Apple: Most iCloud data can now be end-to-end encrypted

December 7 2022, by Frank Bajak

The Apple logo is illuminated at a store in the city center in Munich, Germany, on Dec. 16, 2020. Apple said Wednesday, Dec. 7, 2022, that it will now offer full end-to-encryption for nearly all the data its users store in its global cloud-based storage system. That will make it more difficult for hackers, spies and law enforcement agencies to access sensitive user information. Credit: AP Photo/Matthias Schrader, File

As part of an ongoing privacy push, Apple said Wednesday it will now offer full end-to-encryption for nearly all the data its users store in its global cloud-based storage system. That will make it more difficult for hackers, spies and law enforcement agencies to access sensitive user information.

The world's most valuable company has long placed customer security and privacy at a premium. Its iMessage and Facetime communications services are fully encrypted end-to-end and it has sometimes locked horns with law enforcement agencies, including the FBI, over its refusal to unlock devices.

But a lot of what customers backed up remotely using Apple's iCloud service—including photos, videos and chats—has not been afforded uncompromising protection through end-to-end encryption, a technology that prevents even Apple from decrypting it. That has made it easier for crooks, spies—and criminal investigators with court orders—to get at it.

No longer. The loophole that law enforcement had for getting at iPhone data will now be considerably narrowed.

Apple, which is based in Cupertino, California, did not respond to requests for comment on the timing of the announcement and other issues.

The FBI expressed displeasure.

In a statement, it said it remains a strong advocate of encryption schemes that provide "lawful access by design" so tech companies "served with a legal order" can decrypt data and give it to law enforcement. The agency said it "continues to be deeply concerned with the threat end-to-end and user-only-access encryption pose," insisting they hinder the FBI's ability to protect Americans from crimes ranging from cyberattacks to violence

against children, and terrorism.

Cryptographers and other cybersecurity experts have long argued, however, that attempts by law enforcement to weaken encryption with backdoors are ill-advised because they would inherently make the internet less reliable and hurt vulnerable populations including ethnic minorities.

Last year, Apple announced, then withdrew after a flood of objections, a plan to scan iPhones for photos of child sexual abuse material, or CSAM.

"Where Apple was hesitant about deploying encryption features last year—maybe even backsliding a bit with CSAM scanning proposals—it now feels like they've decided to put the gas pedal down," noted Johns Hopkins cryptography professor Matthew Green on Twitter.

Apple's encryption announcement offers what the company calls Advanced Data Protection, to which users of its devices must opt in. It adds iCloud Backup, Notes and Photos to data categories that are already protected by end-to-end encryption in the cloud, including health data and passwords. Not included in the iCloud encryption scheme are email, contacts and calendar items because they must interoperate with products from other vendors, Apple said.

It said Advanced Data Protection for iCloud would be available to U.S. users by the end of the year and start rolling out to the rest of the world in early 2023.

In a blog post, Apple said "enhanced security for users' data in the cloud is more urgently needed than ever," citing research that says data breaches have more than tripled over the past eight years.

Other tech products that already offer end-to-end encryption include the world's most popular messaging app, WhatsApp, and Signal, a communications app prized by journalists, dissidents, human rights activists and other dealers in sensitive data.

Apple announced a few other advanced security features on Wednesday, including one geared toward journalists, human rights activists and government officials who "face extraordinary digital threats"—such as from no-click spyware. Called iMessage Contact Key Verification, it will automatically alert users to eavesdroppers who succeed in inserting a new device into their iCloud via a breach.

In July, Apple announced a new optional feature called Lockdown Mode that is designed to protect iPhones and its other products against intrusions from state-backed hackers and commercial spyware.

Apple said at the time that it believed the extra layer of protection would be valuable to targets of hacking attacks launched by well-funded groups.

Users are able to activate and deactivate lockdown mode at will.

Citation: Apple: Most iCloud data can now be end-to-end encrypted (2022, December 7) retrieved 22 March 2023 from https://techxplore.com/news/2022-12-apple-beefs-icloud-defense-snooping.html