Urban Justice Center

Sex Workers' rights and Human Trafficking

https://www.urbanjustice.org/2021/08/19/apple-photo-scanning-plan-faces-global-backlash-from-90-rights-groups/

Public Facing Advocacy Writing

Front page layout

Site theme

Sign up or login to join the discussions!

Jon Brodkin - Aug 19, 2021 6:12 pm UTC

More than 90 policy groups from the US and around the world signed an open letter urging Apple to drop its plan to have Apple devices scan photos for child sexual abuse material (CSAM).

"The undersigned organizations committed to civil rights, human rights, and digital rights around the world are writing to urge Apple to abandon the plans it announced on 5 August 2021 to build surveillance capabilities into iPhones, iPads, and other Apple products," the letter to Apple CEO Tim Cook said today. "Though these capabilities are intended to protect children and to reduce the spread of child sexual abuse material (CSAM), we are concerned that they will be used to censor protected speech, threaten the privacy and security of people around the world, and have disastrous consequences for many children."

The Center for Democracy & Technology (CDT) announced the letter, with CDT Security & Surveillance Project Co-Director Sharon Bradford Franklin saying, "We can expect governments will take advantage of the surveillance capability Apple is building into iPhones, iPads, and computers. They will demand that Apple scan for and block images of human rights abuses, political protests, and other content that should be protected as free expression, which forms the backbone of a free and democratic society."

The open letter was signed by groups from six continents (Africa, Asia, Australia, Europe, North America, and South America). Some of the US-based signers are the American Civil Liberties Union, the Electronic Frontier Foundation, Fight for the Future, the LGBT Technology Partnership & Institute, New America's Open Technology Institute, STOP (Surveillance Technology Oversight Project), and the Sex Workers Project of the Urban Justice Center. Signers also include groups from Argentina, Belgium, Brazil, Canada, Colombia, the Dominican Republic, Germany, Ghana, Guatemala, Honduras, Hong Kong, India, Japan, Kenya, Mexico, Nepal, the Netherlands, Nigeria, Pakistan, Panama, Paraguay, Peru, Senegal, Spain, Tanzania, and the UK. The full list of signers is here.

Apple announced two weeks ago that devices with iCloud Photos enabled will scan images before they are uploaded to iCloud. An iPhone uploads every photo to iCloud right after it is taken, so the scanning would happen almost immediately if a user has previously turned iCloud Photos on.

Apple said its technology "analyzes an image and converts it to a unique number specific to that image" and flags a photo when its hash is identical or nearly identical to the hash of any that appear in a database of known CSAM. An account can be reported to the National Center for Missing and Exploited Children (NCMEC) when about 30 CSAM photos are detected, a threshold Apple set to ensure that there is "less than a one in one trillion chance per year of incorrectly flagging a given account." That threshold could be changed in the future to maintain the one-in-one-trillion false-positive rate.

Apple is also adding a tool to the Messages application that will "analyze image attachments and determine if a photo is sexually explicit" without giving Apple access to the messages. The system will be optional for parents and if turned on will "warn children and their parents when receiving or sending sexually explicit photos."

Apple has said the new systems will roll out later this year in updates to iOS 15, iPadOS 15, watchOS 8, and macOS Monterey. It will be in the US only at first.

Advertisement

Both scanning systems are concerning to the open-letter signers. On the Messages scanning that parents can enable, the letter said:

Algorithms designed to detect sexually explicit material are notoriously unreliable. They are prone to mistakenly flag art, health information, educational resources, advocacy messages, and other imagery. Children's rights to send and receive such information are protected in the UN Convention on the Rights of the Child. Moreover, the system Apple has developed assumes that the "parent" and "child" accounts involved actually belong to an adult who is the parent of a child, and that those individuals have a healthy relationship. This may not always be the case; an abusive adult may be the organizer of the account, and the consequences of parental notification could threaten the child's safety and wellbeing. LGBTQ+ youths on family accounts with unsympathetic parents are particularly at risk. As a result of this change, iMessages will no longer provide confidentiality and privacy to those users through an end-to-end encrypted messaging system in which only the sender and intended recipients have access to the information sent. Once this backdoor feature is built in, governments could compel Apple to extend notification to other accounts, and to detect images that are objectionable for reasons

other than being sexually explicit.

On Apple's plan to scan photos for CSAM, the groups wrote:

Many users routinely upload the photos they take to iCloud. For these users, image surveillance is not something they can opt out of; it will be built into their iPhone or other Apple device, and into their iCloud account.

Once this capability is built into Apple products, the company and its competitors will face enormous pressureand potentially legal requirementsfrom governments around the world to scan photos not just for CSAM, but also for other images a government finds objectionable. Those images may be of human rights abuses, political protests, images companies have tagged as "terrorist" or violent extremist content, or even unflattering images of the very politicians who will pressure the company to scan for them. And that pressure could extend to all images stored on the device, not just those uploaded to iCloud. Thus, Apple will have laid the foundation for censorship, surveillance and persecution on a global basis.

The groups urged Apple to "abandon those changes and to reaffirm the company's commitment to protecting its users with end-to-end encryption" and "to more regularly consult with civil society groups, and with vulnerable communities who may be disproportionately impacted by changes to its products and services."

Apple has said it will refuse government demands to expand photo-scanning beyond CSAM. But refusing those demands could be difficult, especially in authoritarian countries with poor human-rights records. Apple has not given any timeline for when it will bring the scanning technology to countries outside the US.

After its plan received a swift backlash from security experts and privacy advocates, Apple said it didn't do a good enough job explaining how it will work. Apple has since provided more detailsfor example,that its CSAM database will only consist of "hashes provided by at leasttwo child safety organizations operating in separate sovereign jurisdictions."Apple's further explanations have been misinterpreted by some news organizations as a change in plans, but the company does not appear to have actually made any substantive changes to the plan since announcing it.

Craig Federighi, Apple's senior VP of software engineering, argued that Apple's new system is "an advancement of the state of the art in privacy" because it will scan photos "in the most privacy-protecting way we can imagine and in the most auditable and verifiable way possible."

"If you look at any other cloud service, they currently are scanning photos by looking at every single photo in the cloud and analyzing it. We wanted to be able to spot such photos in the cloud without looking at people's photos and came up with an architecture to do this,"Federighi told The Wall Street Journal. The Apple system is "much more private than anything that's been done in this area before," he said.