Studio Ghibli AI art trend: A privacy nightmare in disguise, experts warn

While netizens are hooked on the viral trend of transforming personal photos into Studio Ghibli-style art using AI tools, experts warn that the trend conceals a darker reality where casual sharing can lead to unforeseen privacy breaches and data misuse.

Cybersecurity experts caution that while these tools may appear harmless, the terms of services are often vague, raising questions about what happens to user photos after they are processed.

The trend started when OpenAI launched its GPT-4o model, which allows users to recreate personal images in the artistic style of Studio Ghibli, a Japanese animation studio.

Few of the many platforms say that they don't store the photos, or delete them after one-time use, but most of them don't clearly explain what "deletion" really means--whether it's instant, delayed, or partial.

Photos contain more than just facial data. They often include hidden metadata like location coordinates, timestamps, and device details-- all of which can quietly reveal personal information.

These AI tools leverage neural style transfer (NST) algorithms, explains Quick Heal Technologies CEO Vishal Salvi.

These algorithms separate content from artistic styles in uploaded photos to blend the user's image with reference artwork.

While the process appears harmless, vulnerabilities like model inversion attacks where adversaries may reconstruct original pictures from Ghibli images pose significant risks, he noted.

"Even if companies claim they don't store your photos, fragments of your data might still end up in their systems. Uploaded images can definitely be repurposed for unintended uses, like training AI models for surveillance or advertising," Salvi cautioned.

The way these tools are designed makes it easy to overlook what you're really agreeing to, McAfee's Pratim Mukherjee said.

Eye-catching results, viral filters, and fast interactions create an experience that feels light--but often comes with hidden privacy risks.

"When access to something as personal as a camera roll is granted without a second thought, it's not always accidental. These platforms are often built to encourage quick engagement while quietly collecting data in the background.

"That's where the concern lies. Creativity becomes the hook, but what's being normalised is a pattern of data sharing that users don't fully understand. And when that data fuels monetisation, the line between fun and exploitation gets blurry," said Mukherjee, Senior Director of Engineering, McAfee.

The risk of data breaches looms large, with experts cautioning that stolen user photos could fuel deepfake creation and identity fraud.

Vladislav Tushkanov, Group Manager at Kaspersky AI Technology Research Centre, says that while some companies do ensure the safety and security of the data they collect and store, it does not mean that the protection is bullet-proof.

"Due to technical issues or malicious activity, data can leak, become public or appear for sale at specialised underground websites. Moreover, the account that is used to access the service can be breached if the credentials or user device is compromised," he said.

He said numerous accounts and hacker forums on the dark web offer stolen user account data for sale.

"The hard part is, you can't change your face the way you can reset a password. Once a photo is out there, it's out there," Mukherjee warned.

Furthermore, many platforms bury data usage clauses in lengthy terms of service, making it difficult for users to understand how their data is being handled. "These policies are all buried within their terms of service. And that's the issue, those terms are often too vague or too long for most people to really understand. Just because someone clicks accept doesn't mean they're giving truly informed consent.

"If it's not clear how your image will be used, or whether it's deleted at all, it's worth asking if the fun is really worth the risk," said Mukherjee.

Some countries have taken steps to require clearer disclosures, while some are still contemplating. To mitigate these risks, experts recommend that users exercise caution when sharing personal photos with AI apps.

Tushkanov advises users to "combine standard security practices with a bit of common sense," including using strong, unique passwords, enabling two-factor authentication, and being wary of potential phishing websites.

Salvi suggests using specialised tools to strip hidden metadata from photos before uploading them. On the policy front, he suggests that regulators mandate differential privacy certification and standardised audits to close compliance gaps.

Mukherjee calls for governments to mandate simplified, upfront disclosures regarding data usage.

(Only the headline and picture of this report may have been reworked by the Business Standard staff; the rest of the content is auto-generated from a syndicated feed.)