Artificial Intelligence: The New Eyes Of Surveillance

Matthias Pfau

Co-founder of Tuta, a secure email service. We are innovation leaders in encrypted communication and collaboration.

getty

While artificial intelligence (AI) systems continue to be hyped in 2024, the risks posed to data privacy can no longer be ignored. I believe AI must be considered a surveillance technology due to its ability to collect, analyze and interpret vast amounts of data. It is time to not just look at the possibilities of AI but also at its risks, namely regarding everybody's right to privacy.

The rapid developments in the training and use of AI have raised concerns about user consent, the ethical use of personal data and privacy rights in general. Let's explore how AI is trained, what some of the lesser-known risks are and what steps can be taken to ensure the benefits outweigh them.

Understanding AI Training And Its Shortcomings

AI training involves the process of feeding large volumes of data into machine learning algorithms to enable them to learn patterns and make predictions or decisions. Importantly, the nuances in training must be taken into account and addressed by AI developers.

First, it's commonly known by now that AI models may inherit overlooked biases present in the training data. If the data is not representative or contains biases, the model can perpetuate and even amplify them. Understanding and addressing these biases are ongoing challenges in AI development.

As AI technology continues to evolve, it is essential for stakeholders to actively engage in discussions around ethical considerations, transparency and ethical AI deployment. A special focus must be put on ethical development as AI-powered systems can process and analyze enormous volumes of data from various sources. Ensuring that not just any available data can be used for training purposes is key, as this may include data from the web and social media in general, as well as non-public data such as user actions on technology platforms, user profiles or even data from security cameras.

AI systems are frequently trained by merging personal data from both external and internal sources. Most AI algorithms used are considered proprietary, making them difficult to scrutinize. The lack of transparency in how these algorithms operate and make decisions raises concerns about accountability and the potential for biases that may disproportionately impact certain groups, particularly minorities. Information on how the data is used, what consent is required or how its use is regulated must be made clear.

Consequently, AI technology can use any data that is available. Currently, it is difficult to know how personal data is used to train AI systems, where the data is stored and whether it is secured with encryption or not.

The Harm Of AI Tools On Privacy

It's widely understood that AI tools allow people to create content—texts, images, videos and much more can be quickly created with AI. But these tools can also be used to track and profile individuals. AI allows for more detailed profiling and tracking of individuals' activities, movements and behaviors than was ever possible before. AI-based surveillance technology can, for instance, be used for marketing purposes and targeted advertising.

This comprehensive surveillance made possible by AI can lead to invasions of privacy. Individuals may feel scrutinized, and there is the risk of their private lives being used in this way without their knowledge or consent.

AI also facilitates the implementation of facial recognition technology, which can identify and track individuals based on their facial features, even in the real world. This technology is already being used in public spaces, such as railway stations or airports, and by law enforcement agencies. The widespread use of facial recognition raises concerns about the constant monitoring of individuals.

Predicting The Future

AI algorithms can analyze patterns of behavior, both in the real world and in online spaces. This includes monitoring social media activities, online searches and communication patterns.

Through the massive use of personal data to train AI systems, this technology becomes much like a surveillance system that can "know" what people are thinking and can predict what they are going to like, dislike or what they might do in a given context.

Websites or online searches already tend to only show users information that matches their previous online behavior (known as filter bubbles) instead of creating an environment for a pluralistic, equally accessible and inclusive public debate. If gone unchecked, artificial intelligence could make these filter bubbles even worse, potentially predicting what users might like to see and applying filters accordingly.

Overcoming The Challenges

We already live in a world of big data, and the expansion of computing power through AI may drastically change how privacy is protected.

AI is simply the latest technology to present new challenges to consumers, businesses and regulators. It is not the first and not the last of its kind. Thus, companies should apply best practices for data privacy compliance to build user trust. For instance, companies must ensure that the privacy requirements stated in the European privacy regulation GDPR are being met when using the personal data of European citizens.

In addition, organizations can leverage internal resources and adopt specific strategies to enhance privacy and build user trust. This includes fostering a culture of transparency and communication and investing in user education programs to empower individuals with the knowledge to protect their own privacy. Companies should provide resources and guidelines on best practices for secure online behavior and promote the use of encryption. Lastly, every company should emphasize ethical data practices within the organization and incorporate privacy by design. Prioritize collecting only the necessary data and ensure that data is handled responsibly and in compliance with privacy regulations.

The future of data processing by AI software must be monitored closely and it must be made sure that peoples' right to privacy is not being harmed by this new technology. Our pursuit of technological progress must not come at the expense of privacy.
