The hidden cost of AI: Your face, your data

As Gen AI begins to permeate all aspects of our lives— from the hedonic to critical use cases— data privacy is being significantly compromised.

The last couple of years have witnessed rapid advancements in generative AI, with little control over its explosive growth. While the world has marvelled at its capabilities, we may have failed to fully understand —or have perhaps ignored— the serious concerns that such technologies raise.

Generative AI is trained on vast datasets gathered through Web scraping, user-generated content, and individuals' data exhaust. This includes not only information we voluntarily share but also data trails we may unknowingly leave behind. Data is the fuel that powers these massive generative algorithms.

As Gen AI begins to permeate all aspects of our lives— from the hedonic to critical use cases— data privacy is being significantly compromised.

A recent example is the viral wave of Ghibli-style portraits flooding social media. Many users shared intimate and cherished personal photos, including those of children. While the ethical concerns around Studio Ghibli's copyrights form one part of the issue, the more serious problem is that people are handing over personal images voluntarily for a fleeting moment of pleasure. Most are unaware that, along with facial data, they may also be sharing metadata, biometric identifiers, and other personally identifiable information that generative models could exploit without consent.

Unlike other data breaches, a breach of facial data could have serious consequences. Unlike a password, facial data cannot be easily changed. As facial recognition becomes a common means of authentication —for purposes ranging from unlocking a phone to accessing government security and identity systems— a breach of such data can have grave consequences. These range from identity theft and digital impersonation to sophisticated profiling for commercial exploitation, deepfake creation, and even political or ideological manipulation.

Of those who joined the Ghibli trend, how many truly read the terms and conditions or thought of such a repercussion? This only shows how users could be manipulated into voluntarily handing over their personal data in exchange for the momentary pleasure of participating in a viral trend. The fault may not be entirely theirs. Systems are often designed in ways that obscure risks, placing the burden on individuals to decipher the data in fine print and safeguard their privacy.

Another serious concern is the proliferation of derivative applications built by startups and third-party developers using foundational models provided by the major tech companies. While these dominant firms are mostly in the spotlight, making them accountable in cases of data mishandling, the second and third generation "AI-powered applications" that do not have clear regulatory guardrails escape oversight. They could easily piggyback on social

media platforms, being in the regulatory blind spot, and collect necessary data with no transparency on data governance.

Privacy debates on the digital panopticon and surveillance capitalism have been there right since the boom of the data-driven economy. With Gen AI, these discussions take a new avatar, as we are no longer dealing with just one's data exhaust and digital footprint being analysed to send targeted ads, but we are moving beyond, into using some of this data to synthesise, generate, and fabricate new data that appears to be eerily realistic with very fuzzy boundaries to distinguish between what is real and fake.

In 2024, the European Union adopted the EU AI Act, aiming to ensure AI is trustworthy and safe while fostering innovation. Unlike the EU, India lacks a comprehensive AI-specific law to address the unique privacy and ethical challenges posed by AI. India's yet-to-be-implemented DPDP Act 2023 does not explicitly cover AI-related privacy risks. In January 2025, the Ministry of Electronics and Information Technology (MEITY) published the 'AI Governance and Guidelines Development' report with actionable recommendations concerning AI governance. While it is a good start, privacy experts have commented on several lacunae in these guidelines. For example, while the report rightly

addresses the issue of copyrights in training the AI models, it falls short in acknowledging the privacy concerns arising from the same.

In today's AI-driven world, hungry for data, as India makes rapid strides in adopting AI innovations, it needs to balance innovation with privacy-preserving AI regulations and create awareness among users on the ethical and socially responsible use of AI. While India is taking early steps in this direction, it still has a long way to go.

(Rajendra is a professor of information systems at IIM Bangalore, and Sowmya is an assistant professor of IT and analytics at TAPMI Bengaluru)