**Project One**

CS 370 Current/Emerging Trends in CS

Nicholle Caudy

7/19/2025

Neural networks are composed of algorithms utilized in machine learning models. These networks mimic the functions of the human brain and how it interprets information. Neural networks begin with input layers that receive the data intended for classification by the system. Each input neuron in the layer corresponds to a feature in the input data (Ghorakavi, 2025). Input moves through hidden layers, which use weights to process it for the output layer. Within the hidden layers of a neural network, the model learns to capture complex relationships between inputs. The final layer is the output layer which is responsible for producing the network’s classifications or predictions.

Neural networks offer a variety of applications that can enhance the personalization of user experiences. For example, Facebook uses a neural network that collects user information that includes previous searches, advertisements visited, reels or videos watched, and interactions with posts to personalize the user’s home page. This personalization includes loading ads that the user may find interesting, posts from pages or users that they interact with most at the top of the page. Such models, or their equivalents, are implemented in a range of widely used social media platforms, including Instagram, YouTube, and Twitter. Netflix also uses a neural network that collects data from previously watched or searched content to make recommendations to their users, making the experience more personalized.

There are ethical and hidden bias concerns when using neural networks and a “black box” classification system. When such systems are utilized for decision-making, challenges can arise if users are unable to explain the reasoning behind outcomes due to the "black box" nature of these systems. While inputs and outputs may be known, the internal processes that lead to specific decisions remain opaque, potentially leading to significant issues. For example, in 2018 Amazon developed an AI-based recruiting software intended to identify suitable candidates by analyzing data from past employment applications and interviews. The problem with this system was that it favored male applicants over female applicants for no coding reason that could be explained. The developers learned that the model had picked up gender bias based on this bias being present in past interviews. AI can be an effective tool when it is thoroughly tested, implemented, and audited to address ethical and bias concerns at an early stage.

The General Data Protection Regulation (GDPR), established by the European Union, comprises a comprehensive framework of laws and regulations designed to safeguard personal data. The GDPR follows seven principles, accountability, confidentiality, storage limitation, data minimization, purpose limitation, transparency, and accuracy. The GDPR's purpose limitation principle stipulates that data must be collected for specified, explicit purposes and should not be stored or repurposed for unrelated future uses. Personalizing user experiences involves collecting and storing data such as clicks, time spent on various posts or videos, websites visited, and location information for both current and future use. The GDPR’s purpose limitation may affect how this data can be used for personalization. Neural networks' hidden layers can obscure how user data is used, making transparency challenging. Another principle to look at is data minimization which restricts the amount of data that can be collected and analyzed and requires explicit consent for the collection and processing of that personal data, this can limit the data available for creating a personalized experience. Maintaining data accuracy is an important aspect of personalization, as it involves collecting, analyzing, and using data that is both relevant and up to date.

There are specific legal concerns that may arise from using neural networks as classifiers to personalize the user experience, transparency for one. Transparency involves informing users about the use of their data; however, this can be challenging due to the hidden layers, or “black box” characteristics present in neural networks. This can make it difficult to understand or explain how recommendations are made. Storage limitations can also be a legal concern as under GDPR regulations personal data should only be stored as long as necessary and storing personal data in excess could lead to fines. Another area that may create a legal concern is data minimization as collecting excessive data for the purpose of personalization by exceeding the requirements set by the GDRP. Inaccurate recommendations or biases produced from the neural network based on inaccurate data can cause legal concerns as accuracy is another principle of the GDPR.

Considering that we use the data collected to personalize our user’s experience, not collecting this data is not an option. Obtaining and analyzing data using neural networks is a vital part of ensuring our users continue to come back and interact with the software. For instance, if the personalization were not part of our model and users must scroll through numerous screens before they find something interesting, they are less likely to return. Collecting and storing user data also ensures that our users can share what they want, such as a picture or video, and they will be able to find it again in the future. Our users count on our personalization efforts to make their experience enjoyable.

One of the current trends in artificial intelligence and machine learning aimed at preserving privacy is Privacy Preserving Machine Learning (PPML). This initiative focuses on developing techniques to ensure confidentiality and privacy while training machine learning models. Data minimization is also a current trend in preserving privacy by only collecting necessary data to maintain privacy and remain compliant with data protection regulations. Securing informed user consent is a key best practice in AI and machine learning. Securing such consent prior to data collection ensures that users are fully aware of the data being gathered about them, as well as its intended current and future uses.

To be compliant with the GDPR regulations we will ask all our users for their consent to collect, analyze, and use their data to create a personalized experience while interacting with our software. If there are changes to how data will be collected or used, an updated consent will be provided via email and through software notifications. We will also allow our users the option to turn off data collection in the setting option of the menu. To allow for more transparency and user control of our neural network we will give the users a way to visualize how their data is being used and the option to decide what data they will allow our network to collect and use. Purpose limitation will also be part of our new model set up ensuring not to retain any information any longer than required to remain in compliance. Data minimization will also be in practice, gathering the least amount of data possible while still trying to create a personalized experience for our customers.

References:

Ghorakavi, V. (2025, July 11). *What is a neural network?*. GeeksforGeeks. <https://www.geeksforgeeks.org/machine-learning/neural-networks-a-beginners-guide/>

*How neural networks aid in Personalizing user experience*. RoboticsFAQ. (2023, April 12). <https://roboticsfaq.com/how-neural-networks-aid-in-personalizing-user-experience/>

Robinson, S. (2020, June 30). *Understanding how deep learning black box training creates bias: TechTarget*. Search Enterprise AI. https://www.techtarget.com/searchenterpriseai/feature/Understanding-how-deep-learning-black-box-training-creates-bias

Spillane, J. (2022a, December 8). *How GDPR can undermine personalization and user experience*. Business 2 Community. <https://web.archive.org/web/20230330083650/https://www.business2community.com/customer-experience/how-gdpr-can-undermine-personalization-and-user-experience-02108269>

Vrountas, T. (2019, July 2). *How much personalization is still possible in the Post-GDPR Era?*. Instapage. <https://instapage.com/blog/personalization-and-gdpr>

Ruehle, V., Sim, R., Yekhanin, S., Chandran, N., Chase, M., Jones, D., Laine, K., Köpf, B., Teevan, J., Kleewein, J., & Rajmohan, S. (2021, November 9). *Privacy preserving machine learning: Maintaining confidentiality and preserving trust*. Microsoft Research. <https://www.microsoft.com/en-us/research/blog/privacy-preserving-machine-learning-maintaining-confidentiality-and-preserving-trust/?msockid=3784723d78bd659a39576763790a6431>