Breunna Bingham

Southern New Hampshire University

May 24, 2023

CS-370 Current/Emerging Trends in CS

Project One

Neural networks are what make up the human body. The same is true for artificial neural networks. We have an input layer that receives raw information, this can be represented by the human eye and what we visualize with our eyes. The hidden layers are what comes next in the neural network and it is where all the “thinking” takes place. There are nodes which hold small bits of knowledge and this input layer, what we see from our eyes, is transmitted across several individual nodes within the hidden layer to finally arrive at our output layer. This layer is the decision that was made from running through all of the nodes in the neural network. To further break this down let’s use the example of the human eye as I have prior. Let’s say you take the same route to work every day, but today you seen that the traffic is backed up, and if you continue on this route, you will be late for work. That is our input layer. Now the hidden layers with all of the nodes come into play. Now you are thinking about all the possible alternative routes that you can take to get to work so that you are not late. Each route is a different node that holds more information, in this case, some nodes are highways and therefore will get you to work quicker than other nodes that single lane back roads full of school buses picking up children. Obviously, we will avoid the single laned back roads and choose a highway. One highway goes 5 miles out of the way while the other is only 2 miles out of the way. This is where we arrive at out outcome layer. The outcome is that we will choose to take the alternative route that involves a highway that is only 2 miles out of the way to get to work on time. So this is where the action happens and if this wasn’t a good idea, we learned that this route ended up being backed up by heavy traffic, and therefore next time we will avoid it. This is how neural networks learn.

Neural networks are used to aid in the personalization for the user experience by providing them with customized games, contacts, groups to join that have the same shared interests as the user, recommended posts and discussions for the user to see and join. For example, Jane is a 34-year-old, who just announced her pregnancy on social media. Because of this, Jane would now have a personalized experience that suggested new mother support groups to join with other pregnant women. She may also see advertisements about baby and maternity products. If Jane joins a mother’s group, she may be interested in adding a few of the users as personal friends to her social media account, and they would conveniently show up as suggestions. This provides the user with a personalized and enjoyable experience. There are also ethical concerns that can arise from creating such a personalized experience. Hidden bias can be a prime example of an ethical concern. Users should know what data is being used to create this personalized experience as well as the algorithm used to shape that personalized experience. Humans make these algorithms and therefore can contain hidden bias within them unintentionally. The best way to avoid having hidden biases in the algorithm is to make sure the data set used to create this algorithm is accurate and up to date with current trends and users. Additionally, the data needs to be from a mixed cultural perspective and contain both men and women.

Portions of the GDPR can affect personalization. Personalization is everything I stated above. It gives the user a personalized experience that is enjoyable and meaningful for the user. The GDPR has policies that need to be honored, and that can make it difficult to both honor those policies and create and maintain a personalized experience for each user. One portion of the GDPR that affects personalization is the transparency principle. All the personal data obtained from the user needs to be used in a clear and transparent manner that is written out to the user for the user to give permission to use their data. Full transparency can be difficult when there are many different uses for the data that is collected. And any time that data is used for a different reason other than previously obtained permission for, the user needs to re-consent for these changes, which can be annoying to the user and cumbersome. That is why in most cases the permissions that users are asked to involve more uses for the data than it is being used for. Which brings us to another portion of the GDPR that affects personalization, and that is data minimization. Data minimization is the principle that states that all of the personal data that is collected is limited to only the data needed to fulfil a purpose. This means that no longer can companies ask for permissions that they are not actively using but could use in the future. In addition to data minimization, another policy that again falls into this category, is storage limitation. This means that if the user granted permissions for personal data to be used, and the personal data is no longer being used for that purpose, but the data is still being stored anyways, that is against the storage limitation principle of the GDPR. All data that is stored needs to be periodically reviewed and erased when it is no longer needed or used. Lastly, the security principle or the confidentiality and accountability principle of the GDPR. This principle is an important one especially when data stored is excessive and contains personal confidential information, which could be financial information, address, phone, workplace information and more. The more personal data that is stored to provide a personalized experience to the user, also poses a large risk to the company if they fall victim to a security breach. Appropriate security measures need to be in place at any given time to protect all of the personal data that is stored.

The GDPR is affecting the company’s practices by creating legal concerns about the use of personal data as a classifier to create a personalized experience for the user. By being transparent and limiting the data that we obtain on so many different levels of criteria, we will potentially be opening up gaps in the legality side of things and that is a major cause of concern. Permissions for personal data intake and storage need to be written to make sure they comply with the laws, but also the strict standards of the GDPR. The way that the GDPR has written it’s principles is intentionally vague and therefore makes it hard to consistently maintain compliance with their standards. Furthermore, it requires a heightened level of security as well as an increase in the number of employees to carry out such changes and comply with the security standards. Federated Learning may be an avenue that the company can gain more insight into to eliminate the amount of data that the company collects and instead the algorithms that use the data are moved to the user’s computers. Over time the user will help train the model to create a personalized experience for them. If Federated Learning proves to not be an option for the company, then perhaps Matrix Capsules could be an appropriate step in requiring less data for learning.

Some of the current best practices for preserving privacy with machine learning and artificial intelligence include what I mentioned above, which is the Federated Learning. Federated Learning which uses localized devices like computers or mobile phones that train the machine learning models. Another option for preserving privacy is with differential privacy. Differential privacy works by allowing data to be viewed and analyzed but does not reveal any sensitive information that would allow any individual in the dataset to be recognized.

The company needs to make changes to comply with the GDPR. In such ways I believe that Federated Learning can be utilized so that personal data collection is minimized. What data we do collect needs to be transparent to the user in terms of intended use. All data that is collected will be minimized and needs to be utilized properly and expunged when no longer being used. In addition, quarterly checks of accurate information as well as storage limitation practices need to be upheld and kept current. Personal data that is obtained will only be stored for a max of 1 year and then new permissions will be asked. All permissions that are being asked for from our users will all be utilized to their fullest extent as written transparently to our users in our permissions request. Users have the right to revoke their permissions at any time and all personal data stored from the user who previously gave permission will be deleted entirely. Additionally, security measures will be elevated to match the requirements as set forth by the GDPR. We have a right to our users to protect the data that they entrusted to us.

# References

Burns, E., & Burke, J. (2021). What is a neural network? Explanation and examples. *Enterprise AI*. https://www.techtarget.com/searchenterpriseai/definition/neural-network

Dorschel, A. (2021, December 9). Rethinking Data Privacy: The Impact of Machine Learning. *Medium*. https://medium.com/luminovo/data-privacy-in-machine-learning-a-technical-deep-dive-f7f0365b1d60

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

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

*Top five concerns with GDPR compliance*. (n.d.). Thomson Reuters. https://legal.thomsonreuters.com/en/insights/articles/top-five-concerns-gdpr-compliance

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