Privacy concerns in the development of Artificial Intelligence

Artificial intelligence is rapidly developing. Further innovations to AI will result in additional advancements in healthcare, security, and education. Despite these innovations, the ethical concerns surrounding privacy data handling needs to be discussed; the misuse of private data has become a significant problem for consumers.

In the digital age, privacy is more important than ever. Mazurek and Malagocka (2019) emphasise that privacy is a human right; an individual should be able to express themselves freely without data being collected and misused by data companies. When personal information is mishandled, it causes a security risk which can leave the user vulnerable as personal information of the user is open for public access.

As artificial intelligence is reliant on data to work, personal information from individuals is collected and accumulated. Solanas and Balleste (2010) recognises that companies collect vast amounts of data for consumer profiling. Consumer profiling may be beneficial to users as it allows easy access to relevant content. However, data can be held by companies to further sell for profit. Therefore, it is very important that companies regulate the data that can be held and distributed. The authors also explained how citizens have their data collected by political parties to win power over a nation. The company's algorithms will be enhanced through the use of Artificial Intelligence as it advances, this would result in consumer profiling that companies can then use for their benefit.

Data can be collected without the user knowing - the algorithms then use this data to show the user unwanted information and unnecessary adverts, which businesses tend to profit from. As AI continues to evolve, more manipulated data takes a shorter amount of time to process based on their location without the user knowing (Wang and Liu, 2009). Furthermore, Ganesh et al. (2021) highlights the fact that the user cannot determine what information is collected by the companies. They further discussed how deep learning (DP) has been a major factor in the development of AI as DP has improved the text recognition and image classification. DP poses a privacy concern as confidential information is recorded by companies and the government allows the companies to spy on the user.

As AI continues to evolve, companies should regulate what data is being used for the algorithms. The user should also be allowed to have a say in what information is given to companies for the best interest of the user. AI will bring further advancements to society as long as it continues to evolve in an ethical way.

References

Ganesh, S., Dheeraj, C., Padmavathy, R. (2021). 'A deep learning framework to preserve privacy in ederated (collaborative) learning', In Misra, S., Kumar Tyagi, A. (eds.) *Artificial Intelligence for Cyber Security: Methods, Issues and Possible Horizons or Opportunities.* Cham: Springer, pp. 12-28.

Mazurek, G. and Małagocka, K. (2019). 'Perception of privacy and data protection in the context of the development of artificial intelligence', *Journal of Management Analytics*, 6(4), pp. 344–364. Available at: doi: 10.1080/23270012.2019.1671243 (Accessed: 10 November 2021).

Solanas, A. and Martinez-Balleste, A. (2010). *Advances in artificial intelligence for privacy protection and security. World Scientific.* [online]. Available at: https://ebookcentral.proquest.com/lib/manchester/reader.action?docID=1679374 (Accessed: 10 November 2021).

Wang, T. and Liu, L. (2009). 'From data privacy to location privacy', in Tsai, J.J.P. and Yu, P.S. (eds.) *Machine Learning in Cyber Trust.* Boston, MA: Springer, pp. 217-246.