**Matt Knutson**

**CS-370: Current & Emerging Trends In Computer Science**

**SNHU - Instructor Richard**

**September 29th, 2024**

**Project One**

What is an artificial neural network, and how does it work? A neural network is a network of nodes that process data via algorithms in order to recognize patterns and optimize their decision-making. This process is called Deep Learning, a subset of Machine Learning, and is meant to mimic the neuron activity that takes place within the human brain. Within the neural network, there is an input layer, a hidden layer/layers, and an output layer. Typically, the input layer breaks down images into individual pixels and then applies weighted amounts to the data. That data is then sent to the next level of nodes in a hidden layer where a bias is added. The weighted amount, correlating pixel value, and bias are computed, and that value is sent to an activation function. The final result from the activation function determines whether an individual node is relevant and will fire moving forward. This result is presented to the output layer where the system’s predictions are compared to real-world data. The amount of error is also determined during the final stages and the weights and biases are then adjusted throughout the system. The new data is then fed back through the system and the entire process is repeated until the desired result is produced.

Neural networks identify patterns in a user’s data and actions in order to facilitate a unique and personalized experience to the user. This can be accomplished in a couple of different ways, and they rely heavily on the weights located within the neural network. Content Filtering associates’ heavier weights with items that a user enjoys and then groups those items in different categories. New items are then recommended to the user from these categories. A weight can also be associated with how closely each item represents the category it is in, which produces much more accurate results when the system makes suggestions.

Another way neural networks use patterns to provide personalization is called Collaborative Filtering. This approach takes all the known user data and transfers it into a grid with very specific categories. A neural network is then run on the data until an exact replica of the known data is produced in a new grid. During this process all the unknown variables are discovered when the matching set is found. This tactic relies solely on unknown patterns found within data from all the system’s users. Since these are unknown patterns, the ways in which the network has determined biases to adjust the system are also unknown. These are called black-box algorithms, and although they can be useful, they also cause concern for the user. For instance, if these algorithms are making decisions and reconfiguring their bias based on the repetition of the wrong data, or variable, then they can cause havoc in public affairs such as the employment market and the judicial system by making racist and sexist predictions. It is very important for the users and the developers to understand the decision-making process behind these technologies.

The GDPR stands for General Data Protection Regulation, and it is a security and privacy law that is being introduced to protect online users’ data from being exploited by large corporations. When it comes to the black-box situation mentioned earlier, the GDPR aims to hold companies responsible for providing transparency concerning their algorithms. This will help everyone understand how biases are determined and help reduce negatively impacting biases. It also puts responsibility in the hands of the company when disclosing how the user’s data is used in those algorithms. The GDPR also sets limits on the amount, and type, of data that can be collected from users, requires that the users have the option to not have their data collected at all on a website, and gives them the right to be forgotten by the company. This law also limits the amount of time that a user's data can be held in a database and strictly holds the company accountable for keeping the user’s data confidential and unrecoverable.

Due to this application being centered around social media, and in the business of correctly recommending content to its users, it will need to collect some data from each user. Or a user could opt out of any data collection and effectively silence recommendations from the app. When data is being collected, there is a risk of it being tampered with, or stolen, while it is being transferred or stored. This can lead to identity theft and improper use of a user’s data, which pose as large legal concerns for the project. Using artificial neural networks can also create unexpected biases based on the user data it collects, creating a foundation for future lawsuits if the algorithms are not properly understood.

The company has several options it can utilize in order to comply with the GDPR. These strategies should be combined and monitored regularly to ensure that best practices are being

used. First of all, the user should be given an option to whether or not they want their data collected at all. This should be presented in the form of a Consent Banner before the user can proceed and use the app. If they choose to allow for data collection, it should be disclosed to them, in a very clear and easy to understand way, what data is collected, why, and how long it will be stored. It should also be very easy to locate and access data collection settings within the application. This includes the option for the “Right To Be Forgotten”.

Second, the staff of the company will need to be trained on regulations pertaining to the GDPR and learn how to maintain the ongoing flow of data according to these laws. As the company and website grow, there will be a need to implement a Data Protection Officer, or Data Protection Team, to monitor data activity and ensure it is being handled properly throughout the system. All user data that is collected should be organized, monitored, and managed by the team so that it is easy to interpret at any time. Finally, encryption will need to be used throughout the system on data in transit and on data at rest in the database. This adds an extra layer of protection for the user while the application is in possession of their data and prevents data from being hijacked or leaked.

**Citations**

**Beysolow, T. (2019). Applied Reinforcement Learning With Python: With OpenAI Gym, Tensorflow, and Keras. Apress.**

**Current Opinion In Systems Biology. (2017). Grid Cell. ScienceDirect Topics. https://www.sciencedirect.com/topics/biochemistry-genetics-and-molecular-biology/grid-cell**

**Fernandez, E. (2023, October 5). AI Is Not Similar To Human Intelligence. Thinking So Could Be Dangerous. Forbes. https://www.forbes.com/sites/fernandezelizabeth/2019/11/30/ai-is-not-similar-to-human-intelligence-thinking-so-could-be-dangerous/#3fbd0b846c22**

**GeeksforGeeks. (2024, June 16). What Is Markov Decision Process (MDP) And Its Relevance To Reinforcement Learning. GeeksforGeeks. https://www.geeksforgeeks.org/what-is-markov-decision-process-mdp-and-its-relevance-to-reinforcement-learning/?ref=oin\_asr1**

**Gulli, A. (2017). Deep Learning With Keras: Implement Neural Networks With Keras On Theano And Tensorflow. Packt Publishing.**

**Heilweil, R. (2020, February 18). Why Algorithms Can Be Racist And Sexist. Vox. https://www.vox.com/recode/2020/2/18/21121286/algorithms-bias-discrimination-facial-recognition-transparency**

**Hockney, M. (2024, July 22). Organic Intelligence (O.I.): Why Humans Will Always Beat A.I.**

**Khan Academy. (n.d.). Overview Of Neuron Structure & Function. Khan Academy. https://www.khanacademy.org/science/biology/human-biology/neuron-nervous-system/a/overview-of-neuron-structure-and-function**

**Krizhevsky, A. (2017). The CIFAR-10 Dataset. CIFAR-10 And CIFAR-100 Datasets.**

**https://www.cs.toronto.edu/~kriz/cifar.html**

**Maczka, P. (2024, August 21). The Role Of AI And Machine Learning In Data Protection. Storware.**

**https://storware.eu/blog/the-role-of-ai-and-machine-learning-in-data-protection**

**Mandy. (2018). *DeepLizard Reinforcement Learning*. YouTube. https://www.youtube.com/channel/UC4UJ26WkceqONNF5S26OiVw**

**Narayanan, R. (2019, March 27). Myths About AI Decoded. Medium. https://medium.datadriveninvestor.com/myths-about-ai-decoded-c0b9719245f**

**Nicholson, C. (2023). A Beginner’s Guide To Neural Networks And Deep Learning. Pathmind.**

**https://wiki.pathmind.com/neural-network**

**Official Journal Of The European Union. (2016, April 27). Legal Text. General Data Protection Regulation (GDPR).**

**https://gdpr-info.eu**

**Recosense. (2021, September 28). *Deep Learning In Personalization*. Recosense Labs Inc.**

**https://www.recosenselabs.com/blog/deep-learning-in-personalization**

**Schneider, J., & Vlachos, M. (2021). Personalization Of Deep Learning. Data Science – Analytics and Applications, 89–96.**

**https://doi.org/10.1007/978-3-658-32182-6\_14**

**Silipo, R. (2020, March 5). How To Keep Bias Out Of Your A.I. Models. CustomerThink.**

**https://customerthink.com/how-to-keep-bias-out-of-your-ai-models**

**Spillane, J. (2022, December 8). How GDPR Can Undermine Personalization & User Experience. Business2Community. https://www.business2community.com/customer-experience/how-gdpr-can-undermine-personalization-and-user-experience-02108269**

**Stahl, B. C., & Wright, D. (2018, June 25). Ethics and Privacy In AI And Big Data: Implementing Responsible Research And Innovation. IEEE Journals & Magazine. https://ieeexplore.ieee.org/document/8395078**

**Trafton, A. (2022, November 2). Study Urges Caution When Comparing Neural Networks To The Brain. Massachusetts Institute of Technology. https://news.mit.edu/2022/neural-networks-brain-function-1102**

**Ved, A. (2024, February 22). How To Develop Artificial Intelligence That Is GDPR-friendly. TechGDPR. https://techgdpr.com/blog/develop-artificial-intelligence-ai-gdpr-friendly**

**Xiang, M. (2019, November 6). Bias: What It Means In The Big Data World. Medium. https://towardsdatascience.com/bias-what-it-means-in-the-big-data-world-6e64893e92a1**