

Apple auto-opts everyone into having their photos analyzed by AI for landmarks

Homomorphic-based Enhanced Visual Search is so privacy-preserving, iPhone giant activated it without asking

Thomas Claburn

Fri 3 Jan 2025 / 08:34 UTC



Apple last year deployed a mechanism for identifying landmarks and places of interest in images stored in the Photos application on its customers iOS and macOS devices and enabled it by default, seemingly without explicit consent.

Apple customers have only just begun to notice.

The feature, known as Enhanced Visual Search, was called out last week by software developer Jeff Johnson, who expressed concern in [two write-ups](#) about Apple's failure to explain the technology, which is believed to have arrived with iOS 18.1 and macOS 15.1 on [October 28, 2024](#).

In a [policy document](#) dated November 18, 2024 (not indexed by the Internet Archive's Wayback Machine until [December 28, 2024](#), the date of Johnson's initial article), Apple describes the feature thus:

Enhanced Visual Search in Photos allows you to search for photos using landmarks or points of interest. Your device privately matches places in your photos to a global index Apple maintains on our servers. We apply homomorphic encryption and differential privacy, and use an OHTTP relay that hides [your] IP address. This prevents Apple from learning about the information in your photos. You can turn off Enhanced Visual Search at any time on your iOS or iPadOS device by going to Settings > Apps > Photos. On Mac, open Photos and go to Settings > General.

Apple did explain the technology in a [technical paper](#) published on October 24, 2024, around the time that Enhanced Visual Search is believed to have debuted. A local machine-learning model analyzes photos to look for a "region of interest" that may depict a landmark. If the AI model finds a likely match, it calculates a vector embedding – an array of numbers – representing that portion of the image.

The device then uses [homomorphic encryption](#) to scramble the embedding in such a way that it can be run through carefully designed algorithms that produce an equally encrypted output. The goal here being that the encrypted data can be sent to a remote system to analyze without whoever is operating that system from knowing the contents of that data; they just have the ability to perform computations on it, the result of which remain encrypted. The input and output are end-to-end encrypted, and not decrypted during the mathematical operations, or so it's claimed.

The dimension and precision of the embedding is adjusted to reduce the high computational demands for this homomorphic encryption (presumably at the cost of labeling accuracy) "to meet the latency and cost requirements of large-scale production services." That is to say Apple wants to minimize its cloud compute cost and mobile device resource usage for this free feature.

With some server optimization metadata and the help of Apple's private nearest neighbor search (PNNS), the relevant Apple server shard receives a homomorphically-encrypted embedding from the device, and performs the aforementioned encrypted computations on that data to find a landmark match from a database and return the result to the client device without providing identifying information to Apple nor its OHTTP partner [Cloudflare](#).

Thus, Apple unilaterally began running people's Photos through a locally running machine-learning algorithm that analyzes image details (on a purely visual basis, without using location data) and creates a value associated with what could be a landmark in each picture. That value is then used on a remote server to check an index of such values stored on Apple servers in order to label within each snap the landmarks and places found in Apple's database.

Put more simply: You take a photo; your Mac or iThing locally outlines what it thinks is a landmark or place of interest in the snap; it homomorphically encrypts a representation of that portion of the image in a way that can be analyzed without being decrypted; it sends the encrypted data to a remote server to do that analysis, so that the landmark can be identified from a big database of places; and it receives the suggested location again in encrypted form that it alone can decipher.

If it all works as claimed, and there are no side-channels or other leaks, Apple can't see what's in your photos, neither the image data nor the looked-up label.

MORE CONTEXT

- [Apple offers to settle 'snooping Siri' lawsuit for an utterly incredible \\$95M](#)
- [Fining Big Tech isn't working, Make them give away illegally trained LLMs as public domain](#)
- [Apple called on to ditch AI headline summaries after BBC debacle](#)
- [Apple and Meta trade barbs over interoperability requests](#)

Apple claims that its use of this [homomorphic encryption](#) plus what's called [differential privacy](#) – a way to protect the privacy of people whose data appears in a data set – precludes potential privacy problems.

"Apple is being thoughtful about doing this in a (theoretically) privacy-preserving way, but I don't think the company is living up to its ideals here," observed software developer Michael Tsai in an [analysis](#) shared Wednesday. "Not only is it not opt-in, but you can't effectively opt out if it starts uploading metadata about your photos [before](#) you even use the search feature. It does this even if you've already opted out of uploading your photos to iCloud."

Tsai argues Apple's approach is even less private than its [abandoned CSAM scanning plan](#) "because it applies to non-iCloud photos and uploads information about all photos, not just ones with suspicious neural hashes."

Nonetheless, Tsai acknowledges Apple's claim that data processed in this way is encrypted and disassociated with the user's account and IP address.

While there's no evidence at this point that contradicts Apple's privacy assertions, the community concern has more to do with the way in which Apple deployed this technology.

"It's very frustrating when you learn about a service two days before New Years and you find that it's already been enabled on your phone," [said](#) Matthew Green, associate professor of computer science at the Johns Hopkins Information Security Institute in the US.

The Register asked Apple to comment, and as usual we've received no reply. We note that lack of communication is the essence of the community discontent.

"My objection to Apple's Enhanced Visual Search is not the technical details specifically, which are difficult for most users to evaluate, but rather the fact that Apple has taken the choice out of my hands and enabled the online service by default," said Johnson in his second post.

He told *The Register* that it's unclear whether the data/metadata from your Photos library is uploaded before you even have a chance to disable the opt-out setting.

"I don't think anybody knows, and Apple hasn't said," Johnson observed. @

More about

- [Apple](#)
- [iOS](#)
- [Privacy](#)
- [More like these](#)
- [TIP US OFF](#)
- [Send us news](#)

Apple gives fanbois The Sweetest Thing: A delete button for that U2 album

FLASHBACK →



69 COMMENTS



Apple's interoperability efforts aren't meeting spirit or letter of EU law, advocacy groups argue

Free Software Foundation Europe and others urge European Commission to double down on DMA

SOFTWARE 7 days | 27



Apple Intelligence turned on by default in upcoming macOS Sequoia 15.3, iOS 18.3

Plus: Google stuffs Gemini into Workspace, with a hidden off switch?

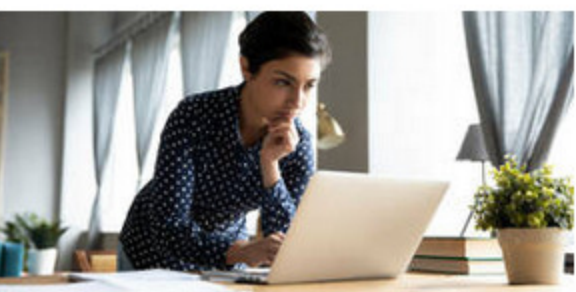
AI + ML 1 day | 60



Biden signs sweeping cybersecurity order, just in time for Trump to gut it

ANALYSIS Ransomware, AI, secure software, digital IDs – there's something for everyone in the presidential directive

PUBLIC SECTOR 6 days | 39



A rethink of parental leave policy

IT workers and programmers set to benefit as Sandvik implements HR reboot

SPONSORED FEATURE



Microsoft eggheads say AI can never be made secure – after testing Redmond's own products

If you want a picture of the future, imagine your infosec team stamping on software forever

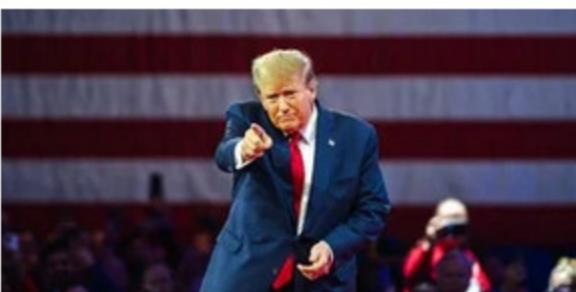
AI + ML 6 days | 84



Apple solves broken news alerts by turning off the AI

Summaries will return when Apple Intelligence has 'improved'

AI + ML 6 days | 46



Infosec was literally the last item in Trump's policy plan, yet major changes are likely on his watch

FEATURE Everyone agrees defense matters. How to do it is up for debate

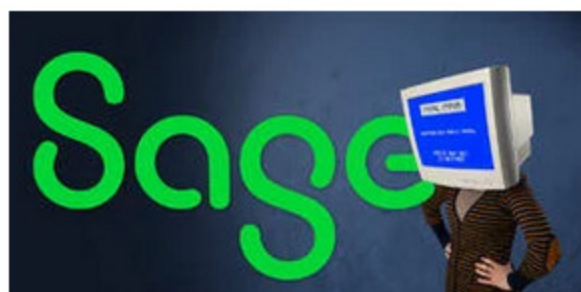
CSO 1 day | 12



Allstate accused of quietly paying app makers for driver data

Insurance giant sued by Texas for using surveillance without consent to jack up premiums, deny coverage

PERSONAL TECH 9 days | 24



Sage Copilot grounded briefly to fix AI misbehavior

'Minor issue' with showing accounting customers 'unrelated business information' required repairs

AI + ML 3 days | 22



OpenAI's ChatGPT crawler can be tricked into DDoSing sites, answering your queries

The S in LLM stands for Security

AI + ML 4 days | 31



Free-software warriors celebrate landmark case that enforced GNU LGPL

On the Fritz: German router maker AVM lets device rights case end after coughing up source code

SOFTWARE 13 days | 41



Look for the label: White House rolls out 'Cyber Trust Mark' for smart devices

Beware the IoT that doesn't get a security tag

SECURITY 14 days | 38