attack have been timely, thorough and are ongoing."

Late on Tuesday, President Donald Trump weighed in on Twitter, saying the government was helping Apple on trade issues "yet they refuse to unlock phones used by killers, drug dealers and other violent criminal elements."

"They will have to step up to the plate and help our great Country, NOW!" he added.

The standoff highlighted the debate between law enforcement and the tech sector about encryption—a key way to protect the privacy of digital communications, but which can also make investigations difficult, even with a court order.

The latest battle is similar to the dispute between Apple and the US Justice Department after the December 2015 mass shooting in San Bernardino, California, when the iPhone maker rejected a request to

develop software to break into the shooter's iPhone.

Attorney General Bill Barr has called on both Facebook and Apple to provide better access to law enforcement seeking access to encrypted devices and content

That fight ended in 2016 when the government paid an outside party a reported $1 million for a tool that circumvented Apple's iPhone encryption.

Barr last year called on Facebook to allow authorities to circumvent encryption to fight extremism, child pornography and other crimes. The social network has said it would move ahead with strong encryption for its messaging applications.

## Opening wrong doors?

Digital rights activists argue that any privileged access for law enforcement would weaken security and make it easier for hackers and authoritarian governments to intercept messages.

"We have always maintained there is no such thing as a backdoor just for the good guys," Apple's statement said.

"Backdoors can also be exploited by those who threaten our national security and the data security of our customers."

Apple and others argue that digital "breadcrumbs" make it increasingly easy to track people, even without breaking into personal devices.

The government's latest demand "is dangerous and unconstitutional, and would weaken the security of millions of iPhones," Jennifer Granick of the American Civil Liberties Union said in a statement.

"Strong encryption enables religious minorities facing genocide, like the Uighurs in China, and journalists investigating powerful drug cartels in Mexico, to communicate safely."

Apple has been implementing stronger encryption on its iPhones, making it harder for law enforcement to access the devices

Granick added that Apple cannot allow the FBI access to encrypted communications "without also providing it to authoritarian foreign governments and weakening our defenses against criminals and hackers."

Kurt Opsahl of the Electronic Frontier Foundation echoed that sentiment, saying Apple "is right to provide strong security" for its devices.

"The AG (attorney general) requesting Apple re-engineer its phones to break that security is a poor security trade-off, and imperils millions of innocent people around the globe," Opsahl tweeted.

James Lewis of the Center for Strategic and International Studies, a Washington think tank, said he believes it's possible to allow law enforcement access without sacrificing encryption.

"You're not weakening encryption, you're making it so it's not end-to-end," Lewis told AFP.

"It means that there's a third party who can look at it under appropriate authority."

But Lewis said he does not expect either side to come out a winner in the battle, and that US officials will likely find another outside party to crack the two iPhones belonging to the shooter, Royal Saudi Air Force 2nd Lieutenant Mohammed Saeed Alshamran, who died in the attack.

"It's a repeat of the movie we saw in San Bernardino," he said.

"It's going to be harder because Apple probably fixed the trick that worked in San Bernardino."