Andrew Vue

SNHU CS-370-H7429

4-2 Project One

Neural networks are a system of algorithms that identify and define the relationships in a collection of data like the way a human brain functions. The neural network contains three layers, the input, output, and hidden layers. The individual layers are connected by nodes that connect similar to the brain synapses. To explain the different layers as simply as possible, the input layer connects to the hidden layers and after running through the algorithms within the hidden layers the results are shown in the output layer.

The input layer consists of functions that takes in data that is fed into the neural network and connects the algorithms within the hidden layer. The hidden layers are made up of nodes of algorithms that are used to process the data for necessary actions. These actions are mainly calculations that are used for a specific outcome or purpose created by the developer. The output layer is where the outcomes or “finished products” of these calculations are delivered.

Neural networks are used to aid in personalization of the user experience in many different fields like finance, healthcare, government, and commercial private sector businesses. Neural networks are used in creating models to calculate personalized preferences. In Amazon they utilize user data to make train their models to make product recommendations based on user activity and purchase history, “Amazon Forecast uses machine learning to generate accurate demand forecasts, without requiring any prior ML experience for inventory planning…Amazon Forecast can now use Convolutional Neural Networks (CNN)” (AWS amazon).

Convolutional Neural Networks are networks that are more advanced and used to handle data that contain image, speech, or audio signal inputs (IBM Cloud Education). The data input that these neural networks utilize come directly from the users themselves as their transactions are recorded and fed back into the network in a loop. With a constant supply of data, the neural network can be configured to give specific item recommendations.

Potential concerns arise from “black box” systems when the algorithms are not tested for bias. There are many occasions where bias occurs in algorithms because of developer/creator biases. There is also bias in data used to train these models, like that of the COMPAS program used by police to identify re-offenders. These models were gave data was bias along with the use of a feedback loop, “the problem of feedback makes traditional batch learning frameworks both inappropriate and incorrect. Hiring algorithms only receive feedback on people who were hired, predictive policing algorithms only observe crime in neighborhoods they patrol, and so on. Decisions made by the system influence the data that is fed to it in the future” (Ensign, et. al.). The lack of transparency and review can lead to unintended consequences due to errors in the process of data collection, utilization, and training of the neural networks.

In the case of COMPAS it may lead to issues of biased policing and biased policies. There are also issues of patient privacy and safety concerns. There was a case where a father found out that his daughter was pregnant through Target ads. This is a major concern for privacy for patients and for customers alike. In cases like the Target ad, it could be that a customer may be in an abusive relationship and can be a cause for concern regarding their health and safety.

The General Data Protection Regulation (GDPR) is one of the strictest privacy and security law in the world. The four important principles are transparency, purpose limitation, data minimization, and accuracy. Transparency refers to the personal data of users, meaning that all use information regarding this type of data must be clear and easy for users to understand. The Purpose Limitation rules limits the collection and use of personal data must be for specific, explicit, and legitimate purposes. Data minimization means that any personal data collected have to be adequate, relevant, and limited to what is required in relation to the purpose it was collected for. The Accuracy portion of the GDPR needs for any and all personal data to be correct and up to date wherever it is required.

Legal concerns may arise from a company’s use of neural networks are at risk of violating the Data Minimization and Purpose Limitation rules. This makes it significantly important for companies that utilize neural networks for personalized user experiences. The collection and use of the user data must be explicit and clearly laid out. There must also be limitations put in place to restrict the ‘unauthorized’ use of the data. Though, this is difficult to prove and track unless a company is strictly audited for violating these laws. Some companies that have violated these laws are Amazon, WhatsApp, Google Ireland, and Google in 2021 (Komnenic).

Company’s business models vary, but all companies collect data regardless of the sector they are in. Any information from a user, client or customer is considered data. This includes intake forms, transactions, invoices, and any interaction. This is because everything is tracked either through literal paper or digitally. There are assumed ‘privacy rights’ that are given up by the customer in certain circumstances, like CCTV or Security Cameras in certain locations. There are companies that operate in certain industries and geographic locations that require some level of data collection. The banking and financial industry require ‘paper trails’ for proper reporting and to have for their audits. The importance of data collection to a company is that of life or death for the company as it allows them to remain relevant and competitive. The utilization and ensuring the are compliant with laws are the main concern for these companies. Many companies are documenting and employing large teams to ensure that their practices are compliant with laws and regulations. Some companies get around this by providing data collection disclosures and agreements to customers.

References:

AWS Amazon. (Aug. 12, 2020). Amazon Forecast now uses Convolutional Neural Networks

(CNNs) to train forecasting models up to 2X faster with up to 30% higher accuracy. Retrieved from <https://aws.amazon.com/about-aws/whats-new/2020/08/amazon-forecast-now-uses-convolutional-neural-networks-cnns-to-train-forecasting-models-up-to-2x-faster-with-up-to-30-percent-higher-accuracy/>

Ensign, D., Friedler, S.A., Neville, S., Scheidegger, C., Venkatasubramanian, S. (Dec 2017).

Runaway Feedback Loops in Predictive Policing. Retrieved from: <https://arxiv.org/pdf/1706.09847.pdf>

Hill, K. (Feb, 16 2012). How Target Figured Out A Teen Girl Was Pregnant Before Her Father

Did. Retrieved from https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=4f84599b6668

IBM Cloud Education (Oct 20, 2020). Convolutional Neural Networks.

Retrieved from <https://www.ibm.com/cloud/learn/convolutional-neural-networks>

Intersoft Consulting (n.d.) General Data Protection Regulation GDPR.

Retrieved from https://gdpr-info.eu/

Komnenic, M. (Mar, 31 2022). 36 Biggest GDPR Fines & Penalties So Far [2022 Update].

Retrieved from https://termly.io/resources/articles/biggest-gdpr-fines/

Krogh, A. (2008). What are artificial neural networks? Nature Biotechnology Vol. 26.

Nature Publishing Group.

Wu, J., &amp; Jia, L. (2022). Neural network model for perceptual evaluation of Product

Modelling Design Based on multimodal image recognition. Computational Intelligence and Neuroscience, 2022, 1–10. <https://doi.org/10.1155/2022/1665021>