

REGULATORY

Whatever it is, it's never what you thought it was.... Intersection between privacy and AI

9 May 2024 5 min read

Lwazi-Lwandile Simelane – Candidate Attorney

The permeation of artificial intelligence ("AI") into our society as a whole and into our personal lives is undeniable. The use of AI has increased significantly in the last few years. However, AI has been in existence since the 1950s. So why the sudden panic? Perhaps it is because AI is becoming and has become more personal in its use and in its development.

The development of generative AI requires the use of data. In order to teach a machine how to "answer" a question or how to even speak a language, those who "teach" the machines must input into the machine data (in the form of words) from which it can learn.

However, as with the launch of Open AI's Sora, AI machines are not only being taught how to "talk" but also how to "draw" and how to "paint". Sora, a generative AI machine, is able to generate images and videos from the prompts that the user gives it. However, this is not the only AI machine requires the input of images as data. Facial recognition companies including Clearview AI have also built AI machines that require the input of images in order to operate.

The use of images in AI development may seem innocuous, but this use of image data raises a whole host of privacy concerns.

But when does privacy become a concern?

Privacy laws are underpinned by the idea that an individual should have autonomy over the use of their personal data or at the very least should be able allowed to manage how their personal data is used. Practices such as data scraping limit that ability for one to have control over the use of their personal data. If the data that is inputted into an AI machine is collected without the consent of the data subject, that means that the data subject is not in control or at least aware of how their personal data may be used.

Information that is collected by AI companies may contain biometric information which raises a major privacy concern relating to safety. For example, images collected may include information which is used to personally identify people, such as retinal scanning. The concern with the use of images that contain such biometric information is that they may very well lead to identity theft. The publicisation of this information and its use for profit therefore potentially poses a threat to the identity security of individuals.

Although the Protection of Personal Information Act, 2023 ("POPIA") stipulates, subject to various conditions, that personal information may be processed for journalistic, literary or artistic purposes, one has to question whether the processing of personal information by AI development companies is in line with this exclusion. It is obvious that facial recognition technology does not serve any artistic, literary nor artistic purpose. However, does AI technology that generates images from user inputs fall squarely inside or outside of this category.

The Cambridge Dictionary defines expression as:

the act of saying what you think or showing how you feel using words or actions^[1]:

Therefore, artistic expression would mean expressing one's feeling using artistic means. Although this is yet to be determined, it is unlikely that an AI machine or company would be exempt from the application of POPIA on this basis. This is simply because AI machines do not have feelings and therefore are not capable of expression but rather re-creation.

It is painstakingly clear that the rate at which artificial intelligence is developing is incongruent with the rate at which the regulatory framework in respect to AI is developing. To a large extent companies have been left to self-regulate. This is evident considering companies such as Amazon, Google, Meta among others, having come together to commit themselves and publish AI Safety Policies.

According to the Cambridge Dictionary, artificial intelligence is:

"a particular computer system or machine that has some of the qualities that the human brain has, such as the ability to interpret and produce language in a way that seems human, recognise or create images, solve problems, and learn from data supplied to it".

Therein lies the rub.

Although there is a mountain of good for which AI can be used, and its potential to alter the world exciting, there also exist numerous ethical dilemmas which are attributable to AI. These include, among others, concerns relating to data collection processes, the quality of data inputted to AI machines and the protection of potentially private information contained in data collected.

A clear illustration of such a data collection concern is in the Clearview AI data collection issue. Clearview AI (a facial recognition company) built its database by scraping images on the internet, which were uploaded onto public platforms and retaining them in order to refine its facial recognition abilities. Australia's private regulator indicated that even though individuals had uploaded the collected images onto public platforms, that did not mean that the users had consented to their images being used for the purpose of developing Clearview AI's artificial intelligence facial recognition machine.

Privacy cannot be ignored when considering AI advancements. It is imperative for all companies which are incorporating AI into their businesses and for AI developers themselves to carefully consider the ethical dilemma of privacy. Always.

Footnote

[1] <https://dictionary.cambridge.org/dictionary/english/expression>



Ahmore Burger-Smidt

Head of Regulatory

[View Profile](#)