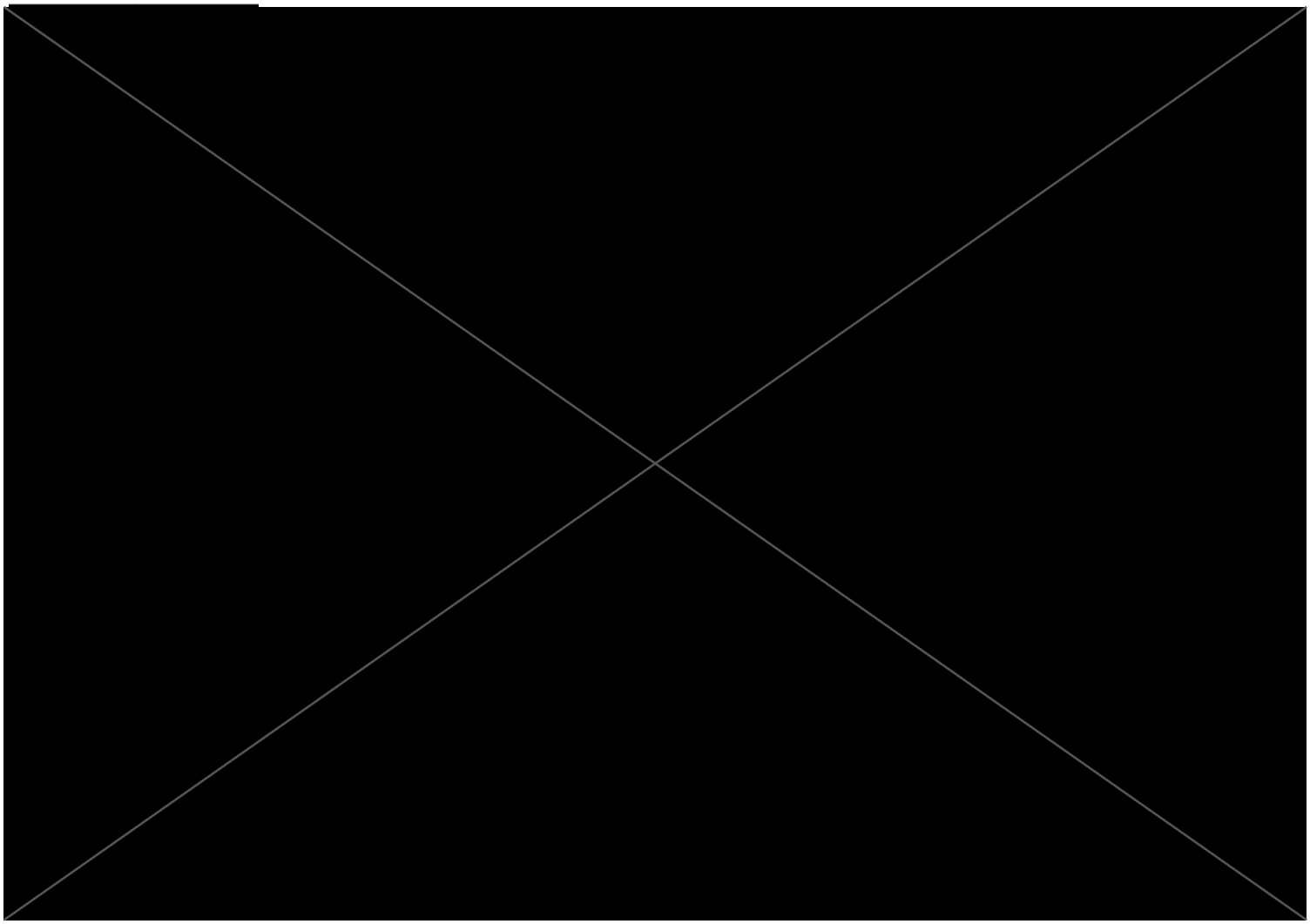

Email received yesterday:

From: Sarah Gardner
Date: August 30, 2023 at 1:24:37 AM GMT+2
To:
Cc:
Subject: Detect CSAM in iCloud: Incoming Campaign

Dear Tim,

This exact time two years ago we were so excited that Apple, the most valuable and prestigious tech company in the world, acknowledged that child sexual abuse images and videos have no place in iCloud. It was an announcement that took bravery and vision - we can live in a world where user privacy and child safety can coexist.

That is why it was so disappointing when you paused, and then quietly killed this plan in December 2022. We firmly believe that the solution you unveiled not only positioned Apple as a global leader in user privacy but also promised to eradicate millions of child sexual abuse images and videos from iCloud. The detection of these images and videos respects the privacy of survivors who have endured these abhorrent crimes – a privilege they undeniably deserve.

I'm writing to let you know that I am a part of a developing initiative involving concerned child safety experts and advocates who intend to engage with you and your company, Apple, on your continued delay in implementing critical technology that can detect child sexual abuse images and videos in iCloud.

We are asking you to honor your original intention to:

- Detect, report, and remove child sexual abuse images and videos from iCloud.
- Create a robust reporting mechanism for users to report child sexual abuse images and videos to Apple.

We wanted to alert you to our presence and our intention to take our very reasonable requests public in a week's time. Should you want to discuss our campaign over the course of the next week, or after we have launched, I can be reached at this email address. We welcome the opportunity to discuss these important issues with you and hear what Apple plans to do in order to address these concerns.

Child sexual abuse is a difficult issue that no one wants to talk about, which is why it gets silenced and left behind. We are here to make sure that doesn't happen.

Kind Regards,
Sarah Gardner
CEO Heat Initiative

***

Apple Response:

August 31, 2023

Ms. Sarah Gardner
CEO, Heat Initiative

Dear Ms. Gardner,

Thank you for your recent letter inquiring about the ways Apple helps keep children safe. We're grateful for the tireless efforts of the child safety community and believe that there is much good that we can do by working together. Child sexual abuse material is abhorrent and we are committed to breaking the chain of coercion and influence that makes children susceptible to it. We're proud of the contributions we have made so far and intend to continue working collaboratively with child safety organizations, technologists, and governments on enduring solutions that help protect the most vulnerable members of our society.

Our goal has been and always will be to create technology that empowers and enriches people's lives, while helping them stay safe. With respect to helping kids stay safe, we have made meaningful contributions toward this goal by developing a number of innovative technologies. We have deepened our commitment to the Communication Safety feature that we first made available in December 2021. Communication Safety is designed to intervene and offer helpful resources to children when they receive or attempt to send messages that contain nudity. The goal is to disrupt grooming of children by making it harder for predators to normalize this behavior.

In our latest releases, we've expanded the feature to more easily and more broadly protect children. First, the feature is on by default for all child accounts. Second, it is expanded to also cover video content in addition to still images. And we have expanded these protections in more areas across the system including AirDrop, the Photo picker, FaceTime messages, and Contact Posters in the Phone app. In addition, a new Sensitive Content Warning feature helps all users avoid seeing unwanted nude images and videos when receiving them in Messages, an AirDrop, a FaceTime video message, and the Phone app when receiving a Contact Poster. To expand these protections beyond our built-in capabilities, we have also made them available to third parties. Developers of communication apps are actively incorporating this advanced technology into their products. These features all use privacy-preserving technology — all image and video processing occurs on device, meaning Apple does not get access to the content. We intend to continue investing in these kinds of innovative technologies because we believe it's the right thing to do.

As you note, we decided to not proceed with the proposal for a hybrid client-server approach to CSAM detection for iCloud Photos from a few years ago, for a number of good reasons. After having consulted extensively with child safety advocates, human rights organizations, privacy and security technologists, and academics, and having considered scanning technology from virtually every angle, we concluded it was not practically possible to implement without ultimately imperiling the security and privacy of our users.

Scanning of personal data in the cloud is regularly used by companies to monetize the information of their users. While some companies have justified those practices, we've chosen a very different path — one that prioritizes the security and privacy of our users. Scanning every user's privately stored iCloud content would in our estimation pose serious

unintended consequences for our users. Threats to user data are undeniably growing — globally the total number of data breaches more than tripled between 2013 and 2021, exposing 1.1 billion personal records in 2021 alone. As threats become increasingly sophisticated, we are committed to providing our users with the best data security in the world, and we constantly identify and mitigate emerging threats to users' personal data, on device and in the cloud. Scanning every user's privately stored iCloud data would create new threat vectors for data thieves to find and exploit.

It would also inject the potential for a slippery slope of unintended consequences. Scanning for one type of content, for instance, opens the door for bulk surveillance and could create a desire to search other encrypted messaging systems across content types (such as images, videos, text, or audio) and content categories. How can users be assured that a tool for one type of surveillance has not been reconfigured to surveil for other content such as political activity or religious persecution? Tools of mass surveillance have widespread negative implications for freedom of speech and, by extension, democracy as a whole. Also, designing this technology for one government could require applications for other countries across new data types.

Scanning systems are also not foolproof and there is documented evidence from other platforms that innocent parties have been swept into dystopian dragnets that have made them victims when they have done nothing more than share perfectly normal and appropriate pictures of their babies.

We firmly believe that there is much good that we can do when we work together and collaboratively. As we have done in the past, we would be happy to meet with you to continue our conversation about these important issues and how to balance the different equities we have outlined above. We remain interested, for instance, in working with the child safety community on efforts like finding ways we can help streamline user reports to law enforcement, growing the adoption of child safety tools, and developing new shared resources between companies to fight grooming and exploitation. We look forward to continuing the discussion.

Sincerely,

Erik Neuenschwander
Director, User Privacy and Child Safety