REUTERS

TECHNOLOGY NEWS

JANUARY 21, 2020 / 12:07 PM / UPDATED 37 MINUTES AGO

# Exclusive: Apple dropped plan for encrypting backups after FBI complained - sources

Joseph Menn

SAN FRANCISCO (Reuters) - Apple Inc (AAPL.O) dropped plans to let iPhone users fully encrypt backups of their devices in the company's iCloud service after the FBI complained that the move would harm investigations, six sources familiar with the matter told Reuters.


The tech giant's reversal, about two years ago, has not previously been reported. It shows how much Apple has been willing to help U.S. law enforcement and intelligence agencies, despite taking a harder line in high-profile legal disputes with the government and casting itself as a defender of its customers' information.

The long-running tug of war between investigators' concerns about security and tech companies' desire for user privacy moved back into the public spotlight last week, as U.S. Attorney General William Barr took the rare step of publicly calling on Apple to unlock two iPhones used by a Saudi Air Force officer who shot dead three Americans at a Pensacola, Florida naval base last month.

U.S. President Donald Trump piled on, accusing Apple on Twitter of refusing to unlock phones used by "killers, drug dealers and other violent criminal elements." Republican and Democratic senators sounded a similar theme in a December hearing, threatening legislation against end-to-end encryption, citing unrecoverable evidence of crimes against children.

Apple did in fact did turn over the shooter's iCloud backups in the Pensacola case, and said it rejected the characterization that it "has not provided substantive assistance."

Behind the scenes, Apple has provided the U.S. Federal Bureau of Investigation with more sweeping help, not related to any specific probe.

An Apple spokesman declined to comment on the company's handling of the encryption issue or any discussions it has had with the FBI. The FBI did not respond to requests for comment on any discussions with Apple.

More than two years ago, Apple told the FBI that it planned to offer users end-to-end encryption when storing their phone data on iCloud, according to one current and three former FBI officials and one current and one former Apple employee.

Under that plan, primarily designed to thwart hackers, Apple would no longer have a key to unlock the encrypted data, meaning it would not be able to turn material over to authorities in a readable form even under court order.

In private talks with Apple soon after, representatives of the FBI's cyber crime agents and its operational technology division objected to the plan, arguing it would deny them the most effective means for gaining evidence against iPhone-using suspects, the government sources said.

FILE PHOTO: A woman uses her Apple iPhone and laptop in a cafe in lower Manhattan in New York City, U.S., May 8, 2019. REUTERS/Mike Segar/File Photo

When Apple spoke privately to the FBI about its work on phone security the following year, the end-to-end encryption plan had been dropped, according to the six sources. Reuters could not determine why exactly Apple dropped the plan.

“Legal killed it, for reasons you can imagine,” another former Apple employee said he was told, without any specific mention of why the plan was dropped or if the FBI was a factor in the decision.

That person told Reuters the company did not want to risk being attacked by public officials for protecting criminals, sued for moving previously accessible data out of reach of government agencies or used as an excuse for new legislation against encryption.

“They decided they weren’t going to poke the bear anymore,” the person said, referring to Apple’s court battle with the FBI in 2016 over access to an iPhone used by one of the suspects in a mass shooting in San Bernardino, California.

Apple appealed a court order to break into that phone for the FBI. The government dropped the proceedings when it found a contractor that could break into the phone, a common occurrence in FBI investigations.

Two of the former FBI officials, who were not present in talks with Apple, told Reuters it appeared that the FBI's arguments that the backups provided vital evidence in thousands of cases had prevailed.

"It's because Apple was convinced," said one. "Outside of that public spat over San Bernardino, Apple gets along with the federal government."

However, a former Apple employee said it was possible the encryption project was dropped for other reasons, such as concern that more customers would find themselves locked out of their data more often.

Once the decision was made, the 10 or so experts on the Apple encryption project - variously code-named Plesio and KeyDrop - were told to stop working on the effort, three people familiar with the matter told Reuters.

## APPLE SHIFTS FOCUS

Apple's decision not to proceed with end-to-end encryption of iCloud backups made the FBI's job easier.

The agency relies on hacking software that exploits security flaws to break into a phone. But that method requires direct access to the phone which would ordinarily tip off the user, who is often the subject of the investigation.

Apple's iCloud, on the other hand, can be searched in secret. In the first half of last year, the period covered by Apple's most recent semiannual transparency report on requests for data it receives from government agencies, U.S. authorities armed with regular court papers asked for and obtained full device backups or other iCloud content in 1,568 cases, covering about 6,000 accounts.

Slideshow (2 Images)

The company said it turned over at least some data for 90% of the requests it received. It turns over data more often in response to secret U.S. intelligence court directives, topping 14,000 accounts in the second half of 2018. Because of gag orders, Apple has not given any such data for 2019.

Had it proceeded with its plan, Apple would not have been able to turn over any readable data belonging to users who opted for end-to-end encryption.

Instead of protecting all of iCloud with end-to-end encryption, Apple has shifted to focus on protecting some of the most sensitive user information, such as saved passwords and health data.

But backed-up contact information and texts from iMessage, WhatsApp and other encrypted services remain available to Apple employees and authorities.

Apple is not the only tech company to have removed its own access to customers' information.

In October 2018, Alphabet Inc's (GOOGL.O) Google announced a similar system to Apple's dropped plan for secure backups. The maker of Android software, which runs on about three-quarters of the world's mobile devices, said users could back up their data to its own cloud without trusting the company with the key.

Two people familiar with the project said Google gave no advance notice to governments, and picked a time to announce it when encryption was not in the news.

The company continues to offer the service but declined to comment on how many users have taken up the option. The FBI did not respond to a request for comment on Google's service or the agency's approach to it.

Reporting by Joseph Menn in San Francisco; Editing by Bill Rigby

*Our Standards:* *The Thomson Reuters Trust Principles.*