SNHU

4-2 Project One

CS-370-11333-M01

Jensen, Bryston
6-1-2024

Bryce Jensen
CS-370-11333-M01
4-2 Project One
6/1/2024

Explain the basics of neural networks and how they work

Imagine you are trying to get a computer to recognize different animals. You want it to identify dogs, cats, birds, and “other” animals. A neural network is a type of artificial intelligence (AI) that would help the computer learn how to do this by looking at thousands of examples.

Here is how it works using an input layer, hidden layers, and an output layer:

Input Layer

This layer takes in the information about the animal, like its shape, color, and size. It gives the computer a whole bunch of clues about what kind of animal it is looking at.

Hidden Layers (there can be many)

This layer is where the magic happens. The input layer sends the clues to the hidden layer, which starts to figure out patterns and relationships between those clues. It’s like the computer is saying, “Ah, I see! So, an animal with a fluffy tail and pointy ears might be a cat!”

Output Layer

This layer takes all of the information it got from the hidden layers and makes a final decision on what type of animal it might be.

How do they interact with one another? Here is a simple example:

Bryce Jensen
CS-370-11333-M01
4-2 Project One
6/1/2024

1. The input layer sends clues (like shape and color) to the hidden layer.
2. The hidden layer looks at all those features and says, “This animal has a straight pointy tail, floppy ears, short hair, and is brown and white. I haven’t seen many cats or birds with those features, but I have seen some of those on a dog before.” The final hidden layer sends all of this to the output layer.
3. The output layer makes a final decision about what category to put it in, dogs, cats, birds, or “other” animals. Based on all the information from the hidden layers it says, “Based on all of these clues, I’m going to guess that this is a dog.”

This is a short and simple explanation of how neural networks work. They use layers of processing to help a computer learn and make decisions based on patterns in data.

Evaluate how neural networks are used to create personalization

Neural networks can be used to personalize the user experience by analyzing individual behavior and preferences. **User profiling** can be used to create detailed profiles of users based on their interactions with a product or service. Those can be used to give **content recommendations** by analyzing the user profiles to recommend personalized content like products to buy, articles to read, or movies to watch. From there **targeted advertising** is used to more strongly resonate with the individual based on their interests and behaviors (Purificato, Boratto, & De Luca, 2024).

Bryce Jensen
CS-370-11333-M01
4-2 Project One
6/1/2024

This is where some ethical concerns arise. The article User Modeling and User Profiling states, “In the past few years, ethical concerns related to user modeling, particularly focusing on bias and fairness issues, have gained significant prominence (Purificato, Boratto, & De Luca, 2024).” Some ethical issues regarding neural networks that should be addressed are:

- Potentially hidden biases: Neural networks are “black boxes” meaning there are generally no clues to how the system generates the results. All the processing is hidden behind layers and layers of computations, and this can make it hard to find bugs or biases in the system (Barber, 2019).
- No user control: Users have almost no control over what (or how) the neural network outputs. Obviously, the prompt or other input can be changed, but the processing that is done in the background cannot be personalized in any way.
- Data privacy: A neural network has the capacity to store user’s data. This depends on how it was set up and what the intended purpose is, but many will store data for further training. This means that it can be trained with sensitive data, including personal information or even political beliefs – something that is extremely biased.

Analyze how portions of the GDPR affect personalization

These are only some locations in the GDPR where the topics are mentioned.

Bryce Jensen
CS-370-11333-M01
4-2 Project One
6/1/2024

Transparency

Found in Article 5.1.a, and Article 12.

Personalization should be transparent to whoever's data it is. This means that there should be clear information on the processing of one's data, including the purpose it is being used for, how it is categorized, and any third party that may receive the data. (GDPR, n.d.) (GDPR, n.d.)

Purpose Limitation

Found in Article 5.1.b.

Data can only be processed for specified, explicit, and legitimate purposes. This means that they must stipulate the purpose for collecting and processing the data when it is collected. They must also limit the processing of that data to those purposes. Using it for any other purpose needs to be avoided. (GDPR, n.d.)

Data Minimization

Found in Article 5.1.c.

Only the necessary personal data should be collected and processed. This helps prevent unnecessary data collection and helps maintain privacy (GDPR, n.d.).

Confidentiality

Found in Article 32.1.b.

Bryce Jensen
CS-370-11333-M01
4-2 Project One
6/1/2024

Personal data should be processed in a way that ensures the security of the data. The maximum security process should be used, with what is available, cost, purpose, risk, and scope taken into account (GDPR, n.d.).

Assess how the GDPR is affecting the company's practices

Based on the GDPR, several specific legal concerns may arise from the company's use of neural networks to personalize the user experience. I list some below along with the topic they fall under:

Transparency

The company must clearly explain how it uses data and what processing occurs. Since neural networks are complex, it is crucial to provide information about their functioning and decision-making processes.

Purpose Limitation

Data must be gathered for pre-specified purposes, not stored, and not used for any future use. The company will need to ensure that data collection is limited to the original purpose of personalizing the user experience. If it would need to be used for any other purpose, the user would need to give express permission to use that data.

Bryce Jensen
CS-370-11333-M01
4-2 Project One
6/1/2024

Data Minimization

The company would need to collect only the minimum required amount of data to achieve the intended purpose. They should avoid any unnecessary data collection or processing.

While it would be great if not collecting data were possible for this company, it is not necessarily a great option to fit our business model for the following reasons

- We have a **data-driven approach**. The company relies heavily on user data to create personalized experiences and adapt advertising strategies.
- It gives us a **competitive advantage**. By utilizing neural networks, the company gains an edge in understanding user behavior, which allows for better – and more targeted – marketing.
- It allows for better revenue generation. Data collection and the analysis that goes with it are essential to generating revenue through targeted advertising and sponsored content.

While not collecting data would seem like the most attractive option to avoid legal concerns, it would significantly impact the company's future, which relies on a data-driven marketing strategy. Therefore, the company must stay ahead of legal concerns by implementing the GDPR's recommended approaches for transparency, purpose limitation, and data minimization.

Bryce Jensen
CS-370-11333-M01
4-2 Project One
6/1/2024

Propose adaptations to the company's practices to act in compliance with the GDPR

Current Trends (Best Practices) in Artificial Intelligence and Machine Learning Aimed at Preserving Privacy:

- **Data anonymization** through something called a **decentralized shuffling algorithm**. Data privacy is super important, and researchers have found a way to allow AI to be used in research without compromising that data (KAUST, 2024). Juexiao Zhou, lead author of the paper said that this method ensures perfect privacy protection (KAUST, 2024).

Changes to comply with GDPR:

- Ensure that personal data is not retained any longer than necessary.
- Minimize the data that is collected. It should only be what is required and relevant to what is required for the application.
- The data the company collects should be accurate and up-to-date.
- The data should be secure. If the company has that data in their possession, they need to be responsible for protecting it.

Bryce Jensen
CS-370-11333-M01
4-2 Project One
6/1/2024

References

Barber, G. (2019, March 6). *Shark or Baseball? Inside the 'Black Box' of a Neural Network*. (WIRED) Retrieved from wired.com: https://www.wired.com/story/inside-black-box-of-neural-network/

GDPR. (n.d.). *Art. 12 GDPR Transparent information, communication and modalities for the exercise of the rights of the data subject*. Retrieved 06 02, 2024, from gdpr-info.eu: https://gdpr-info.eu/art-12-gdpr/

GDPR. (n.d.). *Art. 32 GDPR Security of processing*. Retrieved 06 02, 2024, from gdpr-info.eu: https://gdpr-info.eu/art-32-gdpr/

GDPR. (n.d.). *Art. 5 GDPR Principles relating to processing of personal data*. Retrieved 06 02, 2024, from gdpr-info.eu: https://gdpr-info.eu/art-5-gdpr/

KAUST. (2024, March 5). *Revolutionizing Medical Research: Scientists Develop Groundbreaking Privacy-Preserving AI*. Retrieved from scitechdaily.com: https://scitechdaily.com/revolutionizing-medical-research-scientists-develop-groundbreaking-privacy-preserving-ai/

Purificato, E., Boratto, L., & De Luca, E. W. (2024, Feb 15). User Modeling and User Profiling: A Comprehensive Survey. *arXiv*. Retrieved from https://arxiv.org/html/2402.09660v1#S3

Bryce Jensen
CS-370-11333-M01
4-2 Project One
6/1/2024

LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, *521*(7553), 436–444.

https://doi-org.ezproxy.snhu.edu/10.1038/nature14539