4-2 Project One Submission

Joel De Alba

Southern New Hampshire University

Professor Timothy Alexander

07 / 28 / 23

As a leading social networking company, we must address the concerns raised by the EU regulator regarding potential violations of the GDPR principles. Let us discuss how neural networks work and illustrate their role in creating personalization, evaluate ethical concerns, and analyze how GDPR affects our practices. We will propose adaptations to ensure compliance while preserving user experience and business goals.

Neural networks are a class of machine learning algorithms inspired by the human brain's neural connections. They consist of interconnected layers of artificial neurons that process data and make predictions. In the context of personalization, neural networks use large amounts of user data, such as mouse clicks, navigation, and interactions, to learn patterns and make personalized recommendations. This technology is implemented in most known social media websites and applications. One great example lies in the algorithm of Facebook and how the social media platform calculates the amount of time certain videos are watched from certain pages, influencers, musical artists, groups, etc. to learn more about the end user and accommodate personal user accounts to their interests. These interests are then utilized to aid businesses by providing advertisements based on your cookies or site links and travel data to be able to further interest and sell to the user of said account to the company’s products. Additionally, this personalization process aims to maximize user engagement and click-through rates, enhancing user satisfaction and overall platform performance.

A neural network has three types of layers: the input layer, hidden layers, and output layer. This is titled as a Multi-Layered Perceptron, the more neurons utilized, the better the processed result. The input layer receives raw data from the user, which is then processed through multiple hidden layers that extract features and patterns. Finally, the output layer generates personalized recommendations or classifications based on the learned patterns.

Black Box refers to a system or model whose internal workings and decision-making processes are not transparent or easily interpretable to users or observers. It means that the input-output relationship of the system is known, but the internal mechanisms and logic that lead to those outputs are not explicitly accessible or understandable. The use of "black box" classification systems in neural networks raises a variety of ethical concerns. Hidden and unexpected biases may be a serious factor, resulting in discriminatory recommendations or content filtering without user awareness. To ensure transparency and fairness, these biases must be addressed, and we must make our personalization algorithms more interpretable to users.

This can be done in a couple of ways, one way this process is performed is by implementing bias detection methods to identify hidden and unexpected biases in the neural network's predictions. Address these biases through techniques such as debiasing algorithms or reweighting training data to ensure fair and equitable recommendations. Another process involves conducting regular audits to ensure that the model's performance aligns with fairness and ethical standards. Monitor for any unintended consequences of the algorithm and take corrective actions promptly.

To preserve user experience and achieve compliance in GDPR, we propose introducing the practices of Transparency, Data Minimization, Storage Limitations, Accuracy, Accountability, and implementing ethical AI practices.

In structuring compliance with GDPR, we must clearly communicate to users how their data is used for personalization purposes, including what data is collected and how it informs recommendations. There may be a case that this information could be missing, partial, or not easily identified and as such not easily readable. We should also only collect necessary data for personalized recommendations and not retain data beyond its specific purpose. Regarding security, it is our responsibility to keep user data accurate and update it promptly when inaccuracies are detected.

Data should be retained only for as long as it serves personalized recommendation purposes and another factor to consider is user data confidentiality, we must ensure that user data is securely stored and protected against unauthorized access. Additionally, the company should establish processes and policies to ensure compliance with GDPR principles and be prepared to address any potential violations.

Using neural networks to personalize user experiences raises legal concerns under GDPR. The potential lack of transparency and data minimization could conflict with the purpose limitation principle. Additionally, hidden biases in the algorithms may lead to discriminatory content recommendations, which may violate GDPR's principles of fairness and accountability. As a company that relies heavily on personalization, not collecting data may not be a viable option. Data collection is essential for creating personalized experiences, targeted advertising, and maintaining a competitive edge.

* **Transparency** is the ability to clearly communicate data usage and personalization practices through user-friendly policies and consent mechanisms.
* Regarding **Data Minimization** and **Storage Limitations** we must only collect and retain the data necessary for personalization and set clear retention periods.
* The practices of **Accuracy** and **Accountability** involve implementing processes for users to correct inaccuracies in their data and establish an internal framework for GDPR compliance.
* **Ethical AI Practices** involve adopting AI fairness and interpretability techniques to address hidden biases and ensure personalized recommendations are fair and understandable.

By adopting transparent practices, incorporating ethical AI principles, and adhering to GDPR's guidelines, we can maintain our industry leadership while protecting user privacy and building trust. Complying with GDPR principles and adapting our personalization algorithms will strengthen our position as an ethical and responsible leader in the social networking industry.

Sources

Grother, P., Ngan, M., & Hanaoka, K. (2019). Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. National Institute of Standards and Technology (NIST).

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. Big Data & Society, 3(2), 2053951716679679.

Caliskan, A., Bryson, J. J., & Narayanan, A. (2017). Semantics derived automatically from language corpora necessarily contain human biases. Science, 356(6334), 183-186.

Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. Nature Machine Intelligence, 1-8.

Steve Brunton. (2021, February 12). Reinforcement Learning: Machine Learning meets control Theory [Video]. YouTube. https://www.youtube.com/watch?v=0MNVhXEX9to

Robins, A. (2021, December 22). Stochastic vs Deterministic Models. Understand the Pros and Cons. Retrieved July 26, 2023, from https://blog.ev.uk/stochastic-vs-deterministic-models-understand-the-pros-and-cons

Leonelli, M. (2021, April 19). 1.2 Types of simulations | Simulation and Modelling to Understand Change. https://bookdown.org/manuele\_leonelli/SimBook/types-of-simulations.html

Das, A. (2017). The very basics of reinforcement learning. Medium. Retrieved from https://becominghuman.ai/the-very-basics-of-reinforcement-learning-154f28a79071

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

Lamba, A. (2018). A brief introduction to reinforcement learning - We’ve moved to freeCodeCamp.org/news - Medium. Medium. https://medium.com/free-code-camp/a-brief-introduction-to-reinforcement-learning-7799af5840db