Michael Garramone

CS370 Current/ Emerging Trends in CS

Professor Alexander

1/29/2024

Neural networks for machine learning are based off the design of the human brain and the neural network that functions in the human brain. In the 1980s, Geoffrey Hinton conceptualized the idea of Deep Learning in the form of a structure that was called an artificial neural network (McCallum, 2021). Like the human brain the artificial neural network worked similarly, passing data through an input layer, which passed the data to a hidden layer, and finally to an output layer. Each of these layers are comprised of nodes. “A node combines input from the data with a set of coefficients, or weights, that either amplify or dampen that input, thereby assigning significance to inputs with regard to the task the algorithm is trying to learn” (Pathmind, n.d.). As the data is placed in the input layer, it is analyzed by its weight and calculations are conducted. A function is performed at the end where it will either send the data in one direction which either is where the data is strongly pointing toward what the dataset is training the system to understand, or in another direction where the data does not fall into the certain criteria that the dataset is training for. These pass onto another layer, a hidden layer, and complete more calculations before being passed onto either another hidden layer or the output layer. With more hidden layers, the data being tested and trained with will provide more accurate results. “The output layer gives the final result of all the data processing by the artificial neural network” (Amazon).

“Neural networks can track user activity to develop personalized recommendations. They can also analyze all user behavior and discover new products or services that interest a specific user” (Amazon). With the ability to track user behavior, neural networks can create very personalized user experiences through predicting what the user might want with their searches and purchase history. With the user’s search history and previous purchase history, Amazon and distribution sites similar to it have the ability to predict what the user might want to purchase or come up with more accurate items for sale. Major websites like YouTube, Amazon, and Facebook have been known to provide users with more personalized experiences. “According to Invesp 59% of online shoppers believe that it is easier to find more interesting products on personalized online retail stores, while 56 percent of online shoppers are more likely to return to a site that recommends products” (Platform, 2019). YouTube does this in a similar way as well by providing videos that are close to what has been searched previously by the user. A user’s profile could be curated to a specific genre of videos like gaming or home improvement depending on how much the user has looked up specified videos with similar KEY words that connect that type of video with others in the database. Facebook allows for a more personalized experience than most social media applications. Using its neural networks to create an experience off of what a user likes, decides not to view, and from viewing notifications presented to their page from other users. “It lets its users to either hide content from individual users, hide content that its similar to the one displayed or to turn on the notifications when your favorite friend, person or page post something. It also shows you the posts from friends and pages, with whom you interact the most” (Platform, 2019).

However, the concept of neural networks aiding in personalization does come with ethical concerns. These concerns pertain to the idea of hidden bias being used through the “black box” classification system. “In machine learning, these black box models are created directly from data by an algorithm, meaning that humans, even those who design them, cannot understand how variables are being combined to make predictions” (Rudin & Radin, 2019). With the implementation of the “black box” users cannot see the type(s) of algorithms that are being used inside of the black box. Which destroys the idea of transparency for what the user’s information is being used for. “Credit raters, search engines, major banks, and the TSA (Transportation Safety Authority) take in data about us and convert it into scores, rankings, risk calculations, and watch lists with vitally important consequences. But the proprietary algorithms by which they do so are immune from scrutiny, except on the rare occasions when a whistleblower litigates or leaks” (Trites, n.d.).

For our company to properly run the social media network, we will have to adhere to GDPR law. Some portions of the GDPR will affect how users personalize their experience, but in the end will allow us to operate our social media network properly in the EU. These portions include Data minimisation, Storage Limitation, Purpose Limitation, and Confidentiality. The GDPR states that data minimisation is “Personal data shall be: (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)” (Principle (c): Data minimisation). This means that we are to acquire only the needed amount of personal data from a user for which is needed to fulfil the purpose of bringing them a more personalized user experience, and that if more data is retrieved than what is needed. We are in violation of the principle. In this the network must present what amount of data is needed from the user that will be adequate enough to provide that type of experience for them. The storage limitation principle states that we are allowed to store personal data, but not longer than a specified period. This ensures that the data being stored does not cause inaccuracies due to being out of date and reduces risk in the case that it becomes irrelevant (Principle (e): Storage limitation). The storage limitation principle works well with the GDPR’s idea of confidentiality. The GDPR has it so that the appropriate level of security is needed for personal data that is collected be protected while it is being held. One form of this security is having personal data encrypted. “Information is encrypted and decrypted using a secret key. (Some algorithms use a different key for encryption and decryption). Without the key the information cannot be accessed and is therefore protected from unauthorised or unlawful processing” (What is encryption). The purpose limitation principle states that, ““1. Personal data shall be:(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes” (Principle (b): Purpose limitation). For the purpose limitation, we are making sure that have clearly defined what it is we are collecting from our users in the form of their personal data, we are complying with specified purposes of collecting that data, and if anything were to change in our plan or the possibility of the personal data being disclosed, we as a social network are completely transparent and lawful in the use of that personal data.

With the company’s use of neural networks, there are some legal concerns that do arise. First, is the implication of protection of personal data that users are inputting into our system. If we comply with keeping user information confidential and store the data no longer than what is necessary for the training of the neural network. We would be staying within the guidelines of the GDPR. The company would also be able to actively enhance the user experience with still being allowed to collect personal data, but there would need to be ways incorporated to keep that data safe from negative use or being stolen. Due to neural networks and deep learning in machine learning having an issue with bias. The legal concern that is rooted here would be the liability that the company has for the use of information that was collected to train the neural network. To accurately stay within the guidelines of the GDPR, the social network company would have to hire a diverse team that would pull data from all social standings that people who would use the network come from.

To ensure that our company’s social network is in compliance with the GDPR guidelines, we should focus on current trends that focus on preserving the privacy of our users’ information. In addition, apply changes to our neural network that follow the guidelines. The use of Differential Privacy allows for accurate data analysis and provides privacy as well. “The mechanism used by differential privacy to protect privacy is to add noise to data purposefully (i.e. deliberate errors) so that even if it were possible to recover data about an individual, there would be no way to know whether that information was meaningful or nonsensical” (Ved, 2023). Homomorphic encryption provides another layer of security and enforces GDPR guidelines. “It is a crypto system that allows computations to be performed on data whilst it is still encrypted, which means confidentiality can be maintained without limiting the usage possibilities of the dataset” (Ved, 2023). This allows the neural network to use personal data from users and allows that data to stay protected. If the company was to follow a path without collecting data, we could use Federated Learning. This is a flexible approach to machine learning that allows users to help train the neural network by using their locally available data to input model improvements. There is no sharing of data. The user sends abstract improvements that they input back to the server (Ved, 2023).

References:

McCullum, N. (2021, April 28). *Deep Learning Neural Networks explained in plain English*. freeCodeCamp.org. https://www.freecodecamp.org/news/deep-learning-neural-networks-explained-in-plain-english/

*A beginner’s Guide to Neural Networks and deep learning*. Pathmind. (n.d.). https://wiki.pathmind.com/neural-network

The University. (1978). *What is ...* Amazon. https://aws.amazon.com/what-is/neural-network/#:~:text=Neural%20networks%20can%20track%20user,that%20interest%20a%20specific%20user.

Platform. (2019, July 4). *7 examples of personalization and customization for better UX*. Medium. https://plat4m.medium.com/7-examples-of-personalization-and-customization-for-better-ux-1d6eb78ab159

Rudin, C., & Radin, J. (2019, November 22). *Why are we using black box models in AI when we don’t need to? A lesson from an explainable AI competition*. Harvard Data Science Review. https://hdsr.mitpress.mit.edu/pub/f9kuryi8/release/8

Trites, A. (n.d.). Black Box Ethics: How Algorithmic Decision-making is ... http://gmj-canadianedition.ca/wp-content/uploads/2020/06/03\_Trites-Volume-11-issue-2-Final.pdf

*Principle (c): Data minimisation*. ICO. (n.d.). https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/data-minimisation/

*Principle (e): Storage limitation*. ICO. (n.d.-b). https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/storage-limitation/

*What is encryption?*. ICO. (n.d.-c). https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/encryption/what-is-encryption/

*Principle (b): Purpose limitation*. ICO. (n.d.-a). https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/purpose-limitation/

Ved, A. (2023, April 19). *How to develop artificial intelligence that is GDPR-friendly*. TechGDPR. https://techgdpr.com/blog/develop-artificial-intelligence-ai-gdpr-friendly/