

Apple revives encryption debate with move on child exploitation

August 6 2021, by Rob Lever



Apple claims it can flag images showing child sexual abuse without weakening encryption but critics warn the tool could be exploited by others.

Apple's announcement that it would scan encrypted messages for evidence of child sexual abuse has revived debate on online encryption

and privacy, raising fears the same technology could be used for government surveillance.

The iPhone maker said its initiative would "help protect children from predators who use [communication tools](#) to recruit and exploit them, and limit the spread of child [sexual abuse](#) material."

The move represents a major shift for Apple, which has until recently resisted efforts to weaken its [encryption](#) that prevents third parties from seeing [private messages](#).

Apple argued in a technical paper that the technology developed by cryptographic experts "is secure, and is expressly designed to preserve user privacy."

The company said it will have limited access to the violating images which would be flagged to the National Center for Missing and Exploited Children, a [nonprofit organization](#).

Nonetheless, encryption and private specialists warned the tool could be exploited for other purposes, potentially opening a door to mass surveillance.

"This sort of tool can be a boon for finding child pornography in people's phones. But imagine what it could do in the hands of an authoritarian government?" said a tweet from Matthew Green, a cryptographer at Johns Hopkins University.

Others warned that the move could be a first step toward weakening encryption and opening "back doors" which could be exploited by hackers or governments.

"There's going to be enormous pressure on Apple from governments

around the world to expand this capability to detect other kinds of 'bad' content, and significant interest by attackers across the spectrum in finding ways to exploit it," tweeted Matt Blaze, a Georgetown University computer scientist and cryptography researcher.

Blaze said the implementation is "potentially very risky" because Apple has moved from scanning data on services to the phone itself and "has potential access to all your local data."



In this file photo taken on September 20, 2019 a woman looks at her mobile phone as she walks past advertising for the new iPhone 11 Pro smartphone at an Apple store in Hong Kong.

Tools to protect children

The new image-monitoring feature is part of a series of tools heading to Apple mobile devices, according to the company.

Apple's texting app, Messages, will use machine learning to recognize and warn children and their parents when receiving or sending sexually explicit photos, the company said in the statement.

"When receiving this type of content, the photo will be blurred and the child will be warned," Apple said.

"Apple's expanded protection for children is a game changer," said John Clark, president of the nonprofit NCMEC.

The move comes following years of standoffs involving technology firms and [law enforcement](#).

Apple notably resisted a legal effort to weaken iPhone encryption to allow authorities to read messages from a suspect in a 2015 bombing in San Bernardino, California.

FBI officials have warned that so-called "end to end encryption," where only the user and recipient can read messages, can protect criminals, terrorists and pornographers even when authorities have a legal warrant for an investigation.



WhatsApp, the popular Facebook-owned messaging app, said it would not follow Apple's lead in scanning private images to report child sexual abuse.

Different tack for WhatsApp

Facebook, which has faced criticism that its encrypted messaging app facilitates crime, has been studying the use of artificial intelligence to analyze the content of messages without decrypting them, according to a recent report by The Information.

But WhatsApp head Will Cathcart said the popular messaging app would not follow Apple's approach.

"I think this is the wrong approach and a setback for people's privacy all over the world," Cathcart tweeted.

Apple's system "can scan all the private photos on your phone—even photos you haven't shared with anyone. That's not privacy," he said.

"People have asked if we'll adopt this system for WhatsApp. The answer is no."

Backers of encryption argue that authorities already have multiple sources of "digital breadcrumbs" to track nefarious activity and that any tools to break encryption could be exploited by bad actors.

James Lewis, who heads technology and [public policy](#) at the Center for Strategic and International Studies, said Apple's latest move appears to be a positive step, noting that the company is identifying offending

material while avoiding directly turning over data to law enforcement.

But he said it's unlikely to satisfy the concerns of security agencies investigating extremism and other crimes.

"Apple has done a good job of balancing public safety and privacy but it's not enough for some of the harder security problems," Lewis said.

© 2021 AFP

Citation: Apple revives encryption debate with move on child exploitation (2021, August 6)
retrieved 28 April 2024 from

<https://techxplore.com/news/2021-08-apple-revives-encryption-debate-child.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--