Aaron Shipley

CS 370: Project 1

Southern New Hampshire University

Timothy Alexander

11/17/2022

To understand the application and its functions of data usage, one must first understand the neural networks the application is comprised of. First, we will discuss what a neural network is. A neural network comprises several interconnected neurons, organized in layers, that exchange messages when certain conditions happen (Gulli, Pal, 2017). When neurons exchange messages, it is often referred to as firing. Artificial neural networks (ANN), such as the ones incorporated into the application are inspired by Biological neural networks (BNN). The basis for the neural networks in the application is a class categorized as deep learning. Deep learning neural networks are categorized by many layers of neurons (Gulli, Pal, 2017). These layers can learn sophisticated models based on progressive levels of abstraction. ANNs are better understood as resembling the optic nerve of a mammal's eye. The layers represent the layers within the optic nerve of an eye, and the nodes are the artificial equivalent of the cellular neurons found in a BNN.

The layers that an ANN is comprised of fall into three types of different layers. The first layer is known as the input layer. This layer receives the raw data as input into the neural network. The next layer is known as the hidden layer. This layer contains activation nodes, where training and processing are done within the network (Ognjanovski, 2019). This layer is known as hidden because it is neither an input nor an output layer. The next layer is the output layer. This layer is responsible for the network's output. Within each layer, nodes are contained. Each node is a mathematical function that computes an input weight(s). The larger weight(s) have a greater effect on the neuron's output. Within the input layer, the neurons (nodes) receive raw data input and compute the weight(s) put on the input. The input layer’s nodes are passive due to this being the initial layer of the network (Techopedia, 2018). Each node within the layers is connected to each node within the hidden layer the data is passed to from the input layer after the activation function. According to Sharma (2017), the activation function is used to get the output from a node.

In the hidden layer, the data is then computed with the weights and biases and then passed through the activation function to get the output of each node. This layer is the main layer where computation is heaviest and training of the network is taking place. Each node within the hidden layer is connected to input and output layer nodes. The data is then transferred to the output layer. According to Ponnambalam (2021), The output layer is the final layer in the neural network where desired predictions are obtained. The output layer contains its weights and biases it computes on the data before the desired output is derived from the network.

ANNs are a useful tool among companies that apply them to their applications. For example, our social networking application utilizes ANNs to provide a more personalized user experience. An ANN can use a user’s location and recommend stores, restaurants, businesses, or events relevant to the user's location. It can also be used to collect data via clicks, page time, selected items, or a suggestion of friends based on their current friends list. This data can be used to train a neural network to apply suggestions to the user to create a more positive user experience. The ANN creates these experiences via different models created and trained based on weights and biases put in place on the nodes going through each layer. Each layer can have its own set of weights and biases to better define the desired output of the ANN. For example, potential weights put on data could be keywords (hashtags, titles, tagged people, etc.). This data can then be used on the data in the node to train the network to provide a more accurate output.

With ANNs in social media, some ethical concerns may be raised. A concern that may arise with the use of ANNs is the potential transparency of the ANN itself. Unlike other systems where the code itself is easily explainable to maintain transparency of the system, ANNs contain multiple layers, mainly the hidden layer(s), that are much more complex to explain and help maintain transparency (Long, 2020). Another ethical concern is the storage of data. Among the general public, most users need a more technical understanding of neural networks and the processes used by them. This leads to the issue of black box networks. Black box models in networks collect data and train it within the hidden layer(s) of the network and output the data without a true understanding of how the network computed the prediction (Rudin, Radin, 2019). This issue leads to a need for more transparency as well. The data being trained can be stored for later use as well. This data is stored may not be relevant to users immediately but can be stored for much later use. This storage of data long term increases the severity of potential data breaches with larger implications in contrast to that of a network that only stores relevant data in short-term intervals.

With the GDPR (General Data Protection Regulation) being implemented in 2018, the use of ANNs and the data needed for proper training in such networks have been drastically affected. The EU (European Union) has implemented the GDPR as the “Toughest privacy and security law in the world (GDPR, 2022)”. The reason for the “toughness” of the GDPR is to hold companies and organizations accountable for the responsible and ethical collection and use of data from people within the EU. There are four sections of the GDPR that affect our social media application and the collection and use of data. The four categories are transparency, storage limitation, accuracy, and data minimization. These four areas affect the application the greatest and must be kept at the forefront of the development and implementation of ANNs within the system.

According to the GDPR (2022), transparency is “being clear, open and honest with people from the start about who you are, and how and why you use their personal data.” With the complexity of ANNs, we cannot be completely transparent in terms of why certain data is being used to personalize a user’s experience, but we can be transparent in the amount of data and why we use personal data in general. By identifying who we are and why we use their data, our social media application can openly curate a personalized experience for the user while allowing the user to consent to the collected data and understand its reasoning.

Storage limitation is the next pillar of the GDPR that affects our social media application in its pursuit of creating a personalized experience for the user. This category may be one of the trickier portions of the GDPR to comply with fully. According to the GDPR (2022), data should not be stored for any longer than it is necessary, be deleted or anonymized when the data is not relevant, follow strict policies regarding storage and deletion, and assurance to users of the right to the erasure of data if no longer needed. The first portion of storing data for certain time frames is important to comply with. Nevertheless, how does one know how long is too long? Jams Spillane (2018) discusses how GDPR can undermine personalization via the right to be forgotten. Customers have the right for a business to delete their data after usage. This helps keep companies and organizations from exploiting the data for longer than is relevant but harms other businesses who ethically use the data in a proper time frame from creating a personalized experience. Data storage is a per-use concept that must use policies to enforce the storage time frames

strictly.

The data's accuracy is essential to comply with GDPR standards. A company or organization must ensure that data is accurate and up to date to ensure accuracy. Data must be updated promptly, depending on what it is being used for. Once again, this pillar can undermine the personalization of user experience. For example, say a user consents to cookies being used on the social media platform after the application has initially loaded. This will create an inaccurate personalized experience due to no data being used from the start (Spillane, 2018). This data inaccuracy can lead to one needing to be more compliant with the accuracy of the data being used. Keeping data up to date is tough in this regard as well. A user may find the data collected and used inaccurately if the personalization of their experience matches their expectation. This objective lens of accuracy can lead to difficulties in maintaining compliance.

Data minimization is the final pillar affecting our social media application in terms of personalization. Data minimization must be compliant in multiple facets according to the GDPR. First, data must be complete enough to fulfill the desired purpose of the data collection. Our social media application will collect enough data to fulfill its purpose in order to provide a personalized experience. This data must be relevant as well. The data collected must pertain to the purpose of data collection (GDPR, 2022). Our application must collect data for a specific purpose. It should not collect data that would not be identified within the ANN specification and use the data for unintended purposes. This unethical data collection could lead to the loss of users and inaccurate outputs produced by ANNs. The data must also fit within the amount necessary to fulfill the previous rules. One does not need o collect excessive data if it is not necessary to produce an accurate and personalized experience.

Using ANNs that are not compliant with GDPR or local, state, or federal laws can cause many issues. For example, illegally mining data from a user to exploit it for personal gain can be considered a violation of privacy and even illegal in many places. One such example is in France; a company responsible for an application must be able to disclose, in detail and intelligible format, how this algorithmic process makes its decisions regarding collecting and using data within the ANN (Lavall, 2019).

However, is it possible to personalize an application, such as our social media app, to a user without collecting data? From a professional perspective, the personalization of an application cannot be done without the collection of user data to some degree. As discussed previously, the consent to use cookies in a web app only allows the application to start collecting data after the page's initial load, making it not personalized from the start (Spillane, 2018). Data must be collected in order to personalize an experience. Much like biological neural networks (BNN), ANNs require data to be input into it in order to train and "learn" based on the data. Humans do this within our internal BNNs. For example, one does not simply greet every person they meet with the same generic greeting. A human may greet a close friend differently than a coworker based on the data that has been collected and stored to create a personalized experience with each individual. This basic example justifies the collection of data in order to create personalization. Data collection is hotly debated, but if done ethically and legally, the use of the collected data can positively affect the user's experience.

With the prevalent usage of Artificial Intelligence and Machine Learning, there is a contested debate about the amount of usage is the proper amount. As a result, some AI and ML systems have vulnerabilities that have been publicly exposed. Some of these vulnerabilities are improper data leakage from one ANN to another via the traditional decentralized approach to “training” ANNs. One such counter to this vulnerability is the use of Federated learning. Wiggers (2019) states that federated learning is “a technique that trains an AI algorithm across decentralized devices holding data samples without exchanging those samples, enabling multiple parties to build a common machine learning model without sharing data liberally.” This concept will allow our social media to comply with GDPR standards such as data storage limitation, confidentiality, and minimization.

The data being collected and used for personalization within our application will also remain transparent to the required standards. The amount of transparency will depend on the type of data collected and finding the “correct” amount of transparency to provide a sense of trust from the user without creating a sense of unease and driving users away. Too much transparency can harm the company. This amount will have to be enough to allow the user to clearly understand the data collection and consent to the data being collected. If all parts of the data collection process were fully transparent, it might cause the user to distrust the application due to their ignorance of ANNs and the data collection process.

References

Burns, E., &amp; Burke, J. (2021, March 26). What is a neural network? Explanation and examples. SearchEnterpriseAI. Retrieved November 17, 2022, from https://www.techtarget.com/searchenterpriseai/definition/neural-network

IBM Cloud Education. (2022). What are neural networks? IBM. Retrieved November 17, 2022, from https://www.ibm.com/cloud/learn/neural-networks

Guide to the UK General Data Protection Regulation (UK GDPR). ICO. (2022). Retrieved November 17, 2022, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

Gulli, A., &amp; Pal, S. (2017). Deep learning with Keras: Implement neural networks with Keras on Theano and TensorFlow. Packt.

Kalinski, A. (2019, December 17). Personalization using machine learning - from data science to user experience. Medium. Retrieved November 17, 2022, from https://medium.com/booking-product/personalization-using-machine-learning-from-data-science-to-user-experience-3b1ef5d23ced

Lavall, E. (2019, October 8). Neural Network and liability: When the information lies in Hidden Layers. Lexology. Retrieved November 18, 2022, from https://www.lexology.com/library/detail.aspx?g=c1006a4d-dfbe-4487-a4de-0bc7eb1c64d8

Long, B. (2020, August 13). The ethics of deep learning AI and the epistemic opacity dilemma. Blog of the APA. Retrieved November 18, 2022, from https://blog.apaonline.org/2020/08/13/the-ethics-of-deep-learning-ai-and-the-epistemic-opacity-dilemma/

Ognjanovski, G. (2019, January 14). Neural networks: Everything you wanted to know. Toward Data Science. Retrieved November 17, 2022, from https://towardsdatascience.com/neural-networks-everything-you-wanted-to-know-327b78b730ab

Ponnambalam, K. (2021, November 17). The output layer - deep learning: Getting started video tutorial: Linkedin learning, formerly Lynda.com. LinkedIn. Retrieved November 17, 2022, from https://www.linkedin.com/learning/deep-learning-getting-started/the-output-layer

Rudin, C., &amp; Radin, J. (2019, November 22). Why are we using black box models in AI when we do not need to? A lesson from an explainable AI competition. Harvard Data Science Review. Retrieved November 18, 2022, from https://hdsr.mitpress.mit.edu/pub/f9kuryi8/release/8

Spillane, J. (2018, August 15). How GDPR can undermine personalization and user experience. Business 2 Community. Retrieved November 17, 2022, from https://www.business2community.com/customer-experience/how-gdpr-can-undermine-personalization-and-user-experience-02108269

Ved, A. (2021, November 15). How to develop artificial intelligence that is GDPR-friendly. TechGDPR. Retrieved November 17, 2022, from https://techgdpr.com/blog/develop-artificial-intelligence-ai-gdpr-friendly/

What is an input layer? - definition from Techopedia. Techopedia.com. (2020). Retrieved November 17, 2022, from https://www.techopedia.com/definition/33262/input-layer-neural-networks

Wiggers, K. (2019, December 22). Ai has a privacy problem, but these techniques could fix it. VentureBeat. Retrieved November 18, 2022, from https://venturebeat.com/ai/ai-has-a-privacy-problem-but-these-techniques-could-fix-it/