Dominic Drury

03/25/2024

CS-370

4-2 Project One Submission

A neural network is a type of machine learning that is inspired by how the human brain thinks and analyzes data (Guli & Pal, 2017). By having the neurons either “fire” or “not fire” when certain criteria are met, the network can determine what an object is. The network will also give weight to certain areas to help improve accuracy in the classification of objects. The network receives the input, like a pixel on a screen, then through a series of hidden networks it filters those pixels through and depending on what neurons “fire” will output what object is has been given based on its training.

By using a user's personal information, like their race, gender, age, location, etc., and their behavior, like, streaming history, websites visited, social media used, purchase history, etc., the neural network can predict what topics and products the user will be interested in (Lee, 2023). When using a “black box” classification system this can raise some ethical concerns. For starters, this much personal data is very tempting for malicious intent from thieves or other individuals seeking to target people. The other major concern is the risk of bias, like assuming that because a user is an African American that they will want defense lawyers instead of property ads or that because the user is female that she will want baby products advertised to her instead of job ads. These kinds of stereotypes can be perpetuated by neural network models that use the past as their source of data, and does not consider the systemic problems that past has and how the data is not a result of the user’s interest, but the system they live in.

The GDPR aims to protect user data from the concerns I listed above, and by abiding by its policies we will be able to protect both our users and this company. The GDPR defines personal data as “any information relating to an identified or identifiable natural person” and a natural person as “one who can be identified, directly or indirectly” (ICO, n.d.). The GDPR requires that the personal data be processed lawfully, fairly, and transparently, the data be collected for a specified and legitimate purpose, the data be relevant and limited to its purpose, the data be accurate and current, the data be stored only as long as it is relevant and necessary, the data be keptd secure and confidential, and that we as the controller of this data are responsible and accountable for following these principles (ICO, n.d.).

Since we use our neural network as a classifier to personalize our user experience, we could face penalties and fees if we do not abide by the GDPR. We could face legal action for any damages caused, and any “associates claim for compensation payable to an individual” (ICO, n.d.). Since we need data to train our network to give our customers the personalized experience they expect from us, not collecting the data necessary is not an option for us. Without the data gathered, we would not be able to give relevant suggestions for posts to look at, friend requests, groups to join, news, discussion boards, games, etc. We also fund this company through targeted ads, which would be impossible without this data, and the non-targeted ad revenue would not sustain this company without a complete overhaul of how we run.

I think that adhering to the best practices for our AI will keep us in line with the GDPR, improve our relationship with our customers, and ensure our future. The current trends in AI and ML are to ensure that the AI has no unlawful biases and does not discriminate against our customers, which we can do by investing in research to mitigate the biases (Ved, 2019). Another best practice is to aim to minimize the amount of data we gather, which can be done through researching what data is needed and what data is not, anonymization techniques, and only use solutions that are transparent and explainable (Ved 2019). This will ensure that we keep to the principles of the GDPR and it will likely improve the performance of the neural network since it will have less data to sift through when making its “judgements”. Finally, conducting data protection impact assessments and applying privacy by design and privacy by default will ensure that we adhere to the principles of confidentiality and storage limitation (Ved, 2019).

References

ICO, U. (n.d.). UK GDPR guidance and resources. Ico.org.uk. Retrieved March 25, 2024, from <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/>

Dorschel, A. (2019, April 24). Rethinking Data Privacy: The Impact of Machine Learning. Medium.com. Retrieved March 25, 2024, from <https://medium.com/luminovo/data-privacy-in-machine-learning-a-technical-deep-dive-f7f0365b1d60>

Spillane, J. (2022, December 8). *How GDPR Can Undermine Personalization and User Experience*. Business2community.com. Retrieved March 25, 2024, from <https://www.business2community.com/customer-experience/how-gdpr-can-undermine-personalization-and-user-experience-02108269>

Ved, A. (2019, February 28). *How to develop Artificial Intelligence that is GDPR-friendly*. Techgdpr.com. Retrieved March 25, 2024, from <https://techgdpr.com/blog/develop-artificial-intelligence-ai-gdpr-friendly/>

Intersoft Consulting (n.d.). *General Data Protection Regulation*. Gdpr-Info.eu. Retrieved March 25, 2024, from <https://gdpr-info.eu/>

Beysolow, I. T. (2019). *Applied reinforcement learning with python : With openai gym, tensorflow, and keras*. Apress L. P..

Gulli, A., & Pal, S. (2017). *Deep learning with keras : Get to grips with the basics of keras to implement fast and efficient deep-learning models*. Packt Publishing, Limited.

Lee, M. (2023, August 31). *AI Personalization: 5 Examples + Business Challenges*. Bloomreach.com. Retrieved March 26, 2024, from <https://www.bloomreach.com/en/blog/2023/ai-personalization-5-examples-business-challenges>