



STATE OF KANSAS
OFFICE OF THE ATTORNEY GENERAL

KRIS W. KOBACH
ATTORNEY GENERAL

MEMORIAL HALL
120 SW 10TH AVE., 2ND FLOOR
TOPEKA, KS 66612-1597
(785) 296-2215 • FAX (785) 296-6296
WWW.AG.KS.GOV

March 20, 2026

Tim Cook
Chief Executive Officer
Apple Inc.
One Apple Park Way
Cupertino, CA 95014

Kate Adams
Chief Legal Officer
Apple Inc.
One Apple Park Way
Cupertino, CA 95014

RE: Apple's Inaction on Child Sexual Abuse Material (CSAM) in iCloud

Dear Mr. Cook and Ms. Adams:

As Kansas's chief law enforcement officer, I have serious concerns over Apple's failure to implement safeguards against the proliferation of child sexual abuse material (CSAM) on its cloud platform, iCloud. This inaction has led to iCloud being a leader in the industry for the distribution of CSAM.¹

For years, Apple has consistently reported significantly less CSAM material than other platforms by claiming it is protecting user privacy.² Despite publicly acknowledging the presence of CSAM on its services and proposing a privacy-preserving detection solution in 2021, by 2022, Apple abandoned its commitment.³ Prior to abandoning the CSAM detection tool, Apple had defended the product stating that it would only scan photos shared on iCloud, it would be nearly impossible to falsely flag innocent people, and that there would be a level of human review on

¹ In the *Epic Games v. Apple* lawsuit in 2021, Apple's head of Fraud, Eric Friedman, acknowledged that Apple is "...the greatest platform for distributing child porn..." <https://embed.documentcloud.org/documents/21044004-2020-february-fear-friedman-admits-in-feb-2020-that-app-store-greatest-platform-for-child-porn-predator-grooming/#document/p17>

² <https://archive.ph/1xCvh>

³ <https://www.cnn.com/2022/12/08/tech/apple-csam-tool>

positive matches.⁴ Despite believing in its product, Apple still chose to abandon the CSAM detection tool, claiming to prioritize privacy of users. Prioritizing the privacy of those uploading CSAM to iCloud over the privacy of the victims is abhorrent.

Contrary to Apple's public narrative, polling conducted by Bellwether Research indicates that over 90% of individuals support policies and features that remove and report CSAM. Over 90% of individuals state that it is extremely important to them that tech companies remove and report CSAM. An overwhelming majority of individuals support the detection and removal of CSAM material even at the cost of some of their own privacy.⁵

Protecting children is of the utmost importance to my office and abandoning efforts that are heavily supported by users to detect CSAM on iCloud has serious and long-lasting consequences. Apple's continued failure to safeguard iCloud allows for CSAM to be in constant circulation - retraumatizing victims and inflicting more psychological harm each and every time it's viewed.⁶ Victims are constantly notified when their images are viewed or shared.⁷ They are forced to relive their trauma every day knowing that their photos are also being used to groom children. Abandoning efforts to detect CSAM is a step towards normalizing its presence on platforms and this material should not be normalized and will not be tolerated in Kansas.

Apple's decision not to implement the CSAM detection tool was more than abandoning a controversial product: it was a marked step away from one of the company's core values of protecting children. Instead of focusing efforts on a new product and recommitting yourselves to aid in the detection of CSAM on iCloud, your company put focus on your Communication Safety Feature – an *opt-in* parental control feature. This falls far short of the mark as individuals distributing CSAM on iCloud are likely not “opting in” to this feature. Additionally, the Communication Safety Feature is only designed to detect nudity, as opposed to scanning for known CSAM.

Nothing is prohibiting you from developing alternative methods for detecting and removing CSAM from iCloud. In fact, the research clearly shows that users want these methods, policies, and tools to be implemented. My team and I closely monitor and work hard to protect against risks to the safety and health of Kansas, particularly its children. To be extremely clear: Kansas will hold Apple accountable if it fails to implement a significant course correction or fails to follow the law.

Marketing defective products, failing to warn consumers and parents of your products' risks, and otherwise engaging in deceptive and unconscionable practices implicates civil liability under the Kansas Consumer Protection Act. K.S.A. 50-623, *et seq.*

⁴ <https://www.bbc.com/news/technology-58145943>

⁵ <https://heatinitiative.org/wp-content/uploads/2024/09/National-Sample-Polling-Toplines.pdf>

⁶ <https://techcrunch.com/2024/12/08/apple-sued-over-abandoning-csam-detection-for-icloud/>

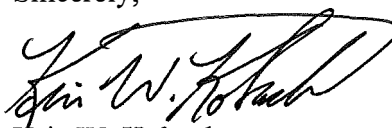
⁷ <https://archive.ph/1xCvh>

Because the stakes are high, I urge you to immediately implement CSAM detection methods in iCloud while preserving privacy and publicly recommit to protecting children on your platforms. I also request additional information about how you intend to safeguard iCloud and comply with Kansas law. Please provide detailed information about the following to my office.

1. Describe, with specificity and detail, how your company approaches user safety.
2. Describe, with specificity and detail, how your company complies with, or intends to implement, age and identity verification measures to prevent access to material harmful to minors.
3. Describe whether, how, and to what degree of certainty your company can ensure that CSAM material is not inappropriately accessed on iCloud.
4. Describe to what extent, if at all, your company monitors the data, information, and pictures stored onto iCloud.
5. Describe, with specificity and detail, how your company intends to prevent the use of iCloud from encouraging or facilitating criminal activity.
6. Describe whether, how, and to what degree of certainty your company can ensure that material containing child pornographic content is not accessed on iCloud.
7. The volume of CSAM reports Apple has received over the past five years.
8. Internal assessments of CSAM prevalence on iCloud.
9. Any current or planned safeguards to detect and remove CSAM.
10. Staffing and resources dedicated to child safety operations.

My office looks forward to reviewing your responses to this letter. Please submit your responses electronically to cprotect@ag.ks.gov and include our file number, CP-26-000155, in the subject line of your correspondence no later than April 17, 2026.

Sincerely,



Kris W. Kobach
Attorney General