Apple to work with law enforcement to scan personal photo libraries for child abuse content

Kevin Reed
11 August 2021

In a significant encroachment on civil liberties, Apple announced on August 5 that it plans to begin scanning the photos on all of its personal computing devices and iCloud storage content for the presence of known images of "sexually explicit activities involving a child."

In a statement published on its website entitled "Expanded Protections for Children," Apple said that it wants to "help protect children from predators who use communication tools to recruit and exploit them and limit the spread of Child Sexual Abuse Material (CSAM)."

The statement said that Apple had created "child safety features in three areas, developed in collaboration with child safety experts" and that these features would be "coming later this year" in the new releases of its operating systems "iOS 15, iPadOS 15, watchOS 8, and macOS Monterey."

The three areas where the expanded features will be implemented are in its text messaging app, such that children and their parents will be warned "when receiving or sending sexually explicit photos," in on-device scanning of images "to detect known CSAM images stored in iCloud Photos" and in expanded guidance in Siri (Apple's virtual assistant) and Search "to help children and parents stay safe online and get help with unsafe situations."

Apple's statement says, "This program is ambitious, and protecting children is an important responsibility. These efforts will evolve and expand over time." The company also says that the program will be implemented only in the US.

The implementation of the on-device image scanning will be integrated with a reporting system that sends data to the National Center for Missing and Exploited Children (NCMEC) and Apple says that "NCMEC acts as a comprehensive reporting center for CSAM and works in collaboration with law enforcement agencies across the United States."

Notably, the company says that it will scan the personal photo libraries of iPhone and iPad users "with user privacy in mind." It claims that on-device matching of images to a "database of known CSAM image hashes provided by NCMEC and other child safety organizations." The other organizations are not named.

In a strained effort to explain how user privacy will be protected with the new invasive system, the company statement goes into the technical details. It says that Apple transforms the database into "an unreadable set of hashes that is securely stored on users' devices." An image hash is a kind of digital fingerprint of a specific photo such that copies of it are easily identifiable.

The explanation says that the matching to the database of image hashes is performed on the device before the images are synchronized with iCloud and "is powered by a cryptographic technology called private set intersection, which determines if there is a match without revealing the result. The device creates a cryptographic safety voucher that encodes the match result along with additional encrypted data about the image. This voucher is uploaded to iCloud Photos along with the image."

Furthermore, Apple says that another technology called "threshold secret sharing" ensures that the content of the "safety vouchers" cannot be interpreted by Apple "unless the iCloud Photos account crosses a threshold of known CSAM content." While Apple does not specify what the threshold is, it says it is "set to provide an extremely high level of accuracy and ensures less than a one in one trillion chance per year of incorrectly flagging a given account."

According to the statement, once the threshold has been breached, Apple then "manually reviews each report to

confirm there is a match, disables the user's account, and sends a report to NCMEC. If a user feels their account has been mistakenly flagged, they can file an appeal to have their account reinstated."

Apple's announcement was immediately denounced by technology, cybersecurity and privacy advocates. Matthew D. Green, a cryptography professor at Johns Hopkins University, told the *New York Times* that Apple's new features "set a dangerous precedent by creating surveillance technology that law enforcement or governments could exploit." Green went on, "They've been selling privacy to the world and making people trust their devices. But now they're basically capitulating to the worst possible demands of every government. I don't see how they're going to say no from here on out."

Greg Nojeim, co-director of the Security & Surveillance Project at the Center for Democracy & Technology, told CNN, "Apple is replacing its industry-standard end-to-end encrypted messaging system with an infrastructure for surveillance and censorship, which will be vulnerable to abuse and scope-creep not only in the US, but around the world. Apple should abandon these changes and restore its users' faith in the security and integrity of their data on Apple devices and services."

In a lengthy statement, the Electronic Frontier Foundation (EFF) said, "All it would take to widen the narrow backdoor that Apple is building is an expansion of the machine learning parameters to look for additional types of content, or a tweak of the configuration flags to scan, not just children's, but anyone's accounts. That's not a slippery slope; that's a fully built system just waiting for external pressure to make the slightest change."

Whistleblower and former intelligence analyst Edward Snowden tweeted, "No matter how well-intentioned, @Apple is rolling out mass surveillance to the entire world with this. Make no mistake: if they can scan for kiddie porn today, they can scan for anything tomorrow. They turned a trillion dollars of devices into iNarcs—'without asking.'"

In response to the deluge of opposition and denunciations, Apple issued on Friday a Frequently Asked Questions document that only served to further expose the bundle of contradictions that the tech monopoly is embroiling within. To the question, "Does this mean Apple is going to scan all the photos stored on my iPhone?" the company responded, "No. By design, this feature only applies to photos that the user chooses to upload to iCloud Photos. ... The system does not work for users who have iCloud Photos disabled. This feature does not work on your private iPhone photo library on the device."

Apparently, Apple is telling customers concerned about privacy invasion that they should not use one of the key features of its platform: the ability to take photos on one device and store them in the cloud such that they can be viewed and accessed by all other devices. In other words, with their CSAM initiative, Apple is destroying its own technology.

Meanwhile, in an internal memo leaked to the news media, Apple defended its plans saying that the widespread opposition was the result of "misunderstandings." While claiming that there have been many "positive responses," the memo included a note from the NCMEC that said, "We know that the days coming will be filled with the screeching voices of the minority."

Beyond the technical and user aspects, the political content of Apple's invasion of privacy initiative dovetails entirely with a right-wing bipartisan bill introduced by the Senate Judiciary Committee in March 2020 aimed purportedly at stopping "online child exploitation."

Jointly introduced by Senate Judiciary Committee Chairman Lindsey Graham (Republican of South Carolina), US Senators Richard Blumenthal (Democrat of Connecticut), Josh Hawley (Republican of Missouri) and Ranking Member Dianne Feinstein (Democrat of California), the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act (EARN IT Act) demanded that online service providers monitor and censor all content on their systems for CSAM in order to qualify for the Section 230 provisions of the Communications Decency Act of 1996.

The going over of Apple to the undemocratic policies of the entire American political and law enforcement establishment is predictable. The massive corporate monopoly and number one entity on Wall Street—with a staggering $2.4 trillion market valuation—is incapable of maintaining even a fig leaf of adherence to democratic rights and defending the Fourth Amendment guarantee against unreasonable searches and seizures.