AUG 09
Mack DeGeurin

Apple faces privacy dilemma with new child exploitation scanner

Article

The news: **Apple** is preparing to roll out an image scanning tool that will **inspect users' images for child sexual abuse media** (CSAM) on iPhones and iCloud**,** according to leaks from John Hopkins University cryptography professor **Matthew Green** later confirmed by The Financial Times and Apple. Though other major cloud services already scan for child sexual

abuse and other harmful content, Apple's software works differently, **scanning images locally on a user's device** before it ever reaches iCloud.

How it works: The software, called **"neuralMatch,"** would use a hashing technology called **NeuralHash** to **scan images on a user's device** and cross-reference them with a database of known CSAM files, all without decrypting the data.

If enough similarities are flagged, the user's data is then reviewed by an Apple employee, and passed along to law enforcement if necessary.

Apple said it's developing another feature that will take action when a user searches for CSAM terms via Siri or Search, as well as new tools that will warn users if a child sends or receives sexual content through the Messages app. It's worth underscoring that while Apple confirmed plans to roll out the features for iOS 15 and macOS Monterey in coming months, **it did so only after leaks and media reports** made the controversial new initiatives public.

Why now? Apple's decision **marks a departure from its industry-leading, hard-line approach to encryption** and comes amid growing calls from lawmakers in the US and around the world to weaken encryption by providing backdoors to law enforcement, often using child exploitation as the principal justification.

The pushback: Though neuralMatch could make a meaningful difference in deterring circulation of CSAM, the program immediately aroused fears from a diverse cast of privacy and security experts over potential misuse.

- The Electronic Frontier Foundation described Apple's move as an "about-face" on user privacy and **accused Apple of opening up a backdoor** for law enforcement.
- Meanwhile, others like infamous National Security Agency whistleblower **Edward Snowden**, worry Apple could expand its search capabilities beyond child sexual abuse content.
- Others still, like the original leaker Matthew Green, have expressed concern over Apple's use of problematic child abuse hashes, which are pulled from a database inaccessible to the public, leaving third parties powerless to review Apple's decision.
- Responding to the criticism in a memo obtained by 9to5 Mac, software vice president Sebastian Marineau-Mes said Apple plans on moving forward despite "misunderstandings" from critics. The new features, Marineau-Mes wrote, will deliver "tools to protect children, but also maintain Apple's deep commitment to user privacy. "

The bigger picture: Despite its good intentions, neuralMatch could muddy Apple's reputation as the vanguard of consumer privacy and bulwark against government anti-encryption efforts. **Apple risks replicating a misstep made by WhatsApp earlier this year**, where user backlash to its new privacy update tarnished its brand identity, resulting in surging downloads of competing messaging apps.

The bottom line: Public perception of a major privacy shift and continued opposition from vocal privacy leaders could present a major challenge for Apple in maintaining its brand image and users' trust.